EDMILSON MASSAO ITO

Análise de Risco do Serviço de Sincronização de Tempo

Dissertação apresentada ao Instituto de Pesquisas Tecnológicas do Estado de São Paulo – IPT, para obtenção do título de Mestre em Engenharia de Computação.

Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

São Paulo
Agosto 2007

Ficha Catalográfica
Elaborada pelo Departamento de Acervo e Informação Tecnológica – DAIT
do Instituto de Pesquisas Tecnológicas do Estado de São Paulo - IPT

I89a **Ito, Edmilson Massao**

Análise de risco do serviço de sincronização de tempo. / Edmilson Massao Ito. São Paulo, 2007.
161p.

Dissertação (Mestrado em Engenharia de Computação) - Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Área de concentração: Redes de Computadores.

Orientador: Prof. Dr. Volnys Borges Bernal

1. Análise de risco 2. Sincronização de tempo 3. Protocolo de tempo 4. NTP (Protocolo de tempo) 5. SNTP (Protocolo de tempo) 6. PTP (Protocolo de tempo) 7. Segurança 8. Tese I. Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Coordenadoria de Ensino Tecnológico II.Título

07-174 CDU 004.057.4(043)

DEDICAÇÃO

Dedico este trabalho a minha esposa que me apoiou e suportou os desafios desta jornada juntamente com nossos amados filhos, Laura e Tales.

À Eliete Tomaz Ito.

AGRADECIMENTOS

Primeiramente, meu sincero agradecimento ao professor orientador, Volnys Borges Bernal, o qual foi fundamental na concepção deste estudo. Sua contribuição foi o diferencial para elevar a qualidade e objetividade do trabalho.

Minha gratidão aos professores Adilson Guelfi e Edison Midorikawa pela formação da banca e por suas contribuições na qualificação e, sobretudo, na defesa da dissertação.

Ao IPT que forneceu todo apoio e tempo necessário para a conclusão deste trabalho.

As pessoas de bem que me fizeram transformar momentos difícies em desafios a serem conquistados.

Por fim, agradeço a Deus que me proporcionou enriquecer meus conhecimentos sobre um tema fascinante com uma singela contribuição aos interessados sobre a sincronização de tempo.

RESUMO

A precisão é uma propriedade importante na sincronização de tempo em sistemas computacionais distribuídos. Manter a precisão temporal em cada equipamento como, por exemplo, dispositivos de redes, estações e servidores, é crucial para garantir a ordem dos eventos ocorridos entre eles. Aplicações como sistemas de auditoria, alguns protocolos criptográficos e de redes, aplicações B2B e B2C necessitam de um serviço de sincronização de tempo na base de suas operações.

Protocolos de tempo possibilitam um serviço de sincronização de tempo preciso. Entretanto, um projeto ou configuração inapropriados podem ter falhas ou vulnerabilidades que, se exploradas, permitem alguns ataques à segurança desse serviço.

Através de uma avaliação de risco, este trabalho propõe determinar os riscos ao serviço de sincronização de tempo. Também, relacionar os possíveis controles de segurança disponíveis nos protocolos NTP, versão 3, NTP, versão 4, SNTP, versão 4, e PTP. E, por fim, selecionar os controles apropriados aos cenários de sincronização de tempo. Essas recomendações são para mitigar os riscos e garantir o funcionamento adequado do serviço sem eventos indesejados.

Palavras-chave: sincronização de tempo, protocolo de tempo, precisão, exatidão, UTC, TAI, X. 800, NTP, PTP e avaliação de risco.

ABSTRACT

The precision is an important property of time synchronization in distributed computer systems. To keep precision time in all equipment, for example, network device, workstations and servers, is crucial to guarantee the temporal order of events occurred between then. Applications such as audit systems, some cryptography and network protocols, B2B and B2C applications needs time synchronization service in their basis operations.

The precision in time synchronization service is aim with time protocols. However, designing a project or inappropriate configuration could be have flaws or vulnerabilities and, if exploits, allowing some security attacks.

A risk assessment is used to establish synchronization time service risks as well as identify the possible security controls of NTP, version 3, NTP, version 4, SNTP, version 4, and PTP. Finally, is selecting the proper controls in time synchronization scenarios. These recommendations are to mitigate risks and guarantee the proper working service method without undesired events.

Keywords: synchronization time, time protocols, precision, accurance, UTC, TAI, X. 800, NTP, PTP and risk assessment.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ACTS	*Automated Computer Time Service*
ATM	*Asynchronous Transfer Mode*
B2B	*Business to Business*
B2C	*Business to Commerce*
BIPM	*Bureau International des Poids et Mesures*
CCITT	*International Telegraph and Telephone Consultative Committee*
CGPM	*Conference Generale des Poids et Mesures*
CTP	*Classless Time Protocol*
DES-CBC	*Data Encryption Standard – Cyber Block Chaining*
DNS	*Domain Name System*
DSH	Divisão Serviço da Hora
FDDI	*Fiber Distributed Data Interface*
FIPS	*Federal Information Processing Standards*
GMT	*Greenwich Mean Time*
GPS	*Global Positioning System*
HDLC	*High-Level Datalink Control*
Hz	*Hertz*
IANA	*Internet Assigned Numbers Authority*
ICMP	*Internet Control Message Protocol*
ICP-Brasil	Infra-Estrutura de Chaves Públicas - Brasil
IDS	*Intrusion Detection System*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IGMP	*Internet Group Management Protocol*
INMETRO	Instituto de Metrologia
IP	*Internet Protocol*
IPS	*Intrusion Prevention System*
IPSEC	*IP Security*
ISC	*Internet Security Consortium*
ITU	*International Telecommunication Union*
KoD	*Kiss of Death*
LAN	*Local Area Network*
MAC	*Message Authentication Code*
MD5	*Message-Digest Algorithm 5*
MII	*Medium Independent Interface*
MPLS	*Multiprotocol Label Switching*
NIST	*National Institute of Standards and Technology*
NTP	*Network Time Protocol*
ON	Observatório Nacional
OSI	*Open Systems Interconnection*
OTM	*Ontime Marker*
PTP	*Precision Time Protocol*
Resinc/HLB	Rede de Sincronismo/Hora Legal Brasileira
RFC	*Request for Comments*
RNP	Rede Nacional de Pesquisa
RPC	*Remote Procedure Calls*
RSA	*Rivest Shamir Adleman*

SI	*Système International D´unités*
SNTP	*Simple Network Time Protocol*
SPB	Sistema de Pagamentos Brasileiro
SSH	*Secure Shell*
TAI	*Temps Atomique Internacional*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*
UTC	*Universal Time Coordinated*
VIM	Vocabulário Internacional de Termos Fundamentais e Gerais de Metrologia
VLAN	*Virtual Local Area Network*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

O termo “tempo” é utilizado, neste trabalho, para determinar uma ordem temporal dos eventos de forma cronológica em um período. Mas é possível abstrair inúmeras perspectivas sobre os seus diversos significados[1] também.

A ordem temporal dos eventos envolve inúmeras aplicações na atual era da informação. Allan, Ashby e Hodge (1997) afirmam que “o número e variedade de aplicações que utilizam precisão do tempo estão surpreendendo e aumentando”. A precisão[2] do tempo é um dos requisitos chave para a garantia da integridade dessas aplicações.

Para Lombardi (2002), são utilizados três tipos de informações relacionadas ao tempo: o instante, o intervalo e a freqüência. O instante é utilizado na programação de tarefas ou no registro de eventos que acontecem em uma determinada data e hora. Essas informações são utilizadas em diversos tipos de atividade no cotidiano do cidadão moderno. Marcar um encontro entre duas pessoas implica programar a presença delas em um local no mesmo instante. Mas, um uso mais sofisticado, e não tão perceptível, é o seu uso em atividades operacionais em bancos, ferrovias, aeroportos, comércio eletrônico, emissoras de televisão, companhia elétrica, as quais sincronizam seus horários para realizar suas operações. A segunda informação é o intervalo do tempo que se refere à duração de um determinado evento. Essa informação é uma medida quantitativa de tempo que pode ser dada em meses, semanas, dias, horas, minutos ou segundos; entretanto há atividades que necessitam de medidas de intervalos menores como milissegundo (10^{-3} s), microssegundo (10^{-6} s), nanossegundo (10^{-9} s) e até mesmo picos segundo (10^{-12} s). A terceira e última informação é a freqüência ou a taxa, na qual um determinado evento acontece. A freqüência pode ser determinada por meses, semanas, dias, horas, minutos ou segundos. Para o *Système International D´unités* (SI), o segundo

[1] O significado de tempo tem diferentes perspectivas dependendo do contexto utilizado; pode ser diferente em uma perspectiva científica, filosófica, histórica ou literária (RYBACZYK, 2005).

[2] Precisão é a proximidade da concordância entre resultados de testes independentes obtidos sob condições estipuladas. (ISO3534-1, 1993).

é uma unidade expressa em *hertz* (Hz) ou o número de oscilações por segundo. Um exemplo quase onipresente é a taxa de um cristal de quartzo utilizado em um típico relógio de pulso. O cristal é projetado para oscilar a 32.768 Hz e marcar a passagem de um segundo em um contador. Para registrar o tempo correto indefinidamente, um relógio deve ter sua freqüência inalterada ao longo do tempo. Porém, isso é praticamente impossível de acontecer:

> O relógio não pode ser ajustado perfeitamente; variações randômicas e sistemáticas são intrínsecas a qualquer oscilador, e quando estas variações randômicas são médias, o resultado oferecido não é bem comportado; tempo é uma função da posição e do movimento (efeitos relativos); e por último e invariavelmente, mudanças do ambiente causam variações da freqüência ideal do relógio (ALLAN; ASHBY; HODGE, 1997, p.15).

A qualidade do relógio depende, então, de como é construído, quão precisa e estável é sua freqüência e quanto imune está a interferências do ambiente. Mesmo um dos melhores relógios atômico[3] da atualidade necessita que sua exatidão temporal esteja em sincronia com uma escala de tempo oficial reconhecida internacionalmente como o *Universal Time Coordinated* (UTC) (BUREAU INTERNATIONAL DES POIDS ET MESURES, 2006).

1.1 UTC

Com a invenção do relógio atômico de césio, em 1955, e a criação do *Temps Atomique Internacional* (TAI), em 1958, foi possível melhorar a forma de registrar o tempo de maneira mais estável e precisa que a escala de tempo *Greenwich Mean Time* (GMT). Com a instituição do TAI, foi criada uma escala de tempo atômico baseada em dados provenientes de um conjunto mundial de relógios atômicos e, assim, instituída uma referência de tempo em conformidade com a definição do segundo instituída em 1967/68 pela 13° *Conference Generale des Poids et Mesures* (CGPM) do *Bureau International des Poids et Mesures* (BIPM). A definição da unidade fundamental de tempo segundo “é a duração de 9.192.631.770 períodos da radiação correspondente à transição entre dois níveis hiper-finos dos átomos de

[3] A incerteza temporal do relógio atômico NIST-F1 é de +- um segundo em 60 milhões de anos (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2006).

césio 133 em seu estado básico" (BUREAU INTERNATIONAL DES POIDS ET MESURES, 2006).

O TAI é uma escala atômica uniforme e estável o qual não mantém relação com a rotação irregular da Terra. Porém, foi necessário criar uma escala de tempo que ao longo dos anos tivesse relação com o GMT. Dessa maneira, a criação do UTC foi justamente para ser idêntico ao TAI, exceto que, de tempos em tempos, um segundo intercalado deve ser adicionado ou removido do UTC para compensar a rotação irregular da Terra. Assim, em 1972, o GMT foi substituído pelo UTC sendo, desde então, uma escala de tempo coordenada que constitui a base de referência para disseminação do tempo e freqüência ao uso público.

1.2 Ambiente Distribuído

Em um ambiente de sistemas distribuídos[4] o sincronismo a uma escala de tempo oficial é algo complexo. Muito mais que simplesmente acertar o relógio de pulso em intervalos freqüentes. Na ordem temporal dos eventos em ambientes de sistemas distribuídos, algumas vezes, é impossível dizer qual evento entre dois eventos ocorre primeiro. Como estudado anteriormente por Lamport (1978), a relação "acontecido-antes é somente uma ordenação parcial de eventos no sistema" (LAMPORT, 1978, p. 01). Na ordenação parcial, uma mensagem que possui o tempo enviado de um determinado evento deve chegar ao destino sempre com um tempo posterior ao enviado. Para Mills (2006a), a relação definida por Lamport é garantida desde que os computadores assumam a mesma freqüência conforme afirmado:

> No estudo de Lamport todos os relógios dos computadores assumem a mesma freqüência e cada mensagem enviada possui o tempo de envio definido pelo relógio do computador-origem. O tempo nunca retroage o que garante a relação "acontecido-antes" sempre ser satisfeita (MILLS, 2006a, p. 2).

Entretanto, relógios reais podem funcionar em diferentes taxas e assim ter diferentes medidas de tempo se comparados entre si. Tais relógios, normalmente, são

[4] Sistema distribuído consiste de uma coleção de processos distintos os quais são separados em relação ao espaço e se comunicam trocando mensagens entre eles. (Lamport, 1978, p. 1)

construídos com cristal de quartzo e sua incerteza temporal pode variar de acordo com sua qualidade e de acordo com o ambiente em que estão inseridos. Para que os eventos em sistemas distribuídos aconteçam sempre de forma cronológica, o tempo registrado pelos relógios deve estar sincronizado ou ser exato em relação a uma referência ou escala de tempo. Existe a possibilidade de ocorrer o sincronismo de forma direta entre cada computador e o relógio de referência, mas isso requer um mecanismo especializado como um receptor GPS (ALLAN; ASHBY; HODGE, 1997), *modem* ou uma conexão com algum servidor de tempo através de um aplicativo ou protocolo de tempo. Por questões de custo e de conveniência, "não é viável equipar cada computador com um mecanismo dedicado para a comunicação com um relógio referência" (MILLS, 2006a, p. 3). Assim, protocolos de tempo têm uma enorme contribuição em ajustar as taxas dos relógios e melhorar a exatidão com uma escala de tempo reconhecida internacionalmente como o UTC, além de satisfazer a ordenação dos eventos.

De maneira geral, protocolos de tempo distribuem o tempo obtido em um ou vários servidores para diferentes computadores clientes e ajustam a diferença dos relógios de cada um deles. Os clientes enviam uma mensagem requisitando o tempo corrente do servidor e esse responde com o tempo registrado em seu relógio. Normalmente, o atraso de propagação da mensagem é calculado e adicionado à diferença dos relógios, oferecendo uma maior precisão.

A sincronização de tempo entre os sistemas computacionais distribuídos é essencial em diversas situações como, por exemplo, no registro da modificação de sistemas de arquivos em um ambiente computacional, serviços de bilhetagem, serviços de correio eletrônico, protocolos de sistemas de autenticação, entre outros. Adicionalmente, aplicações de registros de eventos, rastreabilidade[5] de eventos de segurança e transmissão de arquivos eletrônicos requerem o uso de um tempo preciso. Em outros ambientes, a necessidade da sincronização de tempo é essencial em suas operações como no controle de tráfego aéreo, nos serviços financeiros de

[5] Propriedade do resultado de uma medição ou do valor de um padrão estar relacionado a referências estabelecidas, geralmente a padrões nacionais ou internacionais, através de uma cadeia contínua de comparações, todas tendo incertezas estabelecidas. (INMETRO, 1995, p. 61)

mercado de capitais, na programação de rádio e televisão, nas companhias elétricas, entre outros.

“Para ter a exatidão na ordem de milissegundo é requerido que os clientes troquem mensagens com os servidores a cada quinze minutos. Entretanto, se os requisitos de exatidão forem na ordem de dezenas de milissegundo, as atualizações de tempo podem aumentar para um dia e meio” (MILLS, 2006a, p. 6).

Um serviço de sincronização de tempo confiável em sistemas distribuídos deve prevenir ataques maliciosos e atividades acidentais em seus servidores e clientes e, assim, manter a exatidão temporal, na ordem de milissegundo ou dezenas de milissegundo, como citado por Mills (2006a). Inúmeros sistemas dependem da precisão e exatidão temporal para suas funcionalidades operacionais, comerciais ou até mesmo legais, como a assinatura de contratos de câmbio no sistema financeiro. Também, comprometer o sincronismo de tempo pode ser estratégico em determinados ataques. Assim, é fundamental que o fornecimento do serviço de sincronização de tempo tenha controles de segurança instalados para reduzir os riscos de intrusão, maximizar a disponibilidade do serviço, maximizar a exatidão da disseminação do tempo e minimizar o consumo do processamento de recursos.

1.3 Motivação

A geração, conservação e dissiminação da hora legal através do Observatório Nacional (ON) instituem um marco na utilização do sincronismo de tempo no Brasil. A demanda de sincronismo em tempo real no novo Sistema de Pagamentos Brasileiro (SPB) e para a instituição da infra-estrutura de chaves públicas do Brasil (ICP-Brasil) são exemplos no avanço das necessidades desse serviço. O departamento Divisão Serviço da Hora do ON está estabelecendo uma rede de sincronismo à hora legal brasileira (SILVA, 2002) bem como oferecer os padrões nacionais de freqüência que são a base da rastreabilidade metrológica brasileira em tempo e freqüência conforme designado pelo INMETRO.

Durante os anos, o sincronismo de tempo em sistemas distribuídos sempre foi considerado periférico e observado como um serviço opcional. Sua citação na literatura tem sido supérflua ou inexistente, tanto que na última edição do livro *Computer Networks* de Tanenbaum (2003), não há registro sobre a sincronização de tempo e, muito menos, sobre um dos protocolos mais antigos e divulgados na Internet nos dias de hoje, o NTP (MILLS, 1992). A primeira especificação do protocolo NTP (MILLS, 1985) foi publicada no ano de 1985, apenas dois anos depois da primeira especificação do protocolo *Domain Name Systems* (DNS) (MOCKAPETRIS, 1983). Mas as diferenças na divulgação e o grau de importância dado ao NTP está bem longe do ideal devido as atuais necessidades.

Atualmente, há um aumento na demanda do serviço de dissiminação da hora legal para atender aplicações e serviços que demandam uma referência de tempo. Porém, tal serviço deve oferecer requisitos mínimos de segurança. A ausência do atendimento de tais requisitos pode ser uma deficiência dos mecanismos de segurança oferecidos pelos protocolos ou a não-utilização de controles opcionais existentes que raramente são configurados de maneira satisfatória.

Com o uso mais freqüente do serviço de sincronismo de tempo e sua importância nos dias de hoje, oferecer controles de segurança para a proteção da integridade e

disponibilidade passam a ser requisitos obrigatórios a fim de garantir a confiabilidade de tal serviço.

1.4 Objetivos

Este trabalho tem como objetivos:

a) Apresentar os principais cenários de sincronização de tempo;
b) Realizar uma análise de risco do serviço de sincronização de tempo e identificar os possíveis controles de segurança oferecidos pelos protocolos de tempo do escopo deste trabalho;
c) Selecionar e classificar os controles de segurança que devem ser configurados para a mitigação de riscos de cada cenário.

Este estudo será focado nos serviços de segurança intrínsecos aos protocolos de tempo do escopo proposto. Pressupõe-se que controles em nível de rede não serão estudados, pois não são controles da análise de risco deste trabalho. Por fim, será apresentada uma consolidação dos controles necessários para a instalação e operação de um serviço de sincronização de tempo seguro.

1.5 Escopo

Este trabalho limita-se na análise de risco do serviço de sincronização de tempo oferecida pelos protocolos de tempo do escopo deste estudo. Também, selecionar os serviços e mecanismos de segurança associados a cada um deles, considerando os riscos das ameaças e vulnerabilidades, geradas neste trabalho, para os principais cenários de sincronização de tempo apresentados.

Algumas características foram selecionadas para a escolha dos protocolos a serem comparados, pois, entre as opções, algumas estão em desuso, outras ainda não são referências normatizadas e, por fim, algumas não são adequadas para um modelo de sistema distribuído. Abaixo , as características consideradas:

a) Ser um protocolo projetado para operar em redes TCP/IP;
b) Ser um protocolo com relação custo/benefício viável;
c) Ser uma tecnologia aprovada por organismos internacionais de normalização;
d) Ter o desenvolvimento consistente ao longo dos anos;
e) Ter um cenário de uso prático em sistemas distribuídos.

Dessa maneira, para o escopo do trabalho, foram escolhidos os seguintes protocolos de tempo:

a) NTP, versão 3 e versão 4;
b) SNTP, versão 4;
c) PTP.

A exclusão dos outros protocolos pesquisados - *Time*, *Daytime*, TEMPO, ACTS, CTS e dos serviços de radiofreqüência - deve-se a algum dos seguintes fatos:

a) Nenhum desenvolvimento técnico desde a primeira versão;
b) Uso específico em um determinado cenário;
c) Ser um estudo sem apoio de órgãos de normatização;
d) Não estar disponível para uso comercial no país;

Assim, o foco deste trabalho são os serviços e mecanismos de segurança inerentes aos protocolos NTP, versão 3, NTP, versão 4, SNTP, versão 4 e PTP. Os três primeiros protocolos são tratados como família NTP quando for conveniente agrupar funcionalidades de uso comum. Pressupõem-se alguns controles de rede dos ambientes de redes estudados, mas não é parte da análise de segurança deste trabalho. Também, não são consideradas as vulnerabilidades de sistemas operacionais, de dispositivos de redes, de estações e servidores. Eventualmente, será possível a apresentação de alguns controles adicionais para o enriquecimento deste trabalho e melhor entendimento de eventuais conceitos, mas não é foco deste estudo.

Por fim, não fazem parte do escopo questões relacionadas à análise de desempenho, análise experimental dos protocolos, análises sobre a precisão temporal, implantação de alguma solução ou estudo de caso dos protocolos.

1.6 Materiais e Métodos

A metodologia adotada neste trabalho foi baseada nas seguintes atividades:

a) Coleta e análise de padrões aprovados por entidades especializadas na sincronização de tempo, em segurança da informação, em protocolos de comunicações e na padronização de regras para a comunicação na Internet;
b) Busca do estado da arte em estudos científicos através de levantamento de publicações científicas especializadas em tecnologia sobre a sincronização de tempo e segurança da informação;
c) Identificação dos cenários típicos de sincronização de tempo e os requisitos de segurança em cada um dos cenários;
d) Identificação dos serviços e mecanismos de segurança oferecidos em cada um dos protocolos;
e) Utilizar a metodologia de análise de risco.

1.7 Estrutura da Dissertação

O capítulo dois contém os principais conceitos da exatidão da hora e a precisão dos relógios. Descreve os protocolos e serviços de sincronização de tempo e temas relacionados caso existam.

O capítulo três descreve a recomendação X. 800 *Security Architecture for Open Systems Interconnection for CCITT Applications* (INTERNATION TELECOMMUNICATION UNION, 1991), o qual este trabalho se baseia como orientação das definições e conceitos de segurança. São descritos os serviços e mecanismos de proteção e os tipos de ataques ativos e passivos.

No capítulo quatro há a apresentação aprofundada da arquitetura dos protocolos de tempo do escopo do trabalho e o funcionamento de cada um deles.

No quinto capítulo são apresentados os principais cenários de sincronização de tempo. É descrito como cada cenário é composto pelo ambiente de rede e pelas configurações dos protocolos de tempo, para tratar as questões de disseminação da hora.

No sexto capítulo são listadas as ameaças, as vulnerabilidades, as probabilidade, os impactos e é determinado o grau de risco para cada par de ameaça e vulnerabilidade.

No sétimo capítulo, há a relação dos possíveis controles dos protocolos de tempo determinados no escopo deste trabalho.

No capítulo oito, é realizado a análise de risco dos cenários de sincronização de tempo. Também, é apresentado o resultado da análise com os controles de segurança indicados para mitigação obrigatória, recomendada e opcional de cada cenário. Por fim, é feito uma consolidação dos resultados através de uma visão geral.

No nono capítulo, é feito a conclusão do trabalho onde são descritas as contribuições, as dificuldades encontradas e algumas sugestões para trabalhos futuros.

2 INTRODUÇÃO AOS PROTOCOLOS E SERVIÇOS DE SINCRONIZAÇÃO DE TEMPO

Os protocolos de tempo oferecem diferentes níveis de precisões e diferentes serviços de segurança. Entre aqueles pesquisados, os protocolos *Time* (POSTEL; HARRENSTIEN, 1983) e *Daytime* (POSTEL, 1983) foram normatizados em 1983 e praticamente foram substituídos pelo NTP (MILLS, 1992). Com uso limitado em uma determinada plataforma, o protocolo *TEMPO* (GUSELLA; ZATTI, 1989) tornou-se referência em inúmeros estudos, mas foi praticamente extinto. Há aqueles que sobressaem e têm evoluções em novas versões incluindo novas funcionalidades como, por exemplo, o NTP. Também, vários protocolos são desenvolvidos com funcionalidades para atender lacunas existentes. Esse capítulo apresenta uma visão geral acerca dos protocolos de tempo e de alguns serviços que fazem uso de tais protocolos.

2.1 Protocolos de Tempo

2.1.1 NTP versão 3

O protocolo NTP *Network Time Protocol* (MILLS, 1992) é amplamente utilizado e fornece um método de sincronizar o relógio dos servidores e estações em um ambiente computacional distribuído. “Os mecanismos utilizados permitem, em princípio, a precisão da sincronia do tempo na ordem de nanossegundo” (MILLS, 1992, p. 1). O protocolo inclui provisão para especificar as características e estimar os erros do relógio local e os servidores de tempo com os quais eles sincronizam. Também, há provisão de operações com inúmeras referências de tempo em níveis hierárquicos distribuídos através de relógio atômico ou relógios de radiofreqüência.

Uma associação NTP é formada quando dois parceiros trocam mensagens e um ou ambos criam e mantém uma instância do protocolo, com exceção do modo *broadcast*. Expressões como “servidor, cliente, hospedeiro e parceiro pode ser aplicado ao mesmo dispositivo NTP de acordo com a função no modo o qual o dispositivo opera” (RYBACZYK, 2005, p. 64). Isto se faz observar sempre sob o

contexto do modo de operação. “Clientes fazem as requisições, enquanto servidores respondem as requisições dos clientes ou advertem serviços sem solicitações” (RYBACZYK, 2005, p. 64). O termo hospedeiro diz respeito à instância do protocolo no processador local e a terminologia parceiro refere-se à instância do protocolo no processador remoto (MILLS, 1992).

Os modos de operação do protocolo NTP são categorizados em cinco tipos (MILLS, 1992, p. 17) como descritos a seguir:

a) Modo Simétrico Ativo: um hospedeiro envia mensagens periódicas sem considerar o estado de disponibilidade ou qual é o estrato de seus parceiros. O hospedeiro anuncia sua prontidão de sincronizar e ser sincronizado pelos parceiros;
b) Modo Simétrico Passivo: esse tipo de associação é realizado no recebimento da mensagem dos parceiros que operam no modo simétrico ativo. A associação persiste enquanto o parceiro, em modo simétrico ativo, enviar mensagens. Nesse modo de operação, o parceiro ativo opera em um estrato de grau menor ou igual ao hóspede simétrico passivo, que anuncia sua prontidão de sincronizar e ser sincronizado pelos parceiros;
c) Modo Cliente: o hospedeiro envia mensagens periódicas independentemente do estado de disponibilidade ou do estrato de seus parceiros. Utilizado normalmente em computadores de redes locais, o hospedeiro anuncia sua prontidão para ser sincronizado pelos parceiros;
d) Modo Servidor: essa associação é criada através da chegada da mensagem do cliente requisitando a sincronia. A associação existe somente na resposta da requisição do cliente, depois disso a associação é dissolvida. O hospedeiro, nesse modo, normalmente o servidor de tempo da rede local, anuncia sua prontidão para sincronizar seus parceiros e não ser sincronizado por nenhum deles;
e) Modo *Broadcast*: o hospedeiro envia mensagens periódicas independentemente do estado de disponibilidade ou estrato de seus parceiros. Operando nesse modo, o hospedeiro, normalmente um servidor de tempo na rede local, anuncia sua prontidão de sincronizar todos os seus parceiros e não ser sincronizado por nenhum deles.

Um serviço de sincronização de tempo confiável requer provisões para prevenir ataques acidentais ou maliciosos nos clientes e servidores que participam desse serviço. O NTPv3 inclui mecanismos opcionais como controles de acesso e autenticação simétrica através de chave compartilhada. Não há qualquer mecanismo de distribuição e gerenciamento destas chaves, o que dificulta uma instalação em escala segura.

2.2.2 NTP versão 4

Apesar do protocolo NTP versão 4 consistir de um pacote de extensões da versão 3, “sua especificação definitiva ainda não está disponível” (MILLS, 2006a, p. 12). A versão 4 é compatível com as versões anteriores e novos métodos foram incorporados para descobrir os servidores e selecionar automaticamente entre eles o mais preciso. Outra nova funcionalidade está no tratamento da autenticação que suporta um esquema alternativo denominado *Autokey.* Conforme descrito por Mills (2006):

> Esse esquema é baseado em duas chaves: uma privada e outra pública. A chave secreta é usada para construir uma assinatura e nunca é revelada. A chave pública é distribuída por meios inseguros e é usado pelos clientes para verificar a assinatura. O protocolo que troca as chaves públicas e os valores relativos assim como cada mensagem NTP validada automaticamente (MILLS, 2006a, p. 31).

2.2.3 SNTP (*Simple Network Time Protocol*) versão 4

O protocolo SNTP, versão 4, (MILLS, 2006c) é um subconjunto do protocolo NTP. O SNTP pode ser usado quando não for necessário ou justificado o desempenho do NTP. Por ser um subconjunto do NTP sua interoperabilidade com tal protocolo é compatível com qualquer implantação NTP sem necessidade de alteração do pacote.

A única modificação significativa do SNTP, em relação à versão anterior foi à interpretação do cabeçalho para se adequar à nova versão do protocolo IP (*Internet Protocol*), versão 6, (DEERING; HIDEN, 1998). Também, essa versão inclui

extensões opcionais como modo *manycast* e autenticação baseada em chaves públicas.

No SNTP “uma referência para endereçamento de *broadcast* significa endereçamento de *broadcast* IP, versão 4, endereçamento de grupo *multicast* IP, versão 4, ou endereçamento IP, versão 6, de um escopo apropriado” (MILLS, 2006c, p. 4). O protocolo SNTP pode operar com endereçamento nos modos *unicast* (ponto-a-ponto), *broadcast* e *multicast* (ponto-a-multiponto) ou *manycast* (multiponto-a-ponto) detalhados a seguir:

a) Modo *Unicast*: O cliente envia uma requisição ao servidor em seu endereço *unicast* e aguarda uma resposta dele. Com a resposta é possível determinar o tempo e, opcionalmente, o atraso de viagem do pacote e o deslocamento relativo ao relógio do servidor.
b) Modo *Broadcast* ou *Multicast*: Nesse modo, um servidor de tempo envia periodicamente mensagens não solicitadas ao endereço de *broadcast* IP. Os clientes apenas recebem a mensagem enviada pelo servidor e não retornam nenhuma mensagem.
c) Modo *Manycast*: Esse modo é uma extensão do padrão *anycast* definido na (PARTRIDGE; MENDEZ; MILLIKEN, 1993). O modo *manycast* é projetado para oferecer o serviço de sincronização de tempo através de um conjunto de servidores cooperando entre si e responder as requisições dos clientes. Nesse modo, o cliente envia a requisição a um endereço de *multicast* IP e aguarda uma resposta de um dos servidores configurados em modo *multicast* também. O cliente faz a associação com o primeiro servidor estabelecido na comunicação e opera em modo *unicast* subsequentemente.

O protocolo SNTP é um serviço vulnerável e é fortemente recomendada a instalação de controle de acesso e/ou autenticação criptográfica a fim de prover um grau de segurança adequado. Segundo Mills (2006a) “sem autenticação criptográfica, o serviço SNTP versão 4 é vulnerável a interrupções ocasionadas por mau comportamento ou servidores SNTP ou NTP de *broadcast* hostis” (MILLS, 2006c, p. 23).

2.2.4 Protocolo *Time*

Uma versão mais antiga de sincronização de tempo e menos utilizada nos dias de hoje é o *Time Protocol* (POSTEL; HARRENSTIEN, 1983), que opera tanto sobre o protocolo UDP quanto sobre TCP. O *Time Protocol* permite a sincronização de tempo entre clientes e servidores na ordem de segundos. *Time Protocol* sobre UDP ou TCP não fornece mecanismos de compensação do atraso de propagação da mensagem na rede nem tão pouco erros similar na origem.

2.2.5 Protocolo *Daytime*

Serviço tradicional oferecido por diversos sistemas, porém utilizado somente para a consulta de tempo. Protocolo utilizado em computadores menores que rodam MS-DOS e sistema operacional similar. A comunicação se dá através da porta 13 do servidor o qual responde no formato TCP/IP ou UDP/IP (POSTEL, 1983). O padrão não especifica o formato exato, mas requisita que o tempo enviado seja através dos caracteres ASCII.

2.2.6 TEMPO

Serviço distribuído que sincronizam os relógios do sistema Berkeley UNIX 4.3 BSD (GUSELLA; ZATTI, 1989). TEMPO é um serviço que funciona em uma rede local e consiste em uma coleção de *daemons* de tempo, uma por máquina, e é baseado em uma estrutura mestre-escravo. Um *daemon* mestre mede a diferença de tempo entre o relógio em que está rodando e as outras máquinas. Esta diferença é a média de tempo fornecida por todos os participantes. O mestre envia para cada *daemon* escravo a correção de tempo de cada relógio dos computadores.

2.2.7 ACTS (Automated Computer Time Service)

“O serviço ACTS foi desenvolvido pelo NIST em 1988 com o objetivo de fornecer o sincronismo de tempo através de uma linha telefônica e um modem analógico” (LOMBARDI, 2002, p. 60). Quando um computador utiliza o serviço ACTS ele recebe um código de tempo no padrão ASCII. No computador de origem há um interpretador desse código que atualiza o relógio local à hora correta.

O último caractere do código é um asterisco (*), o qual é denominado *ontime marker* (OTM). Esse caractere determina que a hora enviada seja a hora a ser utilizada. Por exemplo, se foi enviado o instante de tempo 4:15:15, esse é o instante a ser configurado quando na recepção do OTM. A fim de compensar a latência de transmissão do OTM entre a origem e o destino, ele é enviado com antecedência de 45 milissegundos. Isto significa que são utilizados 8 milissegundos no envio do OTM em uma taxa de 1200 *baud*, 7 milissegundos de transmissão média para qualquer usuário-destino nos Estados Unidos e 30 milissegundos no processamento do modem. Esse tempo de 45 milissegundos de antecedência foi escolhido baseado em experimentos pelo próprio NIST.

Também é possível utilizar técnicas de *loop-back* para calibrar a latência de transmissão do pacote para diminuir as incertezas da sincronização. Dessa forma, a precisão aumenta significativamente e o modelo de 45 milissegundos do OTM é inutilizado. Para receber o código de tempo completo, a conexão deve ser realizada a uma velocidade de, no mínimo, 1200 *bauds*.

2.2.8 IEEE 1588 – PTP (*Precision Time Protocol*)

O protocolo PTP descrito em (EIDSON; FISHER; WHITE, 2002) foi desenvolvido originalmente pela empresa Agilent para sistemas de controle e medidas largamente utilizadas em automação industrial. Porém, a necessidade de sincronização, na ordem de microssegundos, é real e não se limita à necessidade original, como apresentado no Quadro 1.

Área de Aplicação	Exemplos	Precisão de sincronização
Sensores de baixa velocidade	Pressão e Temperatura	Milissegundo
Dispositivos eletromecânicos	*Relay*, freios, solenóides e válvulas	Milissegundo
Automação geral	Manuseio de material, processo químico	Milissegundo
Controle de movimento preciso	Empacotamento de alta-velocidade, Impressão e Robótica	Poucos Microssegundos
Dispositivos elétricos de alta velocidade	Medição de sincrofase	Microssegundos
Cobertura eletrônica	Detecção de falhas e triangulação	Submicrossegundo

Quadro 1. Sincronização para algumas aplicações. Fonte: (EIDSON; FISHER; WHITE, 2002).

O padrão IEEE 1588 (EIDSON; FISHER; WHITE, 2002) foi aprovado pelo IEEE em novembro de 2002 e, em 2004, também foi aprovado como um padrão IEC 61588. Com esse protocolo é possível o sincronismo dos relógios locais dos dispositivos com uma precisão menor que microssegundo.

O PTP é baseado na melhor conciliação de tempo entre os dados transmitidos e recebidos. Diferentemente do SNTP, a informação de sincronização não necessita ser transmitida no mesmo pacote, mas é enviada no pacote seguinte. O protocolo foi desenvolvido para redes locais de diferentes tipos. Utiliza pouco recurso computacional podendo ser utilizado em dispositivos terminais de baixo custo. Assim, não necessita de requisitos especiais de desempenho de processamento e do uso de memória, além de uso mínimo de largura de banda dos canais de comunicação de redes.

Dentro do domínio PTP, o algoritmo desenvolvido configura automaticamente o melhor relógio mestre entre os relógios dos dispositivos participantes. Também fornece tolerância a falhas como redundância do relógio mestre. “O protocolo não foi projetado para operar na Internet ou ambiente computacional geral, sendo esses ambientes tipicamente atendidos pela família de protocolos NTP” (EIDSON; FISHER; WHITE, p. 245).

2.2.9 CTP (*Classless Time Protocol*)

O protocolo CTP (GUREWITZ; CIDON; SIDI, 2003) é uma proposta de sincronização de tempo em ambiente distribuído em modo de operação ponto-a-ponto. O objetivo do estudo do CTP é reduzir o ajuste de erros dos relógios utilizando modelo não-hierárquico. Cada nó da rede envia e recebe pacotes *probe* somente para seus vizinhos, ajustando assim apropriadamente seus relógios.

2.3 Serviços de Sincronização de Tempo

2.3.1 Serviço de receptores de radiofreqüência

Uma das desvantagens dos protocolos e dos serviços de conexão discada é a necessidade de se manter conectado em cada instante de sincronização, seja através da Internet, seja através de ligações telefônicas. O sincronismo é realizado sem dependência de provedores de serviços de telefonia, pois é possível utilizar receptores de radiofreqüência para o acerto da hora. Porém, é necessário verificar se o sinal está disponível na área onde será instalado o receptor. Nos Estados Unidos, esse serviço é disponibilizado pelo NIST através de ondas de rádio de baixa freqüência e do GPS.

2.3.2 Serviço Resinc/HLB – Observatório Nacional

O Observatório Nacional, através da Divisão Serviço da Hora (DSH), mantém uma rede de sincronismo à hora legal brasileira (Resinc/HLB) com o objetivo de atender os órgãos públicos, as empresas e outros clientes que necessitam de uma fonte de hora confiável e rastreável pelo padrão nacional e internacional (SILVA, 2002). A Resinc/HLB possui dois serviços de sincronia de relógio. O primeiro, através da Internet, o qual tem imprecisão de um segundo aproximadamente e que atende o público geral. O segundo serviço é oferecido a clientes corporativos que necessitam de maior segurança e é fornecido através de um equipamento próprio utilizando o protocolo ACTS. O acesso a esse sistema é feito através de uma linha telefônica

discada. A sincronização é realizada de hora em hora, com garantia de um erro máximo menor que cinco milissegundos, tanto para mais quanto para menos. Somente esse serviço tem um certificado emitido mensalmente pelo ON, o que garante a sincronização de tal equipamento com o relógio atômico do ON.

3 CONCEITOS DE SEGURANÇA

3.1 Princípios e arquitetura

O foco da segurança de redes consiste de medidas com o objetivo de detectar, prevenir, deter e corrigir violações de segurança que envolve a transmissão de informação. Segundo Stallings (2003), a análise da segurança em um ambiente de comunicação e redes de dados não é tão simples como possa parecer em um primeiro momento. De fato, a maioria dos requisitos aos serviços de segurança pode ser dada uma palavra com rótulo auto-explanatório: confidencialidade, autenticação, irretratabilidade e integridade. E os mecanismos usados para implantar esses requisitos são bem mais complexos segundo Stallings (2003)**.** Similarmente, Tanenbaum (2003) cita que esta divisão grosseira em quatro áreas interligadas, é o que vem em mente quando as pessoas pensam sobre segurança de rede. Para ele, todos esses aspectos ocorrem em sistemas tradicionais, mas com algumas diferenças significantes.

3.2 Arquitetura de Segurança OSI X.800

Ao definir os requisitos de segurança de forma efetiva a fim de assegurar a qualidade necessária dos produtos e das políticas, é preciso um modelo sistemático que atenda as dificuldades de um ambiente de processamento de dados. A recomendação X. 800 – *Security Architecture for OSI* (INTERNATION TELECOMMUNICATION UNION, 1991) define um modelo que atende os requisitos de segurança. Essa recomendação é útil no gerenciamento e na organização das tarefas relativas aos serviços de segurança. Adicionalmente, essa arquitetura é adotada por fabricantes de computadores e fornecedores do segmento de comunicação de dados no desenvolvimento de seus produtos e serviços. A arquitetura de segurança OSI é um padrão internacional e é baseada em uma estrutura de serviços, mecanismos e ataques.

Na recomendação X. 800 (INTERNATION TELECOMMUNICATION UNION, 1991) os serviços de segurança são divididos em cinco tipos de serviços em catorze categorias específicas. Em cada serviço é recomendado um mecanismo para a mitigação de riscos conforme Quadro 2.

		Mecanismos							
Serviços		Criptografia	Assinatura Digital	Controle de acesso	Integridade de dados	Troca de Autenticação	Preenchimento de tráfego	Controle de roteamento	Árbitro
Autenticação	Entidade Parceira	√	√			√			
	Origem dos Dados	√	√						
Controle de acesso	Controle de acesso			√					
Confidencialidade	Com conexão	√						√	
	Sem conexão	√						√	
	Campo seletivo	√							
	Fluxo do tráfego	√					√	√	
Integridade	Com recuperação de conexão	√			√				
	Sem-recuperação na conexão	√			√				
	Campo seletivo com conexão	√			√				
	Campo seletivo sem conexão	√	√		√				
	Sem conexão	√	√		√				
Irretratabilidade	Origem		√		√				√
	Destino		√		√				√

Quadro 2: Mapa de serviços e mecanismos. Fonte: INTERNATION TELECOMMUNICATION UNION (1991).

3.3 Serviços de Segurança X. 800

Um serviço de segurança, segundo a recomendação X. 800 (INTERNATION TELECOMMUNICATION UNION, 1991), é definido como um serviço fornecido por um protocolo de uma camada da comunicação, o qual assegura a adequação da segurança dos sistemas ou da transmissão dos dados. Segundo Shirey (2000), o termo serviço é descrito como:

> Um processamento ou serviço de comunicação que é fornecido por um sistema para dar um tipo específico de proteção aos recursos do sistema. Serviços de segurança implantam políticas de segurança e são implantados por mecanismos de segurança (SHIREY, 2000, p.154).

A disponibilidade[6] não é considerada um serviço de segurança, mas uma propriedade do serviço de comunicação. Porém, neste trabalho, a disponibilidade será entendida como um serviço de segurança dos protocolos de tempo, pois são analisadas vulnerabilidades relacionadas à negação do serviço de sincronização de tempo.

De forma similar, a confiabilidade[7] não é considerada um serviço de segurança na recomendação X. 800 (INTERNATION TELECOMMUNICATION UNION, 1991). Porém, será entendida como um serviço de segurança neste trabalho, principalmente, para determinar uma propriedade particular na configuração dos protocolos da família NTP descrita posteriormente.

3.3.1 Serviço de autenticação

Esse serviço deve garantir que a comunicação é autêntica entre duas entidades e que a conexão não sofreu interferência a fim de permitir personificação de uma das entidades legítimas. Duas autenticações específicas são definidas:

---

[6] A disponibilidade do serviço de comunicação é determinada pelo projeto de rede e/ou protocolos de gerenciamento de rede. Escolhas apropriadas são necessárias para proteção contra a negação de serviço (INTERNATION TELECOMMUNICATION UNION , 1991, p. 27).

[7] A confiabilidade é a habilidade de um sistema operar uma função sob condições estipuladas por um período de tempo especificado (SHIREY, 2000)

a) Autenticação da entidade parceira: usada na associação de identidades parceiras para fornecer confidencialidade entre as entidades conectadas;
b) Autenticação da origem dos dados: em uma transferência sem conexão, esse serviço fornece a garantia de que os dados recebidos são da entidade de origem.

3.3.2 Serviço de confiabilidade

“A confiabilidade é a habilidade de um sistema operar uma determinada função sob condições estipuladas por um período de tempo” (SHIREY, 2000, p. 140). A confiabilidade está relacionada a baixa probabilidade do sistema falhar durante sua disponibilidade operacional. Esse serviço endereça preocupações com a qualidade e robustez durante sua operação e está associada normalmente a capacidade de recuperação e tolerância a falhas.

3.3.3 Serviço de confidencialidade de dados

A confidencialidade deve proteger os dados transmitidos a fim de prevenir a divulgação do conteúdo à entidade não autorizada. São quatro tipos de confidencialidade de dados definidas no padrão:

a) Confidencialidade de conexão: proteção dos dados transmitidos a todos os usuários na conexão TCP/IP;
b) Confidencialidade sem conexão: proteção dos dados transmitidos de todos os usuários em uma única mensagem;
c) Confidencialidade de campo seletivo: proteção dos dados transmitidos em um determinado campo da mensagem;
d) Confidencialidade de fluxo de tráfego: proteção dos dados transmitidos da análise de um atacante no fluxo de tráfego.

3.3.4 Serviço de controle de acesso

Esse serviço limita e controla o acesso aos sistemas e aplicações hospedados em dispositivos através de canais de comunicações. Cada entidade deve ser identificada ou autenticada e fornecer as devidas permissões em cada acesso.

3.3.5 Serviço de Disponibilidade

A disponibilidade é a propriedade de um sistema ou um recurso do sistema ser acessado e usado através de uma entidade autorizada. A disponibilidade está relacionada a muitos outros serviços de segurança. Entretanto, faz sentido existir o termo “serviço de disponibilidade”. Esse serviço endereça preocupações como, por exemplo, os ataques de negação de serviço e, normalmente, depende do serviço de controle de acesso e outros serviços de segurança.

3.3.6 Serviço de integridade dos dados

Esse serviço deve garantir que os dados recebidos são exatamente os enviados por uma entidade autorizada, sem nenhuma modificação, inserção, remoção, ou reenvio da mensagem. São cinco tipos de integridade definidas:

a) Integridade de conexão com recuperação com conexão: integridade dos dados transmitidos e detecção de qualquer modificação, inserção, remoção ou reenvio (*replay*) de qualquer dado em uma seqüência de pacotes, com recuperação;
b) Integridade sem recuperação com conexão: igual à integridade com recuperação, exceto a tentativa de recuperação;
c) Integridade de campo seletivo com conexão: integridade dos dados transmitidos a todos os usuários da conexão de um determinado campo-seletivo dentro dos dados do usuário de um bloco de dados. Determina se um campo seletivo foi modificado, inserido, apagado ou reenviado;

d) Integridade sem conexão: integridade dos dados transmitidos de um único bloco de dados sem conexão e poder detectar a modificação dos dados. De forma limitada, detectar o reenvio da mensagem;
e) Integridade de campo seletivo sem conexão: integridade dos dados transmitidos de um campo seletivo dentro de um único bloco de dados sem conexão e determinar se o campo seletivo foi modificado.

3.3.7 Serviço de irretratabilidade

Fornece proteção contra a negação da identidade por parte de qualquer entidade envolvida em todo ou parte do processo de comunicação. Divide-se em dois o irretratabilidade:

a) Irretratabilidade de origem: o receptor pode provar que a mensagem de fato foi enviada por um determinado emissor;
b) Irretratabilidade de entrega: o emissor pode provar que a mensagem foi de fato recebida por um determinado receptor.

3.4 Mecanismos de Segurança

Shirey (2000) afirma que um mecanismo de segurança é um processo que pode ser utilizado em um sistema para implantar um serviço de segurança. “Alguns exemplos de mecanismos de segurança são: troca de autenticação, *checksum*, assinatura digital, criptografia e preenchimento de tráfego” (SHIREY, 2000, p.153). No Quadro 3 são listados alguns exemplos de mecanismos de segurança, os quais são descritos com mais detalhes logo a seguir.

Classe de Mecanismo	Mecanismos
Criptografia	Chave secreta Chave pública
Assinatura Digital	Assinatura digital
Controle de acesso	Restrição IP
Integridade de dados	*Message Autentication Code*
Autenticação	*Message Autentication Code*

Quadro 3: Exemplos de mecanismos de segurança.

a) Criptografia: uso de algoritmos matemáticos a fim de transformar dados em uma forma não legível. A transformação e a recuperação dependem do algoritmo e de alguma chave criptográfica;
b) Assinatura digital: é a transformação ou adição de uma porção de um dado em uma unidade de dados que permite provar a origem e a integridade pelo receptor;
c) Controle de acesso: uma variedade de mecanismos usados para forçar o direito de acesso em um determinado recurso;
d) Integridade de dados: uma variedade de mecanismos utilizados a fim de garantir a integridade dos dados;
e) Autenticação: um mecanismo para garantir a identidade de uma entidade na troca de informações.

3.5 Ataques

Para a classificação de ataques de segurança são utilizados o termo “ataque passivo” e “ataque ativo”, tanto em SHIREY (2000) quanto no INTERNATION TELECOMMUNICATION UNION (1991) são definidos dessa maneira. Um ataque passivo é a tentativa de obter a informação dos sistemas sem afetar os seus recursos. Um ataque ativo é a tentativa de alterar os recursos dos sistemas ou afetar suas operações (SHIREY, 2000, p.12).

3.5.1 Ataques passivos

Ataque passivo têm como objetivo obter informações através de monitoração e outro mecanismo de escuta na transmissão dos dados. A detecção desse tipo de ataque é difícil, porém, preveni-lo é relativamente simples. Para Stallings (2003), a ênfase está em prevenir esses ataques e não apenas detectá-los, existem dois tipos de ataques passivos:

a) Liberação do conteúdo de mensagem: prevenir a captura das informações na transmissão em algum canal de comunicação de mensagens de correios eletrônicos, de arquivos eletrônicos, conversas telefônicas, entre outros;

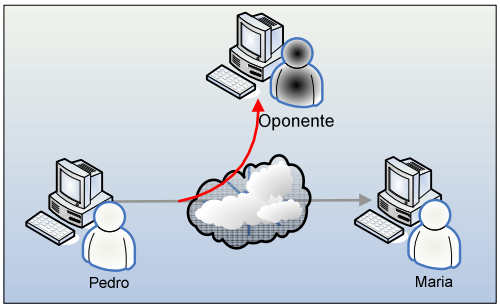

Figura 1. Liberação do conteúdo de mensagem. Adaptação: (STALLINGS, 2003).

b) Análise de tráfego: prevenir a extração das informações dos dados já capturados pelo oponente, uma técnica comum é usar criptografia nos dados de maneira que o oponente não consiga obter a leitura das informações.

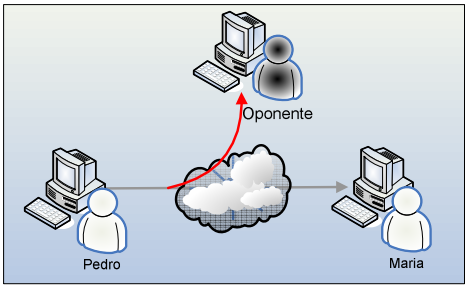

Figura 2. Análise de tráfego. Adaptação: (STALLINGS, 2003).

3.5.2 Ataques ativos

Ataque ativo têm como objetivo modificar ou falsificar, de alguma maneira, os dados transmitidos. São divididos em quatro categorias:

a) Personificação: o objetivo é personificar uma entidade terceira de forma ilegal para assumir seus privilégios;

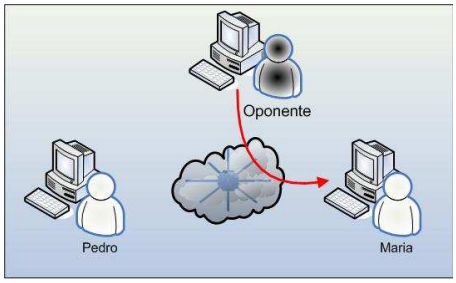

Figura 3. Personificação. Adaptação: (STALLINGS, 2003).

b) Modificação: alterar, atrasar ou reordenar uma mensagem legítima a fim de produzir um efeito não-autorizado;

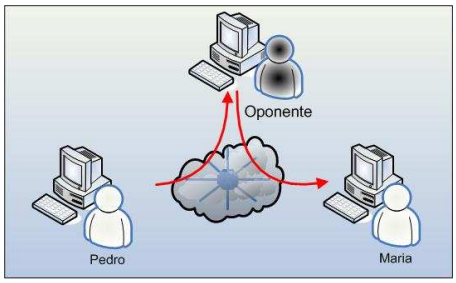

Figura 4. Modificação. Adaptação: (STALLINGS, 2003).

c) Reenvio: envolve uma captura passiva de uma unidade dos dados; posteriormente, é retransmitida de forma a produzir um efeito não-autorizado;

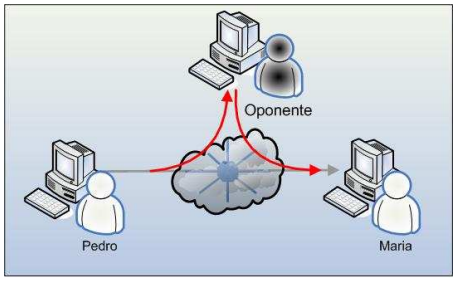

Figura 5. Reenvio. Adaptação: (STALLINGS, 2003).

d) Negação de serviço: causar ruptura ou inabilidade de um uso normal de uma entidade na comunicação dos dados. Também, é possível causar uma indisponibilidade do canal de comunicação ou degradá-lo através de um sobrecarga de mensagens.

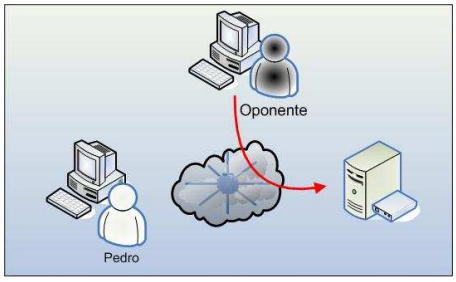

Figura 6. Negação de Serviço. Adaptação: (STALLINGS, 2003).

4 ARQUITETURA DOS PROTOCOLOS DE TEMPO

4.1 NTP Versão 3

4.1.1 Funcionamento

Uma definição importante sobre o comportamento do algoritmo e a arquitetura do NTP é o protocolo buscar a melhor origem da hora a sincronizar. Como afirmado por Deeths (2001a) esta distinção é significante:

> NTP não é baseado no princípio de sincronização entre as máquinas. NTP é baseado no princípio de ter todas as máquinas o mais próximo possível do tempo correto (DEETHS, 2001a, p. 03).

O projeto desse protocolo define três componentes (MILLS, 1992) essenciais relativos ao relógio de referência: diferença de relógio (*clock offset*), latência (*roundtrip delay*) e dispersão (*dispersion)*. A diferença de relógio é o ajuste total para sincronizar o relógio local com o de referência, enquanto latência da mensagem é a capacidade de enviá-la ao destino para chegar dentro de um determinado período. Por fim, a dispersão é quantidade máxima de erros relativos ao relógio de referência.

O conjunto desses três componentes permite o acerto dos relógios locais de todos os computadores o mais próximo da referência escolhida, pois o ajuste do algoritmo prevê a arquitetura de estratos da hierarquia NTP, a latência dos canais de comunicação e as correções de erros relativos à referência.

A hierarquia NTP funciona através de um modelo de estratos conforme Figura 7, a qual poucos servidores fornecem a referência da hora para inúmeros clientes.

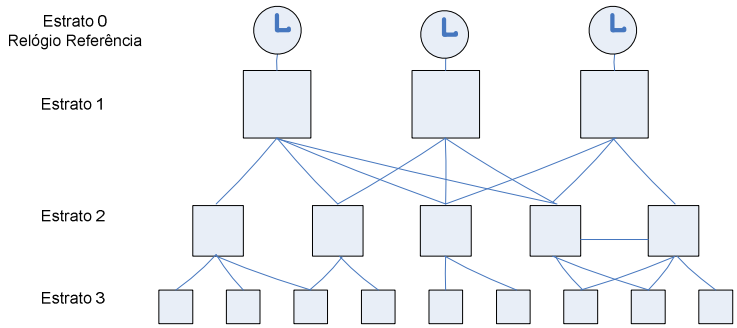

Figura 7: Estratos NTP. Fonte: (RYBACZYK, 2005).

Os servidores do estrato mais baixo, denominado estrato 1, são considerados de alta exatidão, pois estão mais próximos à referência UTC. Esses servidores utilizam receptores GPS, sinais de rádio, *modem* e outros mecanismos de controle de freqüência a fim de manter sua exatidão.

Servidores do estrato 1 podem ser públicos disponíveis na Internet (INTERNET SYSTEMS CONSORTIUM, 2005). Também, é possível configurar um servidor privado como sendo o estrato 1 dentro de uma organização. Atualmente, existem modelos comercias de servidores de tempo com sincronismo através de receptores GPS, rádios entre outros.

“Servidores que se utilizam do estrato 1 como referência, passam a ser referenciado como estrato 2, qualquer servidor que sincroniza sua hora com os servidores do estrato 2 passa a ser o estrato 3, e assim por diante” (REDE NACIONAL DE PESQUISAS, 2000, p. 3). De acordo com Deeths (2001a), o número máximo utilizado por clientes é de 15 estratos, porém, na prática, não ultrapassam os 5.

4.1.2 Campos da mensagem

O NTP é um protocolo da camada de aplicação e suas mensagens são encapsuladas dentro de um datagrama UDP. Os campos de extensão são opcionais e se aplicam somente ao protocolo NTP, versão 4. Também opcionais, os campos de autenticação são para todos os protocolos da família NTP.

A Figura 8 apresenta os campos da mensagem NTP e que são descritos logo a seguir.

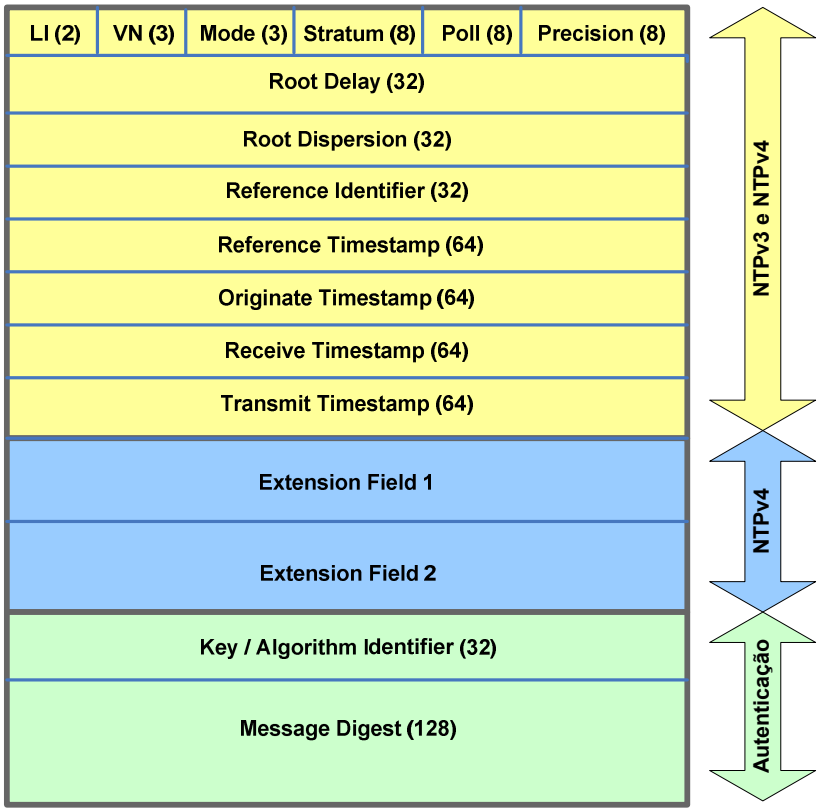

Figura 8: Estrutura da mensagem de dados NTP. Fonte: (MILLS, 2006a).

- Campo *LI*: campo de alerta para que o segundo intercalado seja inserido ou não no último minuto do dia corrente. Esse campo tem relevância apenas nas mensagens do servidor;
- Campo *VN*: campo que indica a versão do protocolo NTP ou SNTP;
- Campo *Mode*: campo que indica o modo de operação do protocolo; como segue na Tabela 1:

Tabela 1. Modos de Operação NTP

Modos de Operação	Descrição
0	Reservado
1	Simétrico Ativo
2	Simétrico Passivo
3	Cliente
4	Servidor
5	*Broadcast*
6	Reservado para mensagem de controle
7	Reservado para uso privado

Fonte: (MILLS, 1992).

Os números entre 1 e 5 representam o modo de operação que existe entre os dispositivos na sincronização de tempo. Os números 6 e 7 são usados pela mensagem de controle conforme Tabela 2.

Tabela 2. Campos da Mensagem de Controle NTP

Código	Descrição
0	Reservado
1	Lê estado do comando/resposta
2	Lê variável do comando/resposta
3	Escreve variável do comando/resposta
4	Lê variável do relógio do comando/resposta
5	Escreve variável do relógio do comando/resposta
6	Configura endereço/porta *trap* do comando/resposta
7	Resposta *Trap*
8 a 31	Reservado

Fonte: (RYBACZYK, 2005).

Mesmo com estruturas diferentes, as mensagens compartilham o campo *Mode* e, no cabeçalho das mensagens, o campo *Mode* fica na mesma posição. Dessa forma, uma mensagem de controle é identificada pelos valores 6 ou 7. Esses controles são utilizados por um comando denominado *restrict*, para parametrizar algumas funcionalidades do serviço NTP em sistemas Unix, detalhadas na seção 4.1.7;

- Campo *stratum*: campo que indica o estrato do servidor. Esse campo tem relevância apenas nas mensagens do servidor;
- Campo *poll*: campo que indica o tempo, em segundos, de intervalo máximo entre as sucessivas mensagens;
- Campo *precision*: campo que indica a precisão do relógio local;
- Campo *root delay*: campo que indica o tempo total de latência, em segundos, do servidor de referência primário. Esse campo tem relevância apenas nas mensagens do servidor;
- Campo *root dispertion*: campo que indica o valor máximo de erro devido à tolerância da freqüência do relógio referência. Esse campo tem relevância apenas nas mensagens do servidor;
- Campo *reference identifier*: campo que indica a origem do relógio de referência. Esse campo tem relevância apenas nas mensagens do servidor;

- Campo *reference timestamp*: campo que indica a última atualização ou correção do tempo do relógio local;
- Campo *originate timestamp*: campo que indica o instante de tempo ao sair do cliente para o servidor no momento da requisição;
- Campo *receive timestamp*: campo que indica o instante de tempo na chegada ao servidor ou da resposta na chegada ao cliente no momento da requisição;
- Campo *transmit timestamp*: campo que indica o instante de tempo ao sair do cliente ou da resposta ao sair do servidor no momento da requisição;
- Campo *extention fields*: campos de uso opcional que possuem requisições e respostas do protocolo *Autokey;*
- Campos de autenticação: campo que indica a existência da opção de autenticação, é subdividido no campo *Key Identifier* e no campo *Message Digest*.

4.1.3 Modos de operação

Segundo Rybaczyk (2005) “um dispositivo NTP assume a nomenclatura de servidor, cliente, hospedeiro ou parceiro dependendo do modo como opera” (RYBACZYK, 2005, p. 64). Um cliente faz requisições, enquanto os servidores respondem aos clientes ou anunciam serviços a eles sem necessariamente ser requisitados. No modo hospedeiro a instância do protocolo é executada localmente. E, no modo parceiro, a instância do protocolo é executada remotamente (MILLS, 1992).

São cinco os modos de operação que formam uma associação e que refletem na natureza da interação entre tais dispositivos, conforme definidos em (RYBACZYK, 2005). Uma associação é formada por dois elementos configurados para trocar mensagens entre si e um deles mantém uma instância do protocolo sendo executada. Abaixo são descritos os modos de operação na ordem do campo *Mode* da mensagem NTP:

1) No modo simétrico ativo, um computador anfitrião periodicamente envia mensagens de sincronia de tempo, independentemente do estado ou estrato de seu par. Nesse modo, o anfitrião anuncia sua intenção de sincronizar e ser

sincronizado pelo par. “Normalmente, esse modo é utilizado por servidores de tempo que operam próximos aos estratos baixos das sub-redes de sincronização” (MILLS, 1992, p. 17). Em um serviço de sincronização de tempo confiável, são configurados dois ou mais servidores de tempo nos estratos mais baixos que os clientes e um servidor de tempo no mesmo estrato;

2) Uma associação no modo chamado “simétrico passivo” é criada ordinariamente no recebimento de uma mensagem com a intenção de sincronizar e ser sincronizado, originada do anfitrião em modo simétrico ativo. Tal associação persiste até que uma mensagem seja enviada na resposta ao seu par. “Porém, na prática, associação no modo passivo em roteadores Cisco persiste até o dispositivo que criou a associação for reiniciado” (RYBACZYK, 2005, p. 68);
3) No modo cliente, normalmente, uma estação de rede local, mensagens periódicas são enviadas com a intenção de ser sincronizada por um servidor, mas nunca sincronizá-lo;
4) No modo servidor, uma associação é estabelecida em resposta às requisições do cliente e existe somente para responder a tais requisições. O dispositivo anuncia sua intenção de oferecer sincronia aos clientes e de nunca ser sincronizado por eles. Nesse modo, associações não são persistentes e não mantém nenhuma informação passada do cliente;
5) No modo *broadcast*, em uma rede local, um servidor envia periodicamente mensagens que anunciam sua intenção de sincronizar todos os clientes e de não ser sincronizado por nenhum deles. Isto é realizado através da transmissão de mensagens de *broadcast* IP. Porém, há maneiras de retransmitir esse tipo de mensagem para outras redes configurando os roteadores.

Adicionalmente, um dispositivo pode ser configurado como primário, através do seu relógio local. Como citado por Rybaczyk (2005):

> Na ausência de um servidor de tempo NTP sincronizado ao UTC através de seu próprio relógio de referência, qualquer dispositivo (roteador, comutador, estação) configurado como um NTP "mestre" pode assumir o papel de servidor estrato 1 e fornecer sincronização relativa de tempo que é tipicamente determinada e configurada manualmente no dispositivo por um administrador de redes. Embora tal configuração forneça sincronização, ela não fornece uma exatidão com o tempo UTC (RYBACZYK, 2005, p. 66).

4.1.4 Serviço de autenticação

No serviço de autenticação do protocolo NTP, versão 3, "cada associação é autenticada com uma chave criptográfica simétrica[8], a qual é armazenada em uma base segura" (MILLS, 1996, p. 6). Originalmente, foi definido na RFC 1305 o algoritmo DES-CBC (*Data Encryption Standard – Cyber Block Chaining*) (FEDERAL INFORMATION PROCESSING STANDARDS, 1980). Mas, adicionalmente, o algoritmo criptográfico MD5 (*Message Digest* 5) (RIVEST, 1992) foi introduzido para criptografar as mensagens de sincronização.

Nas associações ativas, ou seja, simétrico ativo (modo de operação 1), cliente (modo de operação 3) e *broadcast* (modo de operação 5) a chave secreta é determinada pela lista de identificador da chave. Em associações passivas, ou seja, simétrico passivo (modo de operação 2) e servidor (modo de operação 4) a chave é determinada pelo identificador da chave do parceiro conforme descrito por Mills (1992).

No esquema de autenticação, Mills (1996) sustenta a existência de uma lista com as chaves secretas utilizadas para construir um resumo da mensagem em todas as associações. De forma similar ao SPI (*Security Parameter Identifier*) descrito em (KENT; ATKINSON, 1998), cada chave secreta possui um identificador próprio e um identificador do algoritmo usado (MD5 ou DES). Dessa maneira, "se dois parceiros compartilham uma chave, eles devem utilizar o mesmo identificador da chave e do

[8] Na criptografia simétrica a chave utilizada pode ser denominada chave secreta neste trabalho. Igualmente ao livro (STALLINGS, 2003, p. 261).

algoritmo” (MILLS, 1996, p. 6) para criptografar o cabeçalho NTP e o identificador da chave.

Ao enviar a mensagem, a chave secreta é utilizada para construir um resumo da mensagem através de uma função *hash* com o algoritmo MD5 ou DES. O identificador da chave secreta e o resumo da mensagem são armazenados no MAC (*Message Autentication Code*) os quais são transmitidos juntamente com a mensagem conforme Figura 9.

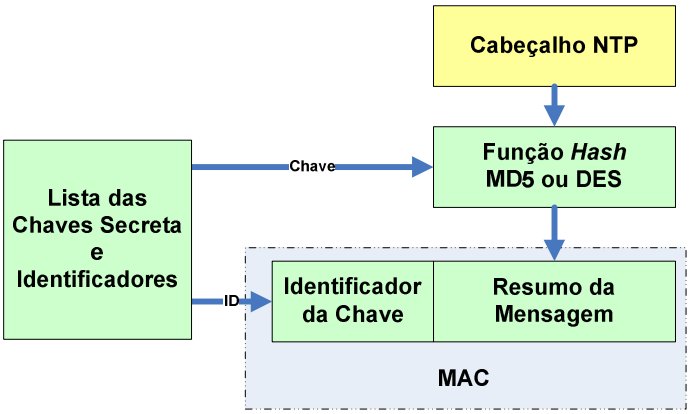

Figura 9: Criptografia da mensagem NTPv3. Adaptação: (MILLS, 2006a).

Mills (1996) descreve que o receptor utiliza o identificador da chave incluído no MAC para recuperar a chave secreta de sua própria base. Computa o resumo da mensagem com o mesmo algoritmo e verifica a autenticidade da mensagem comparando os valores incluídos no MAC conforme Figura 10.

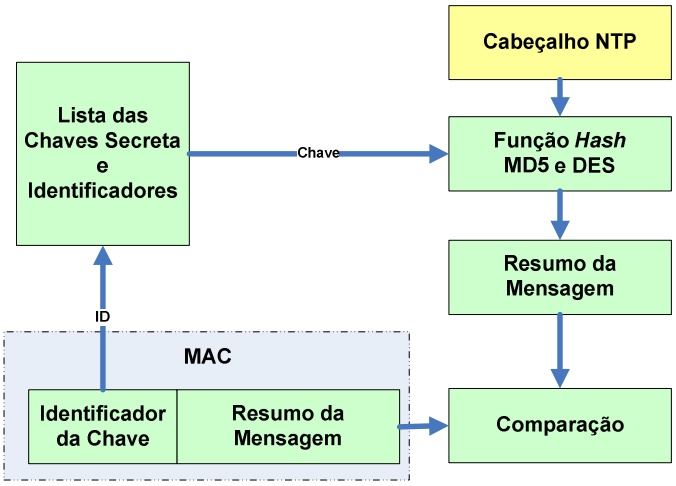

Figura 10: Decriptografia da mensagem NTPv3. Adaptação: (MILLS, 2006a).

O uso de autenticação é um serviço opcional e configurado por cada participante na associação. Quando configurado, o servidor ou o cliente adiciona o código MAC nas mensagens enviadas para os parceiros identificados na associação. Tanto o servidor quanto o cliente podem ter alguns parceiros configurados com autenticação e outros parceiros sem a configuração.

4.1.5 Serviço de confiabilidade

O protocolo NTP fornece uma sincronização confiável utilizando múltiplos servidores redundantes. O algoritmo de tolerância à falhas da família de protocolos NTP prevê a existência de servidor com o relógio inconsistente ou fora de uma amostra de um conjunto de servidores de tempo com o tempo preciso. “Isso é especialmente importante com clientes em modo *broadcast*, pois os servidores podem não ser precisos *a priori*” (MILLS, 2006a, p. 47). Sendo assim, um esquema muito adequado para ambiente de rede local.

Para ter um valor tempo confiável é necessário satisfazer à relação 3*m*+1 de relógios requeridos conforme estudos de Lamport (1978). Sendo *m* o número de relógio inconsistente. Mills (2006a) afirma que “2*m*+1 relógios são requeridos se assinatura digital estiver disponível” (MILLS, 2006a, p. 37), mudando a relação de servidores mínimos necessários.

Dessa maneira, para um serviço de sincronização de tempo robusto e confiável é necessário também relacionar à quantidade de relógios mínimos disponíveis na sincronização de tempo.

4.1.6 Serviço de confidencialidade

O serviço de confidencialidade dos dados não é implementado, Mills (1996) afirma que não é necessário criptografar os campos de carimbo de tempo ou esconder os dados das mensagens NTP, pois são considerados valores públicos.

4.1.7 Serviço de controle de acesso

É utilizado um filtro típico baseado na restrição da associação pelo endereço IP entre os parceiros. Além disso, há comandos específicos para a restrição do “serviço NTP oferecido e requisitado bem como a direção da comunicação” (RYBACZYK, 2005, p. 82), mesmo que a associação seja restrita a alguns parceiros.

Rybaczyk (2005) destaca que a granularidade no controle de acesso muda entre os fornecedores e no tipo de dispositivo a ser implantado pelo NTP. Um exemplo é o “comando *restrict* disponível em uma implantação Unix/Linux” (RYBACZYK, 2005, p. 112) utilizado no controle de acesso de algumas funcionalidades do NTP. Conforme as parametrizações do comando *restrict* são utilizadas as ações das mensagens de controle do protocolo NTP descritas na Tabela 2, na seção 4.1.2.

O Quadro 4 exemplifica um arquivo típico de configuração do NTP, versão 3, com as opções de controle de acesso, detalhados logo abaixo.

Configuração de controle de acesso cliente
#Define a política de acesso padrão restrict default ignore #Configuração de três servidores de tempo para redundância server XXX.XXX.XXX.XXX server YYY.YYY.YYY.YYY server ZZZ.ZZZ.ZZZ.ZZZ #Restringe modificações, parcerias, *queries* e serviço de *trap* aos servidores de tempo restrict XXX.XXX.XXX.XXX nomodify nopeer noquery notrap restrict YYY.YYY.YYY.YYY nomodify nopeer noquery notrap restrict ZZZ.ZZZ.ZZZ.ZZZ nomodify nopeer noquery notrap

Quadro 4. Exemplo de controle de acesso NTPv3. Fonte: (RYBACZYK, 2005).

a) *Default*: palavra usada para definir a política de acesso padrão definida com a utilização do comando *restrict*. Nesse exemplo, os parâmetros serão aplicados em todos os pacotes de entrada, pois não foram especificados um endereço IP e uma máscara de rede. Porém, é permitido que os parâmetros subseqüentes modifiquem a política padrão dependendo das opções utilizadas;
b) Parâmetro *ignore*: com esse parâmetro, o receptor ignora todos os pacotes NTP. Em conjunto com parâmetro *Default,* restringe todos os pacotes de entrada por padrão. Porém, os demais pacotes são permitidos dependendo dos parâmetros subseqüentes. Isso é análogo a regras de *firewall* que negam tudo no início e permitem somente o necessário posteriormente;
c) *Server*: configuração do endereço IP do servidor NTP. Nesse exemplo, são configurados três servidores de tempo por questões de redundância.

Também, restringe esses servidores de desempenhar as ações dos parâmetros configurados pelo comando *restrict*;

d) Parâmetro *nomodify*: com esse parâmetro, o receptor ignora todos os pacotes de controle NTP que tentam modificar o estado do servidor de tempo. Entretanto, se é o único parâmetro utilizado, qualquer servidor com o IP permitido pelo parâmetro *server* pode estabelecer a associação simétrica, desempenhar as requisições e receber as informações de tempo;
e) Parâmetro *nopeer*: fornece a sincronização para os dispositivos que estabelecem a comunicação sem estado de conexão e não permite estabelecer a relação de parceiros com eles. Esse parâmetro previne o dispositivo cliente de associar com os servidores de tempo identificados no comando *restrict* em modo simétrico ativo
f) Parâmetro *noquery*: o receptor com esse parâmetro configurado ignora todos os pacotes de controle NTP que representam *queries* ou comandos requisitados pelos servidores de tempo;
g) Parâmetro *notrap*: o receptor com esse parâmetro configurado ignora todos os pacotes de controle NTP que solicitam o serviço de *trap*;
h) Parâmetro *noserve*: permite pacotes de controle NTP (valores 6 e 7) e ignora os demais pacotes. Esse parâmetro não é usado no exemplo no quadro 3, mas poderia negar o acesso ao serviço de sincronização aos servidores listados no comando *restrict* ou a qualquer outro endereço IP.

4.1.8 Serviço de disponibilidade

O protocolo NTP, versão 3, fornece o serviço de disponibilidade, principalmente, através da configuração de servidores de tempo redundantes prevenindo contra falha ou indisponibilidade de um deles. Do ponto de vista do cliente, isso é possível através de uma configuração explícita no arquivo de configuração do NTP. É possível configurar dois ou mais servidores como referência de tempo. No Quadro 3, por exemplo, o comando *server* explicita três servidores de tempo.

4.1.9 Serviço de integridade

O uso do código MAC, além de permitir a “autenticação criptográfica, é um mecanismo de segurança forte para forçar a integridade dos dados NTP” (RYBACZYK, 2005, p. 82). Quando configurado, garante que seus dispositivos considerem legítimos seus parceiros.

4.1.10 Serviço de irretratabilidade

O protocolo NTP, versão 3, não fornece o serviço de irretratabilidade.

4.2 NTP versão 4

4.2.1 Funcionamento

O protocolo NTP, versão 4, consiste em um conjunto de extensões do NTP, versão 3, (MILLS, 1992), “mas a especificação do protocolo definitiva ainda não está disponível” (MILLS, 2006a, p. 12). Porém, presume-se que “todos os servidores e clientes na Internet estão em conformidade com a versão 3 e os usuários são fortemente encorajados a fazer a atualização para a versão 4” (MILLS, 2006a, p. 12).

4.2.2 Campos da mensagem

Assim como o NTP, versão 3, a mensagem do NTP, versão 4, utiliza o mesmo formato de pacote e os mesmos campos definidos na seção 4.1.2. A diferença está nos campos de extensão. Um ou mais campos de extensão podem ser inseridos logo após o cabeçalho e antes dos campos de autenticação. O protocolo *Autokey* utiliza um campo de extensão para inserir outros parâmetros para a mensagem de requisição e resposta de uso exclusivo dele.

4.2.3 Modos de operação

São três modos de operação descritos em (MILLS, 2006a) tanto para os clientes quanto para os servidores, mudando apenas a origem das requisições de sincronização.

O cliente NTP opera nos modos *unicast*, *broadcast* e *manycast*. No modo *unicast*, o cliente, em modo 3, envia a requisição para um servidor específico e aguarda uma resposta desse servidor em modo 4. No modo *broadcast*, o cliente aguarda por uma mensagem de sincronização no endereçamento de *broadcast* IP de um ou mais servidores em modo 5. No modo *manycast*, o cliente, em modo 3, inicialmente envia uma requisição a um determinado endereço *multicast* e aguarda a resposta de um ou mais servidores em modo 4. O cliente utiliza a primeira resposta recebida de um servidor a fim de estabelecer, subseqüentemente, uma operação *unicast* com ele.

Também, os modos de operação formam associações de três tipos: persistente, preemptiva e efêmera. A associação persistente e preemptiva estão explícitas nos arquivos de configuração e são mobilizadas no início das atividades dos dispositivos participantes da sincronização de tempo. A associação efêmera é mobilizada na recepção da mensagem designada para esse propósito como, por exemplo, no modo *broadcast*.

A associação persistente não é desmobilizada nunca, apesar de ficar inativa quando um servidor associado fica indisponível. Associações preemptiva e efêmera são desmobilizadas depois de algum tempo que o servidor parceiro deixar de responder.

“Associação efêmera sempre deve ser criptograficamente autenticada porque um intruso pode personificar um servidor e injetar valores de tempo falsos” (MILLS, 2006a, p. 22).

4.2.4 Serviço de autenticação

No protocolo NTP, versão 4, há dois esquemas de autenticação disponíveis. O primeiro deles é a autenticação por chave secreta descrita na seção 4.1.4. Esse modelo existe para manter a compatibilidade com a versão 3. E, o segundo esquema é denominado *Autokey*, que possui técnicas de chaves públicas.

O *Autokey* emprega o uso de função *hash*, assinatura digital e algoritmos de chave pública. O algoritmo MD5 (RIVEST, 1992) é utilizado para detectar modificação da mensagem através de um resumo da mensagem (*hash*), o algoritmo RSA (RIVEST; SHAMIR; ADLEMAN, 1978) é usado para verificar a origem da mensagem, utilizando chave pública e privada e o algoritmo Diffie-Hellman gera um valor secreto em certos modos para a troca de chaves. Segundo Mills, “esse esquema tem sido implantado, testado e largamente empregado na Internet nos dias atuais” (MILLS, 2006b, p. 1).

Mills (2006a) descreve uma chave de sessão denominada *autokey* e uma seqüência randômica pré-computada dos *autokeys.* Essa seqüência é identificada e armazenada em uma lista. Cada associação é autenticada pelo protocolo *Autokey* de maneira idêntica à autenticação do NTP, versão 3. Dessa maneira, há diversas seqüências de *autokeys* funcionando de forma independente ao mesmo tempo.

A chave de sessão, ou *autokey,* é computada de quatro campos e, aplicada uma função *hash* pelo algoritmo MD5, produz um valor de 128 bits conforme Figura 11. O valor calculado é armazenado juntamente com o identificador da chave em um *cache* que será usado posteriormente para a decriptografia.

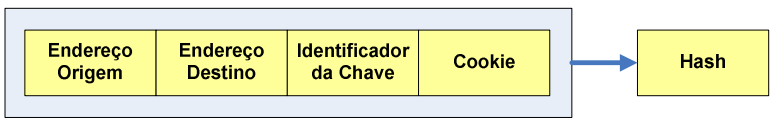

Figura 11: Chave de sessão (Autokey) NTPv4. Fonte: (MILLS, 2006a).

Os campos de endereço origem e destino são tanto no formato IP, versão 4, quanto IP, versão 6. Porém, são campos com 32 bits ou 128 bits respectivamente.

O campo identificador da chave possui 32 bits e é utilizado tanto na criptografia simétrica quanto na assimétrica. Para manter a compatibilidade com NTP, versão 3, o campo é repartido em dois em um ponto pivô 65536. Identificadores de chaves simétricas têm valores menores que o pivô, e tempo de vida indefinida. Identificadores de *autokeys* têm valores randômicos maiores ou iguais ao pivô e são expurgados logo após seu uso.

O campo *cookie* possui 32 bits e tem valores diferentes para cada modo de operação. No modo servidor, o *cookie* é um código *hash* dos endereços de origem e destino e um valor privado. E, no modo *broadcast*, o *cookie* tem um valor público (zero). Ou seja, essas mensagens são sempre assinadas, conforme Figura 12.

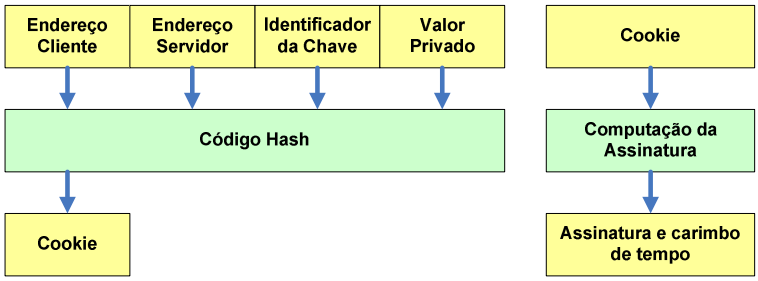

Figura 12: Campo *cookie*. Fonte: (MILLS, 2006a).

“A lista dos identificadores dos *autokeys* consiste em uma seqüência de identificadores de chaves e é iniciada com a primeira chave gerada de uma semente randômica de 32 bits igual ou maior que o pivô” (MILLS, 2006a, p. 156) do campo identificador de chaves.

Conforme Figura 13, o primeiro *autokey* é criado utilizando um determinado *cookie* e o próximo identificador *autokey* é resultado dos primeiros 32 bits na ordem dos *bytes* de rede.

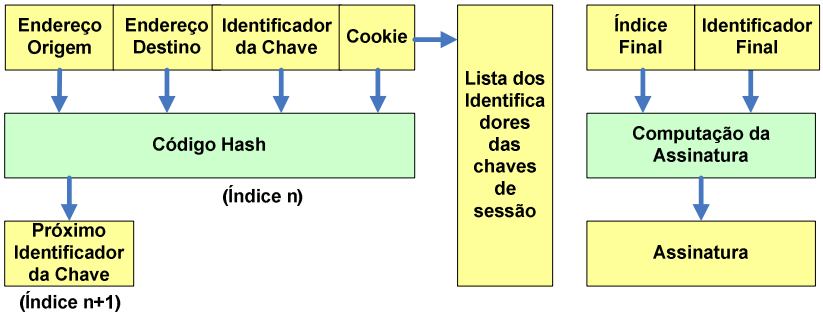

Figura 13: Lista do identificador Autokey. Fonte: (MILLS, 2006a).

A operação continua até gerar a lista completa a qual pode conter mais de cem identificadores. No final, o índice do último identificador na lista é salvo juntamente com o identificador da chave e o conjunto de valores é assinado utilizando um dos algoritmos de assinatura criptográfica.

De forma idêntica ao protocolo NTP, versão 3, o identificador da chave secreta armazenado na lista é usado para construir o resumo da mensagem e ser enviado juntamente com o MAC na mensagem, conforme Figura 14.

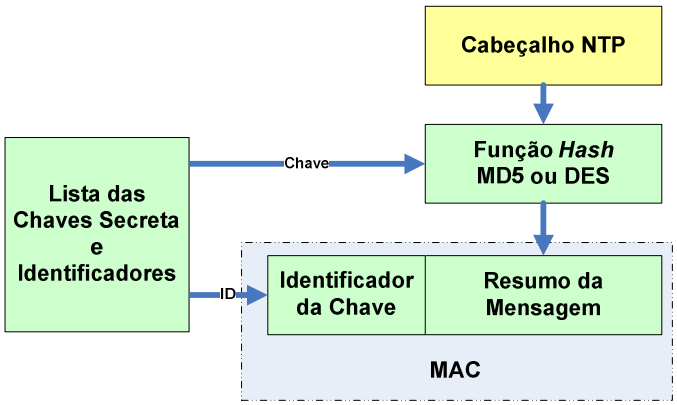

Figura 14: Envio autenticado com Autokey. Fonte: (MILLS, 2006a).

Também, no recebimento da mensagem autenticada, o protocolo NTP, versão 4, trata de forma idêntica a versão 3 do NTP, conforme Figura 15.

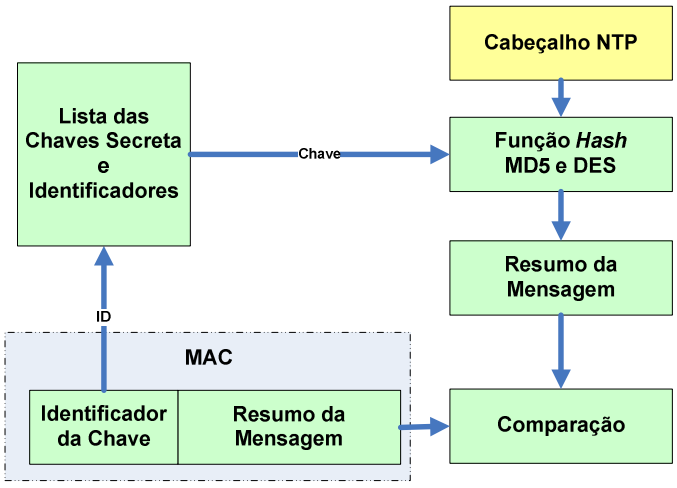

Figura 15: Recepção autenticada com Autokey. Fonte: (MILLS, 2006a).

O receptor utiliza o identificador da chave incluído no MAC para recuperar a chave secreta e verificar a autenticidade da mensagem, computando o resumo da mensagem e comparando com o valor correspondente incluído na mensagem.

Através de requisições e resposta o cliente obtém valores criptográficos e, dessa forma, confirma a identidade do servidor. Segundo Mills (2006a), nas variações de funcionamento o servidor e o cliente concordam com o nome do servidor, esquema de assinatura e de função *hash* e com o esquema de identidade na troca dos parâmetros. Também, o cliente obtém o *cookie* e o valor *autokey* dependendo do funcionamento. E, finalmente, o cliente apresenta seu certificado auto-assinado para o servidor para assinatura na troca de mensagens assinadas.

4.2.5 Serviço de confiabilidade

De maneira idêntica ao protocolo NTP, versão 3, descrito na seção 4.1.5.

4.2.6 Serviço de Confidencialidade

Idêntico ao protocolo NTP, versão 3, o serviço de confidencialidade não é necessário, pois são considerados valores públicos os campos de carimbo de tempo e os dados das mensagens NTP. “Os únicos dados criptografados enviados pela rede são assinaturas digitais e *cookies*. O pacote NTP, incluindo o conteúdo inteiro do cabeçalho e dos campos de extensão, não é criptografado nunca” (MILLS, 2006a, p. 147)

4.2.7 Serviço de controle de acesso

De forma idêntica ao protocolo NTP, versão 3, o controle de acesso da versão 4 é baseado em uma lista de restrição do endereço e máscara IP. A lista possui os valores a restringir o acesso através da comparação dos endereços origem dos pacotes. Caso ocorra a igualdade dos endereços, o pacote é permitido.

Ainda, há dois comandos que são utilizados para restrição de pacotes. O comando *Discard* e o *Restrict*, que protegem o servidor de abuso do cliente.

O comando *Discard* possui parâmetros para restringir o acesso do cliente através de quantidades mínimas e médias entre os pacotes que chegam ao servidor.

O comando *Restrict* possui parâmetros para restringir determinado endereço IP. Alguns parâmetros foram descritos na seção 4.1.7 sobre o controle de acesso NTP, versão 3. Outros parâmetros adicionais são descritos a seguir:

a) *Kod*: pacote *kod* é enviado quando uma violação de acesso ocorre;
b) *Limited*: nega o serviço se os pacotes violarem os limites mínimos especificados no comando *discard;*
c) *Lowpriotrap*: modifica a prioridade de *traps* normais assinaladas pelo algoritmo para baixa prioridade;
d) *Notrust*: nega os pacotes normais. A exceção são os pacotes criptografados e autenticados;
e) *Ntpport:* restringe o pacote à porta UDP 123;
f) *Version*: nega os pacotes NTP que não são da versão atual.

Mills (2006a) ressalta que o controle de acesso pode ser útil para manter a integridade do servidor de cliente indesejado ou malicioso. Porém, não deve ser considerada uma alternativa à autenticação. Pois, restrição baseada em endereço de origem é facilmente evitada por determinada ameaça.

4.2.8 Serviço de disponibilidade

Além do mesmo serviço de disponibilidade do NTP, versão 3, com configurações de servidores redundantes, o NTP, versão 4, tem um novo formato de pacote para evitar o envio de pacotes de clientes indefinidamente.

É possível que um cliente envie pacotes de negação de serviço por um tempo indefinido e, mesmo utilizando parâmetros de restrição, o servidor fique

sobrecarregado. Quando o acesso é negado indefinidamente à única maneira de remover a restrição é reiniciar o servidor. Porém, na especificação do protocolo NTP, versão 4, há um novo formato de pacote para restringir o acesso de clientes, além de requisitar explicitamente que o cliente pare de enviar os pacotes. Esse novo formato é denominado pacote *Kiss-of-Death* e será descrito na sessão 4.2.10.

4.2.9 Serviço de integridade

Igualmente ao NTP, versão 3, esse serviço pode ser garantido com o uso de MAC. Porém, a integridade será mantida enquanto a chave secreta não for revelada.

Também, através do protocolo *Autokey*, é possível garantir a integridade das mensagens de sincronização e a distribuição das chaves privadas de forma segura. Mills (2006a) afirma que:

> O que faz o protocolo *Autokey* especial é a maneira o qual esse algoritmo é usado para desviar ataques de intrusos enquanto mantém a integridade e a exatidão da função de sincronização de tempo (MILLS, 2006a, p. 154).

O *Autokey* é assegurado somente quando a identidade do servidor é confirmada, a assinatura verificada e os valores de tempo obtidos. Mas, “diferentemente do modelo *shell* seguro (ssh), através do qual o cliente deve se autenticar ao servidor, somente o servidor NTP se autentica ao cliente de forma segura” (MILLS, 2006a, p. 149).

4.2.10 Pacote *kiss-o’-death*

Nos pacotes dos protocolos NTP, versão 4, e SNTP existem um campo denominado *Stratum Field.* Nesse campo, quando o valor for zero, não existe funcionalidade associada. Nesse caso, é possível que o servidor utilize esse campo e retorne respostas com o valor zero, informando aos clientes a não enviar pacotes que violem o controle de acesso. Esses pacotes são chamados *Kiss-o’-Death* (KoD).

Com o valor zero no campo *Stratum Field,* outro campo denominado *Reference Identifier* é utilizado para fornecer informações úteis chamadas *kiss code*. O Quadro 5 lista os códigos *kiss code*.

Código	Significado
ACST	Associação que pertence ao servidor *anycast*
AUTH	Falha na autenticação do servidor
AUTO	Falha na seqüência *Autokey*
BCST	Associação que pertence ao servidor *broadcast*
CRYP	Falha na Identificação ou autenticação criptográfica
DENY	Acesso negado pelo servidor remoto
DROP	Perda do parceiro em modo simétrico
RSTR	Acesso negado devido política local
INIT	Associação ainda não sincronizada pela primeira vez
MCST	Associação que pertence ao servidor *multicast*
NKEY	Nenhuma chave encontrada. A chave nunca foi instalada ou não é confiável
RATE	Taxa excedida. O servidor negou acesso temporariamente por que o cliente excedeu a taxa gatilho
RMOT	Alguém está tentando associar de um computador remoto com ntpdc. Nada a se preocupar a menos que a chaves tenham sido roubadas
STEP	Ocorreu uma mudança de fase no sistema de tempo, mas a associação ainda não foi sincronizada

Quadro 5. Códigos *Kiss Code*. Fonte: (MILLS, 2006c).

4.2.11 Serviço de irretratabilidade

O modelo de identificação é baseado em grupos de segurança que consistem de membros que compartilham uma chave secreta. Normalmente, gerada por uma autoridade confiável no estrato 1 da hierarquia NTP. A autoridade confiável gera uma identidade pública e outra privada e distribui o valor selecionado aos membros do grupo através de um meio seguro.

Mills (2006a) descreve que no protocolo NTP, versão 4, há cinco esquemas de identidade: PC (*Private Certificate*), TC (*Trusted Certificate*), IFF (*Identify Friendly or Foe*), GQ (*Modified Guillou-Quaisquater algorithm*) e MV (*Modified Mu-Varadhajan algorithm*). As modificações de alguns algoritmos “são necessárias para que cada esquema funcione com o protocolo *Autokey”* (MILLS, 2006a, p. 163).

O esquema PC gera um certificado privado e utiliza como sendo a chave secreta do grupo. O certificado é distribuído aos membros do grupo através de um meio seguro e nunca é revelado, conforme Figura 16. De acordo com Mills (2006b) esse esquema é robusto enquanto o certificado é protegido. Entretanto, ele pode ser ineficaz quando renovar as chaves ou o certificado. Pois, em um grupo com um número grande de participantes os novos valores devem ser distribuídos e ativados simultaneamente. “É o único esquema funcional no modo *broadcast* NTP” (MILLS, 2006a, p. 165).

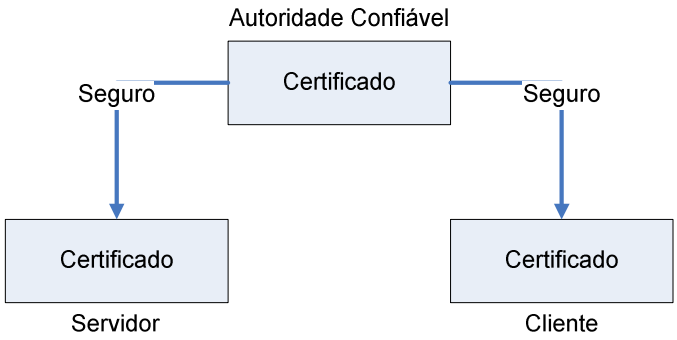

Figura 16: Esquema de identidade PC. Fonte: (MILLS, 2006a).

O esquema TC é a configuração padrão quando não é especificado no parâmetro de troca do *Autokey*. Igualmente nos demais esquemas, cada certificado é assinado por um emissor anterior ao membro confiável o qual tem um certificado auto-assinado. Através do protocolo *Autokey* um membro obtém o certificado de todos os outros ao longo da cadeia iniciada pela autoridade confiável, conforme Figura 17. “Nesse esquema as chaves e os certificados podem ser renovados a qualquer momento, mas uma vulnerabilidade de personificação permanece, a menos que uma requisição para assinar um certificado de cliente seja validada por outros meio como, por exemplo, DNS reverso” (MILLS, 2006a, p. 166).

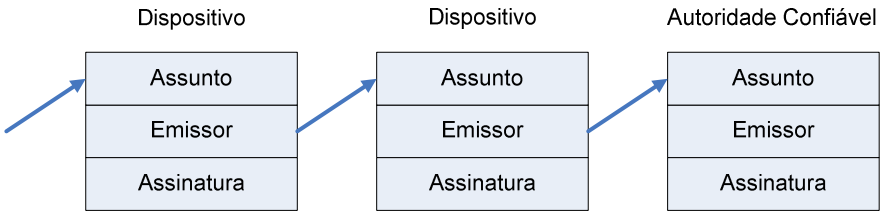

Figura 17: Esquema de identidade TC. Fonte: (MILLS, 2006a).

Os três esquemas IFF, GQ e MV envolvem uma criptografia forte através de trocas de desafio e resposta. Isto dificulta um intruso de descobrir a chave do grupo. Além

disso, nos esquemas IFF e MV, o cliente não conhece o valor da chave do grupo. Porém, no IFF são criados parâmetros que persistem durante a existência do esquema, uma nova geração desses parâmetros devem ser transmitidos de maneira segura a todos os membros antes de serem utilizados. A Figura 18 apresenta a troca de identidade dos esquemas iniciado pelo cliente.

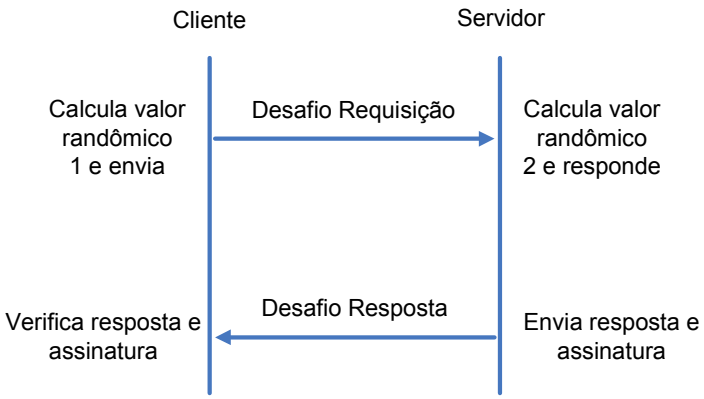

Figura 18: Troca de identidade. Fonte: (MILLS, 2006a).

Mills (2006a) afirma que o esquema IFF “é projetado para os servidores de tempo operados pelo USNO, NIST e outras autoridades”. Também, é útil quando os certificados são gerados por uma entidade terceira como, por exemplo, rotinas OpenSSL ou uma autoridade comercial confiável.

A Figura 19 apresenta o funcionamento do esquema IFF.

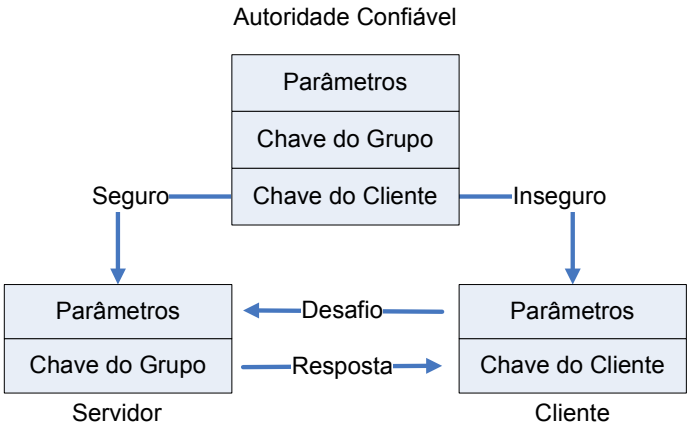

Figura 19: Esquema de identidade IFF. Fonte: (MILLS, 2006a).

“De outra maneira, quando os certificados são gerados pelas rotinas da distribuição do NTP o esquema GQ pode ser uma melhor escolha” (MILLS, 2006b, p. 12). Nesse

esquema o servidor ofusca os parâmetros e a chave secreta do grupo a cada renovação do certificado, conforme Figura 20. Mas, ainda, possui a fragilidade da chave ser conhecida por todos os membros e pode comprometer o grupo todo se divulgada.

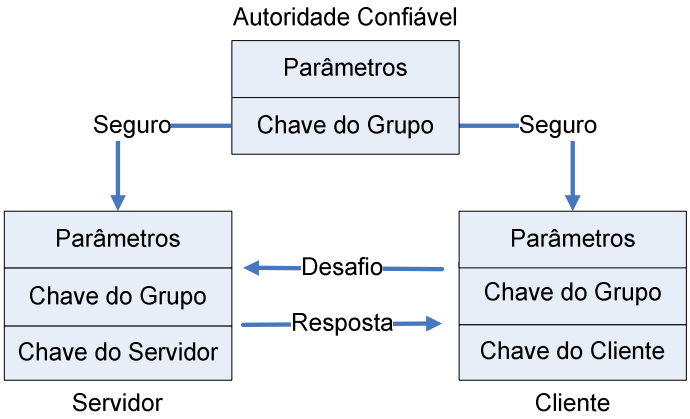

Figura 20: Esquema de identidade GQ. Fonte: (MILLS, 2006a).

O esquema MV pode ser utilizado “quando um número reduzido de servidores fornece sincronização a uma população enorme de clientes” declara Mills (2006a, p. 170). E, onde pode haver um risco de comprometimento entre os servidores e clientes. Originalmente desenvolvido para criptografar a transmissão em modo *broadcast* onde os receptores não transmitem dados. Há uma chave de criptografia do transmissor e outra chave de decriptografia do receptor conforme apresentado na Figura 21.

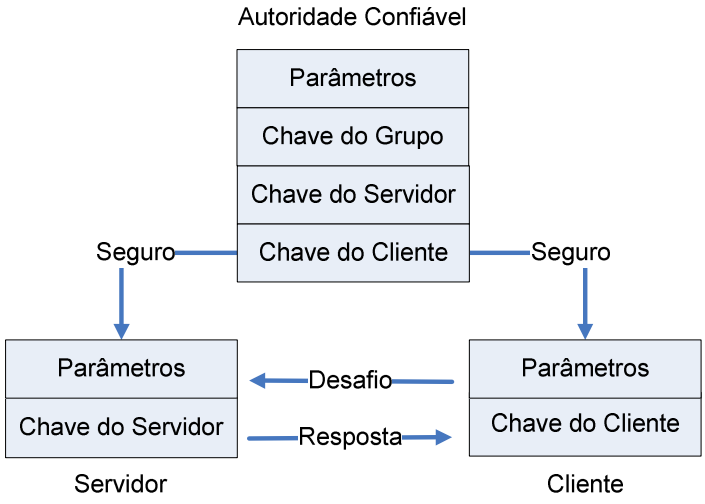

Figura 21: Esquema de identidade MV. Fonte: (MILLS, 2006a).

É possível que um membro participe de mais de um esquema de identidade, porém apenas um é selecionado na troca dos parâmetros. A ordem de escolha é do esquema mais seguro ao menos seguro, ou seja, GC, IFF e TC. O esquema PC não opera com nenhum outro.

A combinação de autenticação (chave secreta ou *autokey*), assinatura e esquema de identidade (PC, TC, IFF, CQ e MV) é denominada *cryptotype* por Mills (2006b) embora nem todas as combinações sejam possíveis. Uma *cryptotype* pode operar com sucesso entre si, mas nem sempre representa uma boa prática de segurança (MILLS, 2006b, p. 55). A *cryptotype* de uma associação é determinada no momento da mobilização, ou na configuração ou algum tempo depois que o pacote apropriado chegar ao receptor. Um servidor responde a qualquer cliente que combinar com sua *cryptotype.* Dessa maneira, um servidor que recebe uma mensagem não autenticada responderá com outra mensagem não autenticada. O mesmo servidor que receber uma mensagem com uma determinada *cryptotype* responderá com outra mensagem no mesmo modelo. Entretanto, associações em modo *broadcast*, *manycast* ou simétrico passivo não mobilizarão a menos que o servidor suporte uma *cryptotype* compatível com a primeira mensagem recebida.

4.3 SNTP versão 4

4.3.1 Funcionamento

O SNTP, versão 4 (MILLS, 2006c), meramente denominado SNTP neste trabalho, é uma simplificação do acesso aos servidores e clientes, usando as versões anteriores do NTP (MILLS, 1992) e do SNTP (MILLS, 1996). Além disso, “o acesso é idêntico ao paradigma UDP/*Time*. De fato, é possível adaptar facilmente uma implantação desse protocolo, utilizando o SNTP” (MILLS, 2006c, p. 02). O protocolo SNTP foi projetado para operar em uma configuração com um servidor dedicado. incluindo um relógio de rádio integrado.

A única mudança significativa do protocolo da versão anterior é a modificação da interpretação do cabeçalho a fim de acomodar a versão do protocolo IP, versão 6. “Também, o SNTP inclui extensões opcionais, como o modo de operação *manycast* e um esquema de autenticação baseado em chaves públicas projetado especificamente para aplicações no modo *broadcast* e *manycast*” (MILLS, 2006c, p. 2). Entretanto, o modo de operação *manycast* e a autenticação devem ser considerados provisórios (MILLS, 2006c). A nova versão do SNTP introduz também uma mensagem denominada *kiss-o’-death*, a qual pode ser utilizada pelos servidores para possibilitar a suspensão das requisições de clientes.

Servidores SNTP não mantém um estado de conexão e suportam um enorme número de clientes. Entretanto, diferentemente da maioria dos clientes NTP, os clientes SNTP normalmente operam somente com um servidor de tempo por vez.

Segundo Mills (2006c), é recomendado que servidores de tempo SNTP operem somente no estrato 1 das sub-redes e que eles sejam configurados somente com origem de sincronização através de uma fonte confiável como relógio de radiofreqüência. É altamente recomendado que clientes SNTP sejam configurados nos estratos mais altos da sincronização.

4.3.2 Campos da mensagem

Assim como o NTP, a mensagem do SNTP utiliza o mesmo formato de pacote e os mesmos campos definidos na seção 4.1.2. Exceto os campos de extensão somente válidos para o NTP, versão 4.

4.3.3 Modos de operação

De forma idêntica aos modos de operação do NTP, versão 4, (MILLS, 2006c), descrito na seção 4.2.3, o SNTP opera nos modos *unicast*, *broadcast* e *manycast*. Porém, servidores NTP podem assumir o modo simétrico que não está disponível no SNTP.

4.3.4 Serviço de autenticação

No protocolo SNTP o serviço de autenticação é idêntico ao descrito anteriormente sobre autenticação por chave secreta na seção 4.1.4 e o esquema com o protocolo *Autokey* descrito na seção 4.2.4.

4.3.5 Serviço de confiabilidade

De forma idêntica ao NTP, versão 3, descrito na seção 4.1.5.

4.3.6 Serviço de confidencialidade

Idêntico aos protocolos NTP, versão 3, e NTP, versão 4, o serviço de confidencialidade não é necessário.

4.3.7 Serviço de controle de acesso

Igualmente aos protocolos NTP, versão 3 e versão 4, o controle de acesso é baseado em uma lista de restrição com o endereço e máscara IP.

4.3.8 Serviço de disponibilidade

O SNTP não possui o modo de operação simétrico, dessa forma, não há servidores de tempo operando em grupo. Porém, é possível a existência de dois ou mais servidores operando de forma independente fornecendo assim duas ou mais referências de tempo. Além disso, o pacote *Kiss-of-Death* descrito na seção 4.2.10 é uma alternativa para impedir sobrecarga do servidor por excesso de requisições.

4.3.9 Serviço de integridade

Esse serviço é garantido com o esquema de MAC ou com o esquema de chave assimétrica através de ou do protocolo *Autokey.*

4.3.10 Serviço de irretratabilidade

De forma idêntica ao NTP, versão 4, descrito na seção 4.2.11.

4.4 IEEE1588 - PTP

4.4.1 Funcionamento

O protocolo PTP (EIDSON; FISHER; WHITE, 2002) possui um algoritmo que estabelece automaticamente uma relação mestre-escravo entre os relógios dos dispositivos conectados à sub-rede. O dispositivo mestre é selecionado quando tem a melhor exatidão e rastreabilidade à referência UTC. Baseado no princípio de estrato, normalmente, é aquele que está no estrato mais perto da referência UTC. Posteriormente, os escravos sincronizam seus relógios locais com seus mestres trocando mensagens conforme ilustrado na Figura 22.

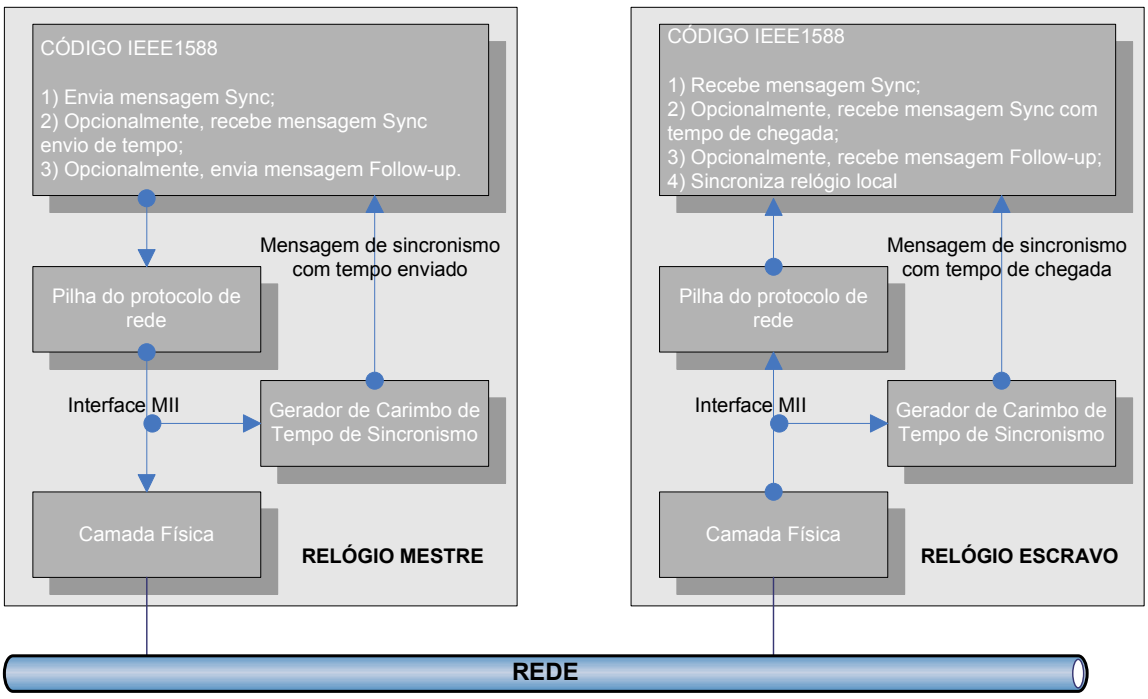

Figura 22. Sincronização IEEE1588. Fonte: (EIDSON; FISHER; WHITE, 2002).

Periodicamente, o relógio mestre envia uma mensagem de sincronismo (mensagem *sync*) para os escravos através de comunicação *multicast*. Essa mensagem de

sincronismo possui uma instância de tempo de quando foi colocada na rede. No dispositivo escravo, essa mensagem é recebida e, imediatamente, sincroniza seu o relógio.

Opcionalmente, em uma rede *Ethernet*, pode existir um detector na interface independentemente do meio (MII – *Medium Independent Interface*) onde o mestre carimba o instante de tempo enviado, baseado em seu relógio local. Isso evita as flutuações temporais nas camadas adjacentes da pilha do protocolo TCP/IP.

Se o mestre e o escravo são equipados dessa forma, o carimbo de tempo é enviado ao escravo pela mensagem de acompanhamento (*follow_up message)*. O escravo recebe a mensagem de sincronismo e carimba o instante de tempo de chegada, logo na interface MII. Com os instantes de tempos da mensagem de sincronismo e da mensagem de acompanhamento, é feita a correção dos relógios dos dispositivos escravos (EIDSON; FISHER; WHITE, 2002).

Também, é usada a informação do caminho percorrido de ida e volta para computar a latência. Assume-se, assim, que o caminho percorrido seja simétrico. O escravo utiliza esta latência medida na correção de seu relógio local. Esse procedimento corrige as flutuações de tempo dos relógios dos dispositivos participantes e a latência existente na rede de comunicação. Flutuações introduzidas pelos dispositivos de redes também causam erros de tempo influenciados pela latência de comunicação. Roteadores introduzem flutuações muito grandes e inconsistentes, principalmente, no ambiente *Ethernet.* Reduzindo a exatidão de tempo.

O padrão IEEE 1588 especifica um mecanismo de transferência padrão, denominado “relógio de borda” (*boundary clock*) a fim de eliminar tais flutuações na comunicação do protocolo PTP. O relógio de borda é fornecido em cada dispositivo de ponta em cada sub-rede. Tais dispositivos utilizam um relógio local que age como um mestre para as sub-redes. De qualquer maneira, a utilização dos relógios de borda forma uma hierarquia na qual é eleito um único relógio de referência, que serve como origem primária de tempo, podendo ou não ser sincronizado com uma origem de tempo UTC.

4.4.2 Campos da mensagem

No padrão IEEE1588, ainda não foram definidos os campos das mensagens do protocolo PTP. A versão 2 da especificação é aguardada no segundo semestre de 2007.

4.4.3 Modo de operação

O protocolo PTP é baseado na comunicação *multicast* IP e, até o momento, os estudos se restringem à rede *Ethernet*. Um servidor mestre pode servir inúmeros escravos com um único par de mensagens de sincronismo e de acompanhamento. Além disso, comunicação *multicast* oferece uma vantagem na administração mais simplificada. Não há necessidade de administração do endereçamento IP em cada dispositivo escravo. Também, por esta razão, as mensagens de gerenciamento desse padrão utilizam o endereçamento *multicast*.

O PTP é um protocolo da camada de aplicação e opera sobre o protocolo de transporte UDP. Ele utiliza a porta 319 nas mensagens com o carimbo de tempo, ou seja, mensagem de sincronismo e mensagem de requisição de atraso. Todas as outras mensagens utilizam a porta 320.

A precisão da sincronização desse protocolo depende da latência da comunicação de rede. Linhas de comunicação ponto-a-ponto entre o mestre e o escravo oferecem precisão mais alta. Mas, dispositivos de rede como, por exemplo, repetidores impõem perdas entre 300 e 400 nanossegundos. Comutadores podem produzir um processamento a mais na comutação de pacotes, tipicamente na ordem de 10 microssegundos, com uma carga muito baixa da comunicação de rede.

Dessa forma, o padrão IEEE1588 define um modelo chamado relógios de borda disponíveis em comutadores específicos. Esse comutador sincroniza-se com o relógio mestre e, posteriormente, atua como um relógio na borda da sub-rede para os demais escravos conectados a ele, atuando como um mestre a esses

dispositivos. Com isso, toda latência do comutador é compensada e não afeta a precisão do sincronismo.

4.4.4 Serviços de segurança

Ainda não estão definidos os serviços de segurança do protocolo PTP (KONSTANTIN; TSANG, 2006) por não ter a especificação definitiva.

Porém, uma análise de segurança apresentado por Konstantin e Tsang (2006) sugere que o protocolo PTP é carente em garantir a integridade da mensagem transmitida e validar a autenticidade do remetente, falhando contra ameaças de modificação, personificação, atraso, reenvio e negação de serviço.

Esta análise é sugestiva para que o padrão considere os serviços de segurança que são essenciais para um serviço de sincronização de tempo robusto.

5 PRINCIPAIS CENÁRIOS DE SINCRONIZAÇÃO DE TEMPO

Há cuidados peculiares que devem ser considerados na distribuição de tempo e, conseqüentemente, refletem nos ambientes de sincronização de tempo. Conforme já afirmado por Mills:

> A ciência de construir as configurações do NTP, mesmo para uma grande corporação com diversas conexões internacionais, não é mais difícil que qualquer outro serviço baseado em sub-redes, como serviço de *email* e de DNS, mas há alguns cuidados peculiares na distribuição de tempo. (MILLS, 2006a, p. 77).

Mills (2006a) descreve que há projetos que consideram a melhor exatidão possível, utilizando quaisquer meios necessários. Outros consideram a melhor resiliência para falhas indesejáveis, sejam elas intencionais ou não. E, há projetos que necessitam de um serviço menos intrusivo nas redes de comunicação e na infra-estrutura de servidores. Para Rybaczyk (2005), o projeto e a implantação é um processo que envolve quatro passos-chave:

a) Escolher o relógio de referência UTC;
b) Decidir a topologia NTP;
c) Determinar as funcionalidades NTP;
d) Monitorar e gerenciar as operações NTP.

Mesmo sendo passos de um processo definido para a família de protocolos NTP, pode ser utilizado como referência em serviço de sincronização de tempo que utiliza outros protocolos de tempo.

Um cenário de sincronização de tempo deve considerar o ambiente de rede e a configuração do serviço de sincronização de tempo. Um ambiente de rede tem suas características de comunicação como vazão, taxa de erro e disponibilidade, que são fortemente influenciadas pelos protocolos e suas configurações. Cada configuração do serviço de sincronização reflete um modo de operação típico relevante para a instalação desse serviço em um ambiente de rede. Dessa maneira, a composição dos cenários é um fator relevante na análise de riscos no final deste trabalho.

5.1 Modelos de Sincronização de Tempo

Um típico modelo de sincronização de tempo inclui relógios de referência UTC, servidores primários, servidores departamentais, servidores controladores de domínio, estações de trabalho e computadores pessoais. Possivelmente, um equipamento do núcleo da rede pode também estar envolvido. Conforme descrito por Mills (2006a) pode ser considerada uma regra geral:

> Como regra geral, roteadores centrais corporativos ou de universidades não sincronizam a relógios de referência; geralmente sincronizam com servidores primários e, possivelmente, com outros roteadores como redundância. Dessa forma, operam no estrato 2. Servidores departamentais e controladores de domínio operam no estrato 3 ordinariamente. Estações de trabalho e computadores pessoais operam no estrato 4 ordinariamente, usando os modos *unicast* ou *broadcast* (MILLS, 2006a, p. 82).

Nesse modelo, Mills (2006a) descreve o serviço de sincronização de tempo com um relógio de referência com o objetivo de manter a rastreabilidade com o UTC. Mas isso não é um requisito obrigatório a todos os participantes de uma arquitetura de distribuição de tempo. Há aqueles que não necessitam de tal sincronização e adotam uma referência de tempo local.

São descritos três modelos principais de sincronização de tempo:

a) Modelo de sincronização de tempo com referência UTC;
b) Modelo de sincronização de tempo sem referência UTC e sem resiliência;
c) Modelo de sincronização de tempo sem referência UTC e com resiliência.

Cada modelo de sincronização possui configurações típicas para a dissiminação de tempo. Tais configurações são apresentadas pelas letras X, Y, W, Z e K inseridas em cada modelo descritos a seguir:

5.1.1 Modelo de sincronização de tempo com referência UTC

Esse modelo exige a sincronização de tempo com um relógio de referência UTC. Isso é realizado através de um servidor denominado primário. Normalmente, existem duas alternativas na escolha desse servidor. A primeira alternativa utiliza uma comunicação sobre uma rede pública e a segunda, uma rede privada. Uma vez realizada a comunicação entre o relógio de referência UTC e o servidor primário, há a distribuição da informação de tempo para os demais participantes através de um servidor secundário dentro da rede interna. O servidor primário no estrato 1 pode ser um servidor localizado na Internet ou um servidor privado com a função de manter o sincronismo com alguma referência UTC, conforme Figura 23.

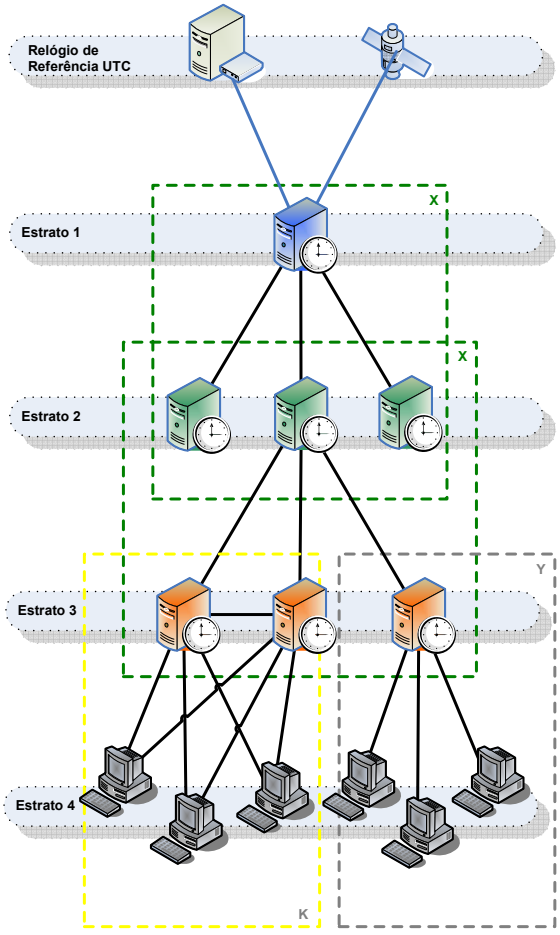

Figura 23. Sincronização de tempo com um relógio de referência UTC.

A distribuição para dos demais participantes ocorre de maneira hierárquica, na qual os números maiores dos estrato representam maior latência à referência UTC,e, conseqüentemente, menor exatidão.

5.1.2 Modelo de sincronização de tempo sem referência UTC e sem resiliência

Esse modelo apresenta um servidor de tempo primário localizado na rede local sem necessidade de sincronização com um relógio de referência UTC conforme Figura 24. Esse equipamento deve possuir um relógio local preciso suficiente para manter a distribuição de tempo. É provável que, nesse servidor, seja necessário o ajuste de seu relógio local com alguma periodicidade. Pois, o mecanismo que mantém sua freqüência não é perfeito e, conseqüentemente, a precisão é afetada. Há equipamentos dedicados extremamente precisos que têm em sua construção um relógio muito estável, porém, com um custo muito alto.

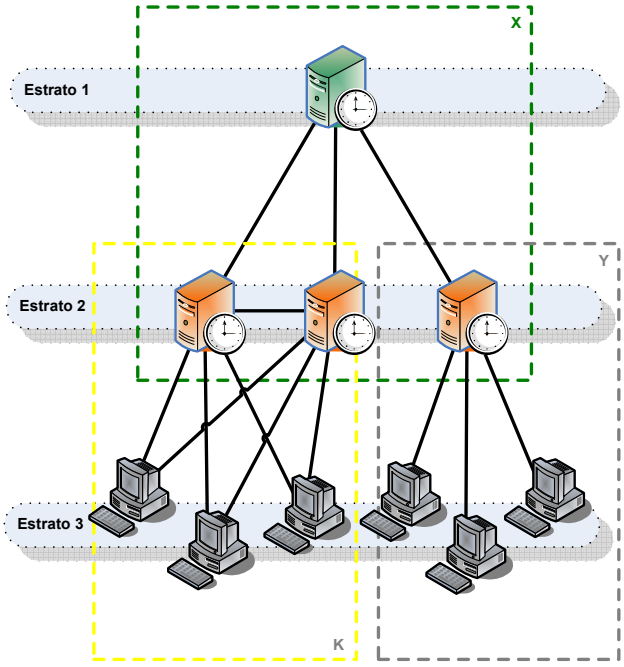

Figura 24. Sincronização com um servidor dedicado sem referência UTC.

5.1.3 Modelo de sincronização de tempo sem referência UTC com resiliência

Esse modelo também apresenta um servidor de tempo primário localizado na rede interna sem necessidade de sincronização com um relógio de referência UTC. Porém, é considerada uma configuração com servidores primários e secundários redundantes entre si a fim de atender à resiliência do serviço de distribuição de tempo, conforme estrato 1 e 2 da Figura 25. Além disso, os clientes participantes consideram os servidores redundantes para uma maior disponibilidade do serviço de acordo com a Figura 25.

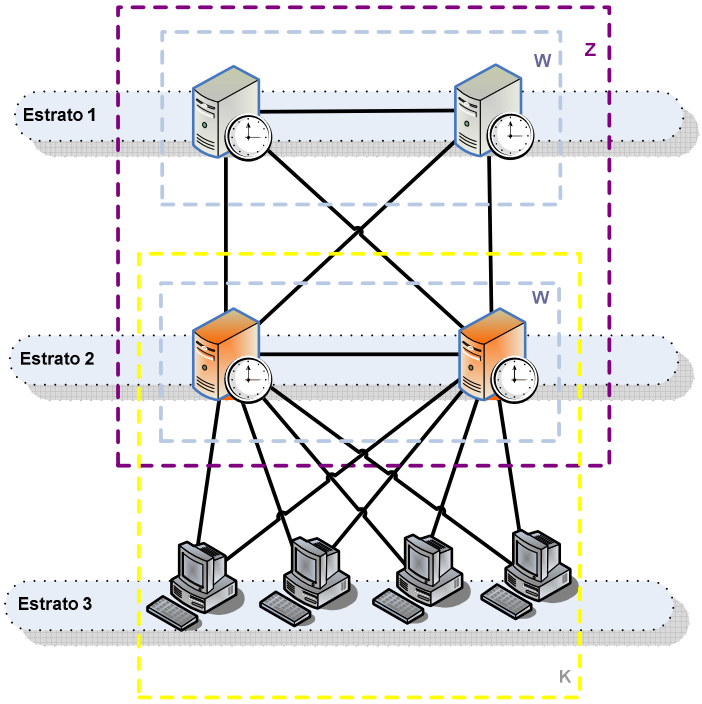

Figura 25. Sincronização considerando resiliência do serviço.

5.2 Configurações de Sincronização de Tempo

O projeto de um serviço de sincronização de tempo deve considerar o uso correto dos modos de operação, com o objetivo de obter a melhor distribuição de tempo, ou seja, todos os relógios devem estar o mais próximo da referência utilizada, seja local ou UTC. As configurações X, Y, W, Z e K são partes dos três modelos anteriores e são detalhadas a seguir:

5.2.1 Sincronização de tempo entre servidores (X)

Há uma configuração denominada cliente/servidor, na qual o computador cliente envia uma mensagem, solicitando a sincronia de tempo ao computador em modo servidor. O computador em modo servidor retorna a mensagem com as informações requisitadas sem manter nenhum estado de resposta, conforme ilustrado na Figura 26, os servidores clientes estão no estrato “n+1”.

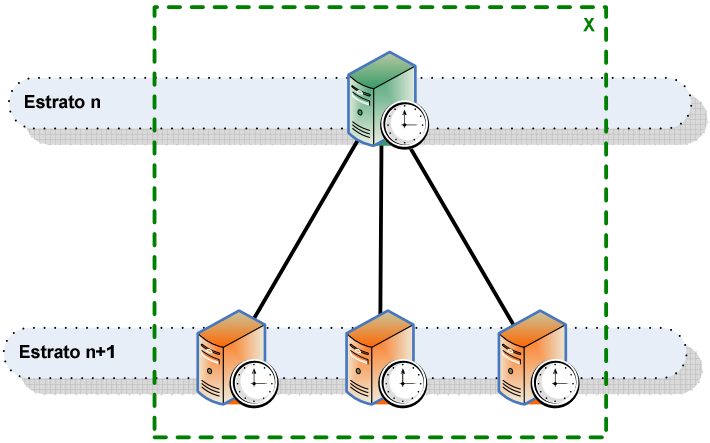

Figura 26. Sincronização entre servidores de tempo.

Nesse modelo, o tipo de comunicação pode ser considerado um mecanismo RPC (*Remote Procedure Call*) simplificado sem significante perda de exatidão e robustez, especialmente quando utiliza redes locais de alta-velocidade (Mills, 1992).

5.2.2 Sincronização de tempo entre servidor e cliente (Y)

A distribuição de tempo na configuração "*broadcast*" considera uma rede local de alta velocidade para atingir um grande número de estações, e onde uma maior exatidão não é requerida segundo Mills (1992). Essa configuração possui pelo menos um servidor de tempo, conforme Figura 27. O servidor envia mensagens de sincronia de tempo periodicamente para as estações, que determinam o tempo de latência na ordem de poucos milissegundos.

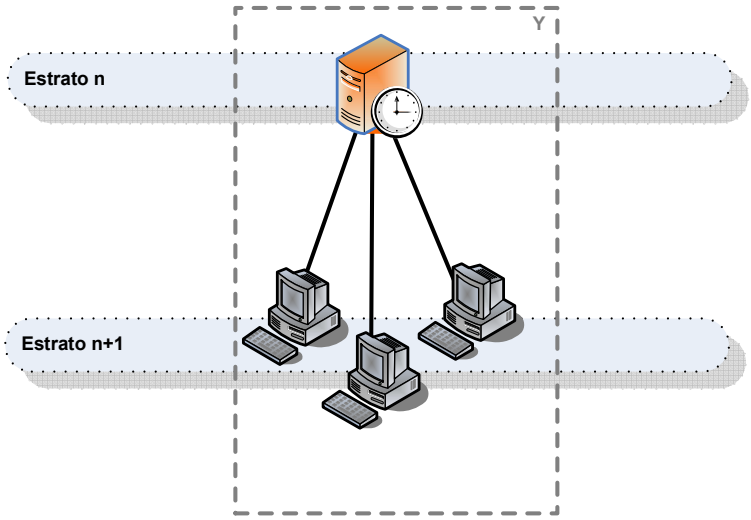

Figura 27. Sincronização entre servidor de tempo e Cliente.

5.2.3 Sincronização de tempo simétrica entre servidores (W)

A troca de mensagens entre parceiros é uma forma de endereçar questões de disponibilidade, conforme Figura 28. Nessa situação, os servidores de tempo atuam de forma cooperativa na determinação de referência do tempo.

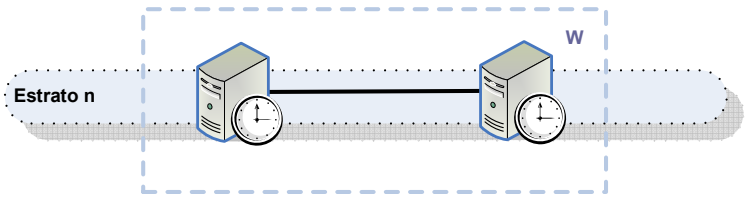

Figura 28. Sincronização simétrica entre servidores de tempo.

Cada parceiro, normalmente, opera com uma ou mais referência de tempo. Caso um dos parceiros perca a referência ou pare de funcionar, o outro assume a função de distribuição de tempo para os demais participantes.

5.2.4 Sincronização de tempo entre servidores com resiliência (Z)

Em um serviço de sincronização de tempo com resiliência, cada servidor de tempo, normalmente, opera com uma ou mais referência de tempo, conforme Figura 29. Caso um dos parceiros perca a referência ou pare de funcionar, o outro assume a função de distribuição de tempo para os demais participantes.

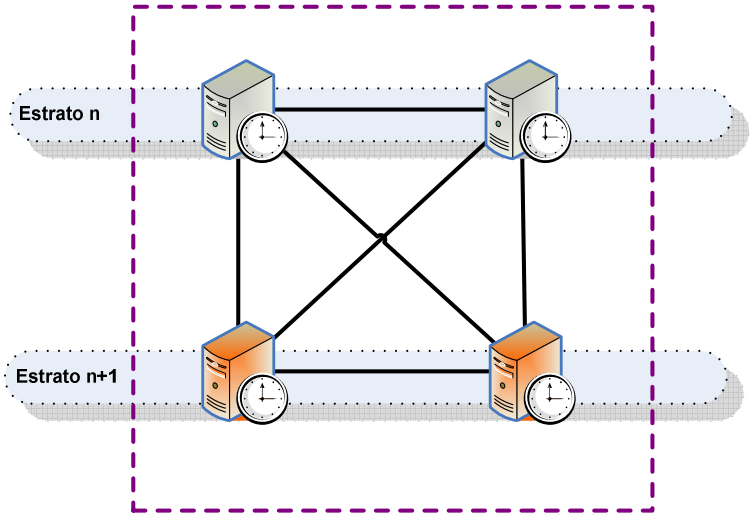

Figura 29. Sincronização entre servidores de Tempo com Resiliência.

5.2.5 Sincronização de tempo entre servidor e cliente com resiliência (K)

A troca de mensagens entre parceiros, localizado no estrato “n” dessa configuração, é uma forma de endereçar questões de disponibilidade no serviço de sincronização, conforme Figura 30. Para os clientes, há mais de um fornecedor do serviço.

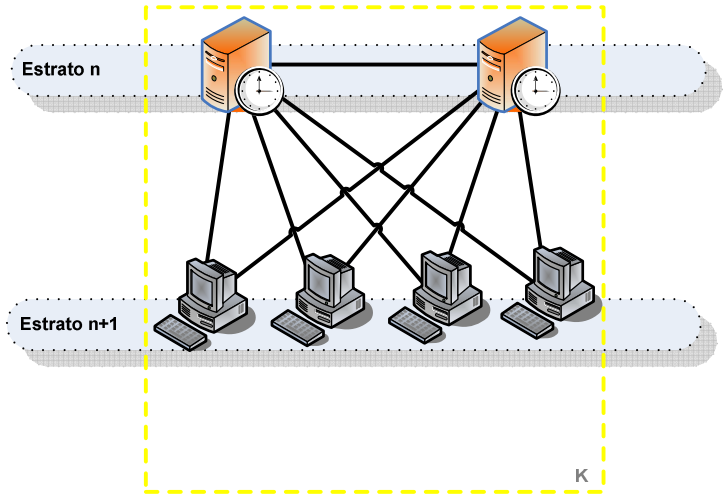

Figura 30. Sincronização entre servidores de tempo e clientes com resiliência.

Cada servidor, normalmente, opera com uma referência de tempo. Caso um deles perca a referência ou pare de funcionar, o outro assume a função de distribuição de tempo aos demais participantes. Para os clientes, essa funcionalidade deve ser feita através de uma reconfiguração automática.

5.3 Ambientes de Redes

Os protocolos de tempo da família NTP e o protocolo PTP são protocolos de camada de aplicação. Sendo assim, projetados para operar, utilizam os serviços oferecidos pela camada de transporte da pilha TCP/IP, especificamente o datagrama UDP. Além disso, utilizam-se de funcionalidades de transmissão *broadcast* e a *multicast*. E, por fim, há considerações sobre o ambiente de rede, ou seja, rede local ou rede de longa distância.

Uma das dimensões para classificação da rede é a escala, ou o tamanho físico da rede conforme adaptação de Tanenbaum (2003). A classificação inicia com redes menores de um metro e termina com a rede de local físico de 10.000 km, considerada a maior delas, conforme Tabela 03. Dessa maneira, a escala de rede foi um dos elementos considerados para determinar o ambiente de rede utilizado neste trabalho.

Tabela 3: Escala de Redes neste Trabalho.

Distância	Local Físico	Rede
1 m	Metro Quadrado	Local
10 m	Sala	Local
100 m	Prédio	Local
1 km	Campus	Local
10 km	Cidade	Local
100 km	País	Longa Distância
1000 km	Continente	Longa Distância
10000 km	Planeta	Longa Distância

Adaptação: (TANENBAUM, 2003).

Esse dimensionamento não considera as tecnologias de redes envolvidas e, portanto, não é o único aspecto a ser considerado para definir os ambientes de rede neste trabalho, principalmente, quando o protocolo PTP definido pelo IEEE (2004) for utilizado.

5.3.1 Rede local

As redes locais são utilizadas na interconexão de equipamentos processados com a finalidade de trocar dados, conforme Figura 31. São redes com menor latência, maior vazão, menor taxa de erros e maior disponibilidade em comparação com a rede de longa distância. Além de ter uma escala com limites físicos conforme adaptação de Tanembaum (2003) descrito na seção anterior.

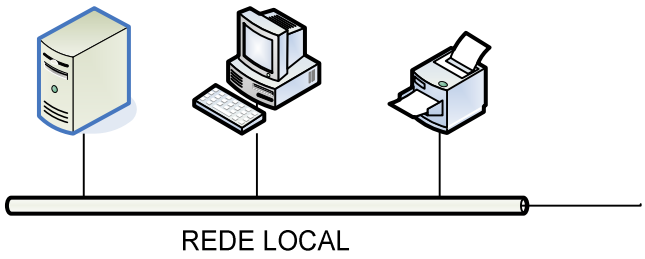

Figura 31. Rede Local. Fonte: (TANENBAUM, 2003).

Porém, neste trabalho, a definição de ambiente de rede local também considera a tecnologia de rede utilizada na arquitetura de rede. A tecnologia de rede *Ethernet* (SPURGEON, 2000) predomina nas redes locais e é largamente utilizada pelos protocolos da pilha TCP/IP. Instalações com outras tecnologias como, por exemplo, *token ring*, FDDI ou 802.11(a)(b)(g) são mínimas.

Em rede *Ethernet* o limite geográfico depende do tipo de enlace físico utilizado. Por exemplo, o padrão 1000 Base-LX suporta um único segmento de 5.000 metros. “O tamanho máximo indicado para o cabo é o mesmo de um cabo de fibra óptica em monomodo normalmente utilizado” (SPURGEON, 2000, p. 163).

Dessa forma, neste trabalho, um ambiente de rede local é aquele que utiliza a tecnologia *Ethernet* e possui baixa latência, alta vazão e baixa taxa de erros em operação normal. Além disso, os protocolos de tempo dependem exclusivamente da camada de transporte UDP. Sendo assim, são as redes locais IP.

5.3.2 Rede de longa distância

Rede de longa distância abrange uma grande área geográfica com distância acima de dez kilômetros, segundo Tanenbaum (2003). De maneira geral, é aquela que permite interligar redes locais separadas geograficamente. Para Tanenbaum (2003), o ambiente de rede de longa distância fica caracterizado pelo conjunto de sub-redes com endereçamento IP. São interligadas por enlaces de comunicação através de roteadores e, geralmente, possuem maior latência, menor vazão, maior taxa de erros e menor disponibilidade em comparação com a rede local, conforme apresentado na Figura 32.

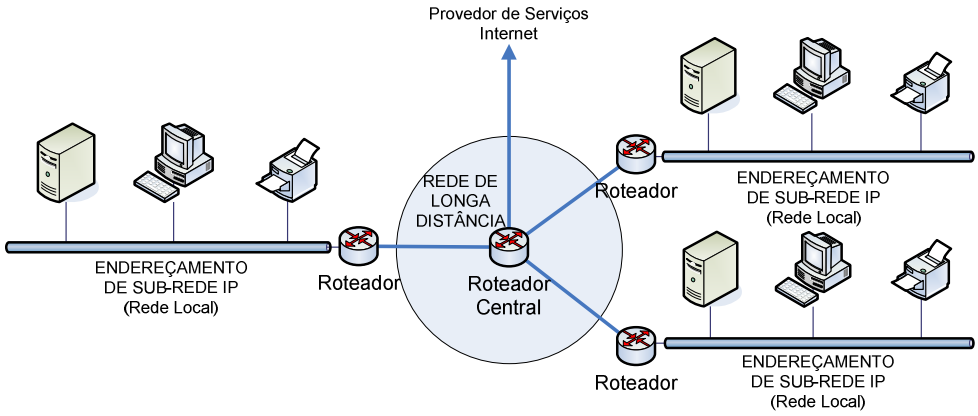

Figura 32. Coleção de endereçamento de redes. Fonte: (TANENBAUM, 2003).

Exemplos para tecnologia de rede de longa distância utilizados hoje são: X. 25, HDLC, ATM, MPLS e *Frame Relay*.

5.4 Cenários de Sincronização de Tempo

Topologia de rede física e o ambiente geográfico são correlatos à qualidade e à confiabilidade da infra-estrutura de redes. De acordo com Rybaczyk (2005), essa afirmação acontece quando canais de comunicação de longa distância estão presentes nessa infra-estrutura. Ainda, “congestionamento de rede, por sua vez, impacta a latência de comunicação entre os servidores NTP e os clientes,e, conseqüentemente, na exatidão do tempo” (RYBACZYK, 2005, p. 106).

Sendo assim, a fim de atender as necessidades de resiliência do serviço de sincronização de tempo, há uma dependência intrínseca à redundância da infra-estrutura de redes.

Adicionalmente, os protocolos de tempo utilizam serviços da camada de transporte da pilha TCP/IP. Desta maneira, em cada cenário há configurações que possibilitam a existência de vulnerabilidades e ameaças ao ambiente e, conseqüentemente, ao serviço de sincronização de tempo.

A composição de protocolos de tempo, configurações de operação e ambientes de redes formam cenários típicos de sincronização que serão utilizados posteriormente para a análise de risco.

5.4.1 Cenário de sincronização de tempo entre servidores em rede local

O serviço de sincronização de tempo tem precisão e robustez em redes locais pois são redes com menor latência, maior vazão, menor taxa de erros e maior disponibilidade em comparação com a rede de longa distância. Esse é um ambiente favorável em um modelo de comunicação não orientado à conexão, como é a maioria dos protocolos de tempo. Nesse cenário, não é considerada nenhuma linha de comunicação externa e a referência de tempo é local. Dessa maneira, não há sincronização com uma referência de tempo UTC.

Esse cenário possui apenas servidores mas a configuração comum é o modo de operação característico cliente/servidor. O computador cliente, representado no estrato “n+1”, envia uma mensagem solicitando a sincronia de tempo ao computador em modo servidor. O servidor retorna a mensagem com as informações requisitadas sem manter nenhum estado de resposta. Outra configuração possível é o modo de operação simétrico ativo/passivo, mas não é usual nessa configuração. A Figura 33 corresponde a sincronização realizada entre os clientes do serviço e o servidor em uma rede local.

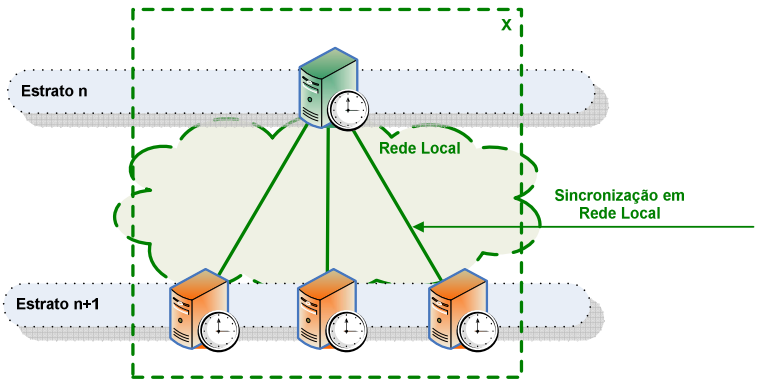

Figura 33. Sincronização de tempo entre servidores localizados em rede local

Sincronização de tempo em redes locais tem exatidão e robustez suficientes para os protocolos NTP, versão 3, NTP, versão 4 e SNTP. Porém, algumas aplicações que necessitam de precisão abaixo de microssegundos uma proposta é do IEEE (2002) que sugere o uso do protocolo PTP.

Para o protocolo PTP o modo de operação é denominado de mestre/escravo. Há uma seleção do melhor servidor-mestre na topologia PTP através do algoritmo *best master clock algorithm*, que, normalmente, é chamado de grande-mestre. Nesse caso, o servidor de tempo grande-mestre envia mensagens de sincronização periódicas ao servidor de tempo em modo escravo.

5.4.2 Cenário de sincronização de tempo entre servidores em rede de longa distância

O serviço de sincronização de tempo em redes de longa distância tende a uma precisão e robustez menor, pois são redes com maior latência, menor vazão, maior taxa de erros e menor disponibilidade em comparação com a rede local. Esse é um ambiente menos favorável em um modelo de comunicação não orientado à conexão, como é a maioria dos protocolos de tempo. Também, nesse cenário a referência de tempo é local e são consideradas linhas de comunicação externas entre as localizações dos servidores de tempo.

As linhas de comunicação entre a rede local e a rede de longa distância podem ter características de uso privado, podendo utilizar equipamentos próprios ou do fornecedor desse serviço, mas deve existir a segregação dos dados transmitidos. Normalmente, criam-se redes privadas virtuais ou circuitos virtuais privados. Mesmo em redes compartilhadas em nível de redes IP, as redes de longa distância são tratadas da mesma forma, pois os controles de segurança são pertinentes em qualquer situação.

Igualmente ao cenário anterior esse cenário possui apenas servidores mas a configuração comum é o modo de operação característico cliente/servidor. Porém, a Figura 34 corresponde a sincronização realizada entre os clientes do serviço, representados no estrato “n+1”, e o servidor em uma rede de longa distância.

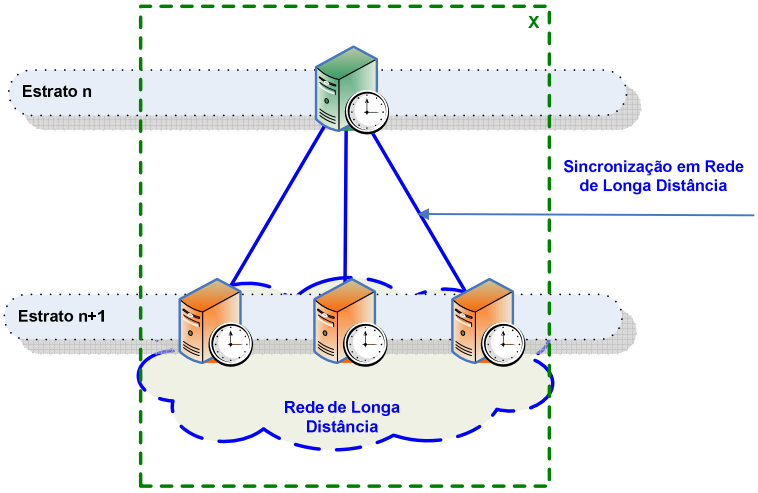

Figura 34. Sincronização de tempo entre servidores em rede de longa distância segregada.

Para os protocolos NTP, versão 3, NTP, versão 4 e SNTP, pode ter um desvio na sincronização devido à latência inerente dos canais de comunicação. Sendo assim, é um ambiente de rede desfavorável para um modelo de comunicação não orientado à conexão. Mesmo com essas dificuldades, os protocolos da família NTP conseguem sincronizar os relógios em níveis adequados para algumas das aplicações que necessitam desse serviço. Nesse cenário, a configuração comum à família de protocolos NTP entre os servidores de tempo é a configuração em modo de operação cliente/servidor.

Diferentemente, no protocolo PTP esse tipo de ambiente de rede é inadequado, pois a proposta é a sincronização abaixo de microssegundo. O que é impossível utilizando canais de comunicação de longa distância.

5.4.3 Cenário de sincronização de tempo entre servidor e cliente em rede local

Esse cenário é composto pelo ambiente de rede local e a comunicação cliente/servidor, conforme Figura 35. A referência de tempo é local e não são consideradas linhas de comunicação externas. O serviço de sincronização de tempo possui um servidor de tempo centralizado e a sincronização do tempo aos clientes localizados no estrato “n+1”. É um ambiente favorável devido as características da rede local.

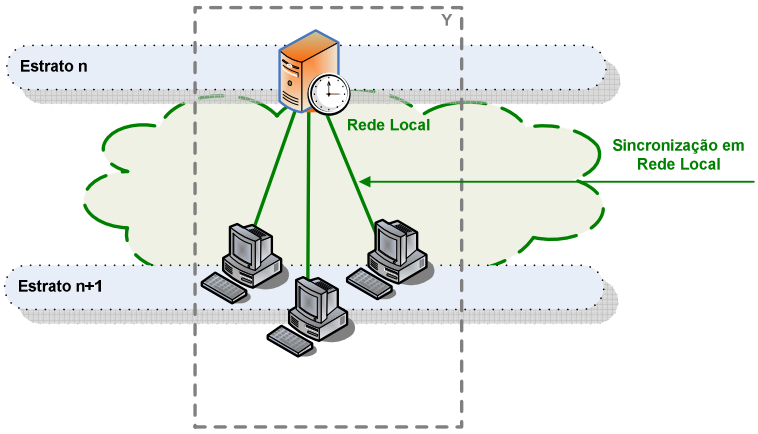

Figura 35. Sincronização de tempo entre servidores e clientes.

Sincronização de tempo aos clientes em redes locais tem exatidão e robustez suficientes aos protocolos NTP, versão 3; NTP, versão 4 e SNTP nos modos de operação *broadcast* e *multicast*.

Para o protocolo PTP, é um ambiente de rede ideal na sincronização abaixo de microssegundo, através de propagação *multicast*.

5.4.4 Cenário de sincronização de tempo entre servidores simétrico em rede local

O serviço de sincronização de tempo em modo simétrico possui a característica de dois ou mais servidores se sincronizarem atuando de forma cooperativa na determinação de referência do tempo. Esse cenário é composto pelo ambiente de rede local e uma comunicação entre servidores de tempo, conforme Figura 36. A referência de tempo é local e não são consideradas linhas de comunicação externas. Em caso de perda de um servidor o outro mantém a disponibilidade do serviço.

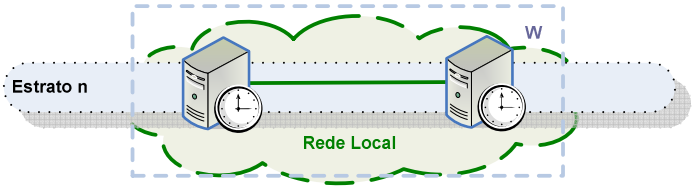

Figura 36. Sincronização de tempo entre servidores em modo simétrico.

Os protocolos de tempo NTP, versão 3, e NTP, versão 4, suportam a sincronização simétrica. Para tanto, os servidores de tempo operam em modo simétrico ativo e passivo. Nessa configuração, o servidor ativo envia uma mensagem de sincronização de forma periódica ao seu parceiro em modo passivo. O servidor ativo anuncia sua intenção de sincronizar e ser sincronizado pelo seu par. Tal associação persiste enquanto uma mensagem de resposta seja enviada pelo par caso contrário, a associação é desfeita.

No padrão IEEE (2002) ainda não está definida a forma de manter servidores de tempo em redundância a fim de atender questões de disponibilidade do serviço.

5.4.5 Cenário de sincronização de tempo entre servidores com resiliência em rede local

Um serviço de sincronização de tempo robusto depende também da sua disponibilidade, devido a falhas de componentes do próprio serviço e do *hardware* suportado, além do ambiente de rede propício a uma comunicação eficiente.

Dessa maneira, é possível oferecer um cenário com alta disponibilidade com servidores de tempo redundantes conforme Figura 37.

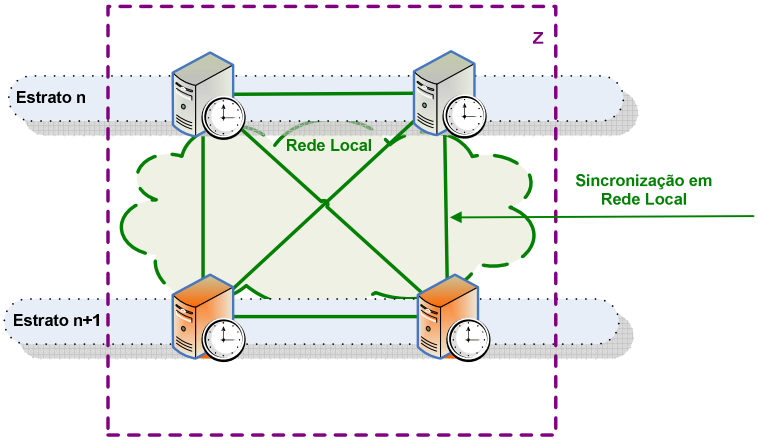

Figura 37. Sincronização de tempo entre servidores com resiliência.

Nos protocolos de tempo NTP, versão 3, e NTP, versão 4, é possível a sincronização de tempo em redes locais com um alto grau de disponibilidade. Nessa configuração, cada servidor de tempo do extrato inferior tem outros três servidores de tempo redundantes. Uma maneira de fazer isso é quando os servidores de tempo assumem os modos de operação simétrico ativo e passivo.

No padrão IEEE (2002) isso ainda não está definido e não há como considerar a disponibilidade do serviço de sincronização de tempo.

5.4.6 Cenário de sincronização de tempo entre servidores com resiliência em rede de longa distância

Nesse cenário, o serviço de sincronização de tempo depende da disponibilidade dos componentes do serviço, do *hardware* suportado e do ambiente de rede propício a uma comunicação eficiente. Com linhas de comunicação reduntantes também é possível oferecer um cenário com alta disponibilidade com servidores de tempo redundantes conforme Figura 38.

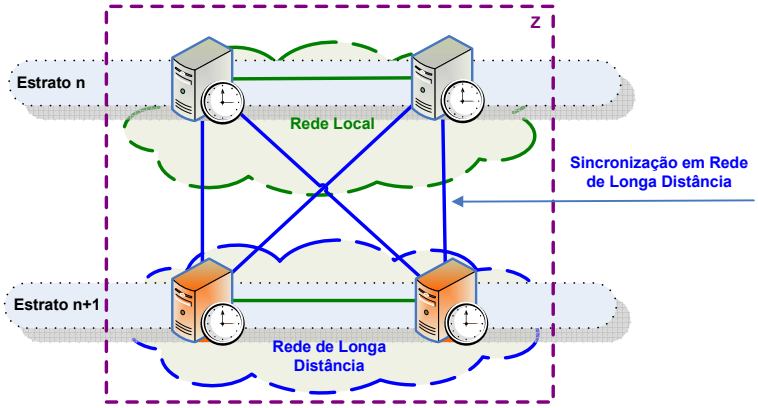

Figura 38. Sincronização de tempo com resiliência entre servidores em rede de longa distância.

Esse cenário também propicia um alto grau de disponibilidade e utiliza os protocolos NTP, versão 3, e NTP, versão 4. Os clientes são atendidos de forma totalmente redundante. A diferença está nas linhas de comunicações que são de longa distância. Por questões de desempenho da rede de longa distância, o serviço de sincronização de tempo pode ter desvios na precisão, o quais o ambiente da seção anterior são menos prováveis de acontecer.

5.4.7 Cenário de sincronização de tempo entre servidor e cliente com resiliência em rede local

O serviço de sincronização de tempo é idêntico ao exposto na seção 5.4.3 mas sendo complementado com a redundância de servidores em modo simétrico da seção 5.4.4. Nesse cenário de sincronização há um alto grau de disponibilidade do serviço utilizando dois ou mais servidores de tempo e um ambiente de rede local, conforme Figura 39.

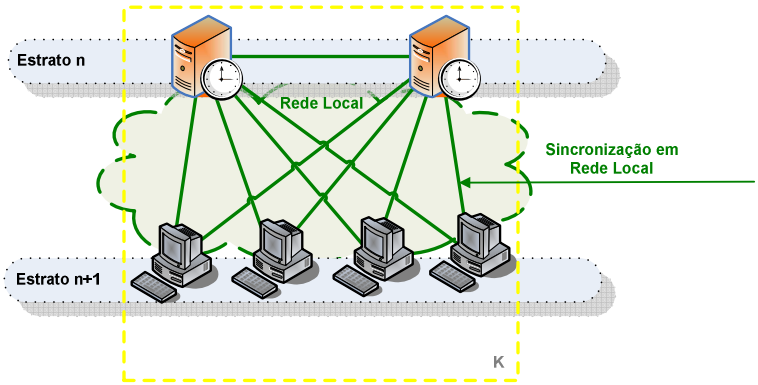

Figura 39. Sincronização de tempo entre servidores e clientes com resiliência em rede local

Para os protocolos de tempo NTP, versão 3, e NTP, versão 4. O modo de operação dos servidores é o simétrico ativo/passivo e, dos clientes, o mais adequado é o modo de operação *manycast*. Os clientes requisitam as informações de tempo em um endereço de *multicast* IP a fim de receber a sincronização de um dos servidores nesse grupo.

No padrão IEEE (2002) não há algo similar ainda.

6 DETERMINAÇÃO DE RISCO DO SERVIÇO DE SINCRONIZAÇÃO DE TEMPO

Para determinar o grau de risco do serviço de sincronização de tempo foi utilizado como base a publicação SP800-30 *Risk Management Guide for Information Technology Systems* (STONEBURNER; GOGUEN; FERINGA, 2002). O processo de avaliação de risco desta publicação foi resumida no apêndice A deste trabalho. Nesse processo, são identificadas as ameaças e vulnerabilidades para determinar o grau de probabilidade, a magnitude do impacto e o grau de risco, caso a vulnerabilidade seja explorada intencionalmente ou acionada acidentalmente.

As ameaças e vulnerabilidades do serviço de sincronização de tempo geradas neste trabalho são, geralmente, conseqüencias de fontes de ameaças primárias como, por exemplo, falha de componentes do sistema. Para o enriquecimento do trabalho também serão listadas as fontes de ameaças conforme SHIREY (2000).

Ao determinar o grau de probabilidade da vulnerabilidade ser explorada ou acionada, é necessário analisar o ambiente de rede o qual a vulnerabilidade está contextualizada, pois, a probabilidade de uma vulnerabilidade ser exercitada é mais suscetível em uma ambiente de rede de longa distância, por exemplo. Para determinar a magnitude do impacto ao serviço de sincronização de tempo, tal análise do ambiente de rede é independente do contexto. Pois, o serviço é impactado de maneira idêntica em qualquer situação.

A mensuração de impactos pode ser medida de forma quantitativa e/ou qualitativa. “Medidas quantitativas são perdas de receitas, custo de reparos de sistemas ou grau de esforço requerido a fim de corrigir problemas ocasionados por uma ameaça bem sucedida” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 22). Impactos de outros tipos, como perda de confidencialidade, perda de credibilidade ou perda de imagem são difíceis de ser mensurados por unidades específicas. Assim, podem ser qualificados na magnitude do impacto como sendo: altos, médios ou baixos.

Na análise de impacto deste trabalho, as medidas quantitativas não são possíveis devido à natureza do conteúdo ser generalizada. Não há medidas com valores de referência já definidos.

No ambiente de rede são consideradas as ameaças mais comuns ao meio de transmissão, tipicamente aquelas que afetam a disponibilidade do serviço, integridade da mensagem e interferência no serviço ocasionando erros ou desvios inesperados. Essas ameaças são analisadas para o enriquecimento do trabalho sem considerar os controles em nível de rede, pois não é objetivo deste estudo. A existência de tais controles de rede interferem na análise de segurança intrínseca dos protocolos objeto deste estudo. Dessa maneira, os riscos são identificados sem os controles em nível de rede como, por exemplo, controle de acesso 802.1x. Além disso, conceitos gerais de segurança e riscos que estão ligados à falha ou vulnerabilidade dos sistemas operacionais estão fora do escopo desta análise.

Por fim, é determinado o grau de risco das ameaças e vulnerabilidades no ambiente de rede local e em rede de longa distância. Essas listas de riscos serão utilizados no capítulo 8, na análise de risco dos cenários de sincronização de tempo, a fim de recomendar os controles necessários para a mitigação dos riscos.

6.1 Identificação de Ameaça

Um serviço de sincronização de tempo permite garantir a ordem temporal dos eventos que ocorrem no ambiente. Uma interrupção, modificação ou atraso das mensagens do protocolo de tempo podem ocasionar desvios de tempo. Conseqüentemente, as aplicações que dependem de tal serviço são afetadas.

A lista de fontes de ameaças (SHIREY, 2000) é utilizada como referência para o Quadro 6, o qual apresenta as possíveis fontes de ameaças que causam as ameaças ao serviço de sincronização de tempo.

Fonte de Ameaça	Descrição
Desastre natural	Qualquer evento ou circunstância inesperada ocasionada por um desastre que interrompe as operações do sistema. Alguns exemplos são: enchentes, incêndio, tempestades, entre outros.
Destruição física	Destruição deliberada de algum componente do ambiente que interrompe operações do serviço.
Erro de *hardware* ou *software*	Erros ocasionados por falhas de componentes do sistema que interrompam suas operações.
Erro humano	Ação ou falta de alguma atividade não-intencional que afeta algum componente do sistema e interrompe suas operações.
Inserção de dados falsos	Introdução de dados falsos para dissimular uma entidade autorizada.
Interferência	Ruptura na operação do serviço de sincronização de tempo bloqueando a comunicação entre os clientes e servidores, impedindo o fluxo dos dados do serviço ou da informação de controle.
Personificação	Acesso não-autorizado pelo sistema de forma a atuar como se fosse um acesso autorizado a fim de desempenhar uma ação maliciosa.
Sobrecarga do serviço	Sobrecarga na operação do serviço devido ao excesso de requisições ao processamento dos componentes do sistema.
Substituição de dados falsos	Substituição de dados válidos com dados falsos para dissimular uma entidade autorizada na sincronia de tempo.

Quadro 6. Possíveis fontes de ameaças. Adaptação: (SHIREY, 2000).

As ameaças específicas que afetam o serviço de sincronização de tempo são determinadas, principalmente, pelo impacto adverso ao funcionamento do serviço. Tais ameaças foram geradas neste trabalho e são listadas no Quadro 7.

Ameaças Específicas	Descrição
Desvio significativo de sincronismo em um cliente	Qualquer evento ou circunstância inesperada que ocasione a imprecisão do sincronismo de tempo no cliente. Algumas fontes de ameaças: falha de componente ou sobrecarga de processamento.
Perda de sincronismo em um cliente	Qualquer evento ou circunstância que interrompa o sincronismo. Algumas fontes de ameaças: personificação ou destruição física.
Desvio significativo de sincronismo em um servidor	Qualquer evento ou circunstância inesperada que ocasione a imprecisão do sincronismo de tempo no servidor. Algumas fontes de ameaças: falha de componente ou sobrecarga de processamento.
Perda de sincronismo em um servidor	Qualquer evento ou circunstância que interrompa o sincronismo. Algumas fontes de ameaças:interferência ou destruição física.
Subversão de um servidor legítimo	Qualquer evento intencional que ocasione a subversão da referência do sincronismo. Algumas fontes de ameaças: personificação ou apropriação do serviço.

Quadro 7. Ameaças específicas ao serviço de sincronização de tempo.

6.2 Identificação de Vulnerabilidade

A identificação das vulnerabilidades considera o ambiente de rede, as funcionalidades e os serviços de segurança descritos na seção 3.3. Vulnerabilidades do meio de comunicação são analisadas dadas as características dos protocolos de tempo, as quais utilizam os serviços oferecidos pela camada de transporte utilizando o protocolo UDP. Tal dependência aliada à ausência de controle no ambiente de rede como, por exemplo, VLAN, controle de acesso 802.1x ou criptografia IPSec na transmissão dos dados, cria riscos à camada de aplicação.

Mills (1996) afirma que há dois cenários nos quais um intruso pode afetar a qualidade de sincronismo: “no primeiro, um intruso pode interceptar e retransmitir uma mensagem entre o cliente e o servidor. No segundo cenário, o intruso pode interromper as operações do servidor ou do cliente” (MILLS, 1996, p. 20).

O Quadro 8 apresenta as vulnerabilidades dos protocolos de tempo geradas neste trabalho.

Vulnerabilidade	Descrição
Ausência de autenticação do servidor de tempo	Falta ou não configuração do serviço de autenticação
Ausência de identificação do servidor de tempo autorizado	Falta ou não configuração do serviço de identificação
Ausência de servidor de tempo redundante	Falta ou não configuração de um servidor de tempo redundante
Alta latência no enlace de comunicação	Alta latência entre a comunicação dos participantes do sincronismo de tempo
Ausência de enlace de comunicação redundante	Falta ou não configuração de um enlace de comunicação redundante
Negação do serviço de tempo	Susceptibilidade a degradação ou indisponibilidade do serviço de tempo

Quadro 8. Vulnerabilidades dos protocolos de tempo.

6.2.1 Ausência de autenticação do servidor de tempo

A ausência de autenticação do servidor de tempo é uma vulnerabilidade que possibilita diversos tipos de ataques ao serviço, principalmente, em associação efêmera. Ou seja, aquela que é mobilizada sem necessidade de configuração explícita nos arquivos de configuração.

Mills afirma que a “associação efêmera sempre deve ser autenticada porque um intruso pode personificar um servidor e injetar valores de tempo falsos” (MILLS, 2006a, p. 22).

Além disso, se a autenticação existir e for comprometida é possível interceptar uma mensagem legítima do servidor, modificar um ou mais campos do protocolo e reenviar a mensagem alterada.

6.2.2 Ausência da identificação do servidor autorizado

De acordo com Shirey (2000), a identificação é uma ação ou processo que apresentada uma credencial ao sistema que permite o reconhecimento da entidade e distingui-la de outras entidades.

Apesar da existência de um servidor autorizado, essa vulnerabilidade existe quando a identidade do servidor não é conhecida previamente e, portanto, não é possível verificar se é um servidor autorizado. De fato, Mills (1996) afirma que o modo de operação *manycast* traz novos problemas no contexto de segurança, onde “a identidade do servidor não é conhecida de maneira antecipada” (MILLS, 1996, p. 8).

6.2.3 Ausência do servidor de tempo redundante

A falha de um servidor de tempo pode ser crítica caso não exista redundância do serviço. Para possibilitar um serviço de sincronização de tempo resiliente, é necessário existir mais de um servidor de tempo. “Mas um número ideal é subjetivo para muitos e conflita com problemas de engenharia” (MILLS, 2006a, p. 83), para tanto, há algumas regras para uma implantação NTP:

a) Com apenas um servidor disponível, pode acontecer sua falha ou esse servidor se tornar uma referência imprecisa. Conseqüentemente, os clientes perderão a sincroniza ou precisão de tempo por falha do serviço ou pela referência imprecisa;
b) Com dois servidores de tempo, mas com a perda de um deles, os clientes mantém com a sincronia de tempo. Mas não há garantia de que o servidor disponível se torne uma referência imprecisa;
c) Com três servidores de tempo disponíveis, um deles pode se tornar um servidor impreciso aos clientes;
d) Com quatro ou mais servidores de tempo disponíveis, o algoritmo de *cluster* pode encontrar os três melhores sobreviventes, contribuindo para uma diferença média de tempo, mesmo no caso de um servidor impreciso.

Para determinar a falha de um servidor e a vulnerabilidade, é necessário prever a quantidade de servidores de tempo disponíveis para identificar o grau de risco do serviço de sincronização de tempo.

6.2.4 Alta latência no enlace de comunicação

Para o serviço de sincronização de tempo, que depende do tráfego da rede, essa vulnerabilidade é muito difícil de ser detectada. Mills (1996) afirma que “de fato, não é possível, de outra maneira que por análise estatística, determinar se tal ataque está em progresso ou é o resultado de outros padrões de carga da rede” (MILLS, 1996, p. 26). Para Mills (2006a), servidores primários e secundários devem fornecer um serviço contínuo de tempo preciso e, em alguns casos, exato. “Mesmo com significantes variações de atraso e oscilações da rede” (MILLS, 2006a, p. 16).

A alta latência afeta a qualidade do sincronismo e deve ser endereçada com mecanismos de disponibilidade adicionais como, por exemplo, servidores redundantes na sub-rede de sincronismo.

6.2.5 Ausência de enlace de comunicação redundante

Segundo Mills (2006a), uma das premissas para o desenvolvimento do protocolo de tempo é fornecer uma sub-rede de sincronismo confiável e sobrevivente, “mesmo em condições instáveis da rede e quando há perda da conectividade por um período de dias” (MILLS, 2006a, p. 16).

Dessa forma, o serviço de sincronização de tempo deve prever a possibilidade de servidores redundantes, diferente linhas de transmissão e algum mecanismo para restabelecer em caso de perda do serviço.

6.2.6 Negação de serviço do servidor de tempo

A negação de serviço é caracterizada pela sobrecarga dos recursos ou componentes do serviço, ocasionado por uma exploração ou acionamento involuntário. Os resultados inesperados podem produzir efeitos indesejados como, por exemplo, a imprecisão do tempo e, até mesmo, a indisponibilidade do serviço.

Mills (1996) reforça que o servidor de tempo NTP em modo cliente/servidor ou *multicast* responde às mensagens de qualquer cliente sem a necessidade de autenticá-las ou verificar se os dados são válidos. E, “como o processamento necessário para responder as requisições dos clientes é modesto e nenhum estado de persistência é gerado, essa vulnerabilidade da negação de serviço do servidor é mínima” (MILLS, 1996, p. 26).

Porém, se o volume de mensagem válido, originado por um ataque ou clientes mal-configurados, for gerado em uma taxa maior que a capacidade de processá-las, o resultado pode ser uma paralisação do serviço, ou um congestionamento da rede, ou qualquer indisponibilidade do recurso envolvido. Como exemplificado por Mills (1996):

> Experiências operacionais com alguns servidores primários (estrato 1) com uma população de clientes muito grande em uma determinada rede têm demonstrado que os clientes pobremente configurados podem produzir um enorme volume de requisições, que pode sobrecarregar os caminhos de rede até um servidor. Isto ocorre quando administradores de rede clonam um arquivo de configuração e copiam em milhares de clientes naquela rede (MILLS, 1996).

Também, é possível que essa vulnerabilidade esteja associada a ataques ao meio de comunicação por inundação de mensagens tipicamente UDP ou ICMP, desde que o controle de acesso ao meio de comunicação não seja adequado ou for infringido.

6.3 Determinação de Probabilidade

Uma classificação da probabilidade considera a motivação e capacidade da ameaça explorar a vulnerabilidade. Também, se há controles adequados e efetivos para prevenir ou impedir os ataques. Um critério utilizado (STONEBURNER; GOGUEN; FERINGA, 2002, 2002) para classificar o grau de probabilidade é resumido no Quadro 9.

Definição	Probabilidade
A origem da ameaça é altamente motivada e suficientemente capaz de exercer o ataque. E, controles para prevenir a vulnerabilidade são ineficientes.	ALTA
A origem da ameaça é motivada e capaz de exercer o ataque. No entanto, controles estão no local para prevenir o ataque à vulnerabilidade.	MÉDIA
Falta motivação ou capacidade para exercer o ataque. Ou, controles estão no local para prevenir, ou impedir significativamente, o ataque à vulnerabilidade.	BAIXA

Quadro 9. Critério para o grau de probabilidade. Fonte: (STONEBURNER; GOGUEN; FERINGA, 2002).

Com o grau da probabilidade definido, é possível aplicá-lo às vulnerabilidades da seção 6.2. O Quadro 10 resume o grau de probabilidade de um par de ameaça e vulnerabilidade acontecer em um ambiente de rede local.

Ameaças Específicas	Vulnerabilidades	Prob.
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIA
	Ausência de identificação do servidor de tempo	MÉDIA
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXA
	Ausência de enlace de comunicação redundante	BAIXA
	Alta latência no enlace de comunicação	BAIXA
	Ausência de proteção contra negação do serviço de tempo	MÉDIA
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	MÉDIA
	Ausência de servidor de tempo redundante	MÉDIA
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA
	Ausência de enlace de comunicação redundante	BAIXA
	Alta latência no enlace de comunicação	BAIXA
	Ausência de proteção contra negação do serviço de tempo	MÉDIA
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	MÉDIA
	Ausência de servidor de tempo redundante	MÉDIA

Quadro 10. Probabilidade das ameaças em rede local.

Pressupõe-se que os possíveis controles dos protocolos de tempo não estão configurados ainda.

Para o enriquecimento da análise do grau da probabilidade, foi feito uma análise do grau de probabilidade em rede de longa distância também. Conforme o Quadro 11, os mesmos pares de ameaça e vulnerabilidades foram classificados no ambiente de rede de longa distância.

Ameaças Específicas	Vulnerabilidades	Prob.
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIA
	Ausência de identificação do servidor de tempo	MÉDIA
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXA
	Ausência de enlace de comunicação redundante	ALTA
	Alta latência no enlace de comunicação	ALTA
	Ausência de proteção contra negação do serviço de tempo	ALTA
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTA
	Ausência de servidor de tempo redundante	ALTA
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA
	Ausência de enlace de comunicação redundante	ALTA
	Alta latência no enlace de comunicação	ALTA
	Ausência de proteção contra negação do serviço de tempo	ALTA
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTA
	Ausência de servidor de tempo redundante	ALTA

Quadro 11. Probabilidade das ameaças em rede de longa distância.

6.4 Análise de Impacto

Um impacto adverso a qualquer um dos objetivos de segurança tem conseqüências indesejadas ao serviço de sincronização de tempo. Neste trabalho, a mensuração é determinada de forma qualitativa, pois não há perdas quantitativas estipuladas por ser um conteúdo generalista.

O Quadro 12 descreve a magnitude do impacto conforme alguns critérios utilizados em (STONEBURNER; GOGUEN; FERINGA, 2002). Porém, neste trabalho serão considerados para os ítens (1) e (2).

Definição	Impacto
(1) Pode resultar em perdas de altos valores dos principais recursos ou ativos tangíveis. (2) Pode resultar de forma significativa violação, danificação ou impedir a missão da organização, reputação ou interesses. (3) Pode resultar em ferimentos humanos graves inclusive morte.	ALTO
(1) Pode resultar em perdas de valores de recursos ou ativos tangíveis. (2) Pode resultar a violação, danificação ou impedir a missão da organização, reputação ou interesses. (3) Pode resultar em ferimentos humanos graves.	MÉDIO
(1) Pode resultar em perdas de alguns de recursos ou ativos tangíveis. (2) Pode afetar a missão da organização, reputação ou interesses.	BAIXO

Quadro 12. Critério para a magnitude do impacto. Fonte: (STONEBURNER; GOGUEN; FERINGA, 2002).

Diferentemente da análise de probabilidade, a magnitude do impacto é considerada idêntica para o ambiente de rede local e de longa distância.

O Quadro 13 resume o impacto de um par de ameaça e vulnerabilidade caso aconteça e, para a elaboração desse quadro, pressupõe-se o uso dos critérios do Quadro 12. Assim, é considerado que o serviço de sincronização de tempo é crucial para a missão das organizações e a falta desse serviço pode resultar em perdas significantes.

Ameaças Específicas	Vulnerabilidades	Impacto
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIO
	Ausência de identificação do servidor de tempo	MÉDIO
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXO
	Ausência de enlace de comunicação redundante	BAIXO
	Alta latência no enlace de comunicação	BAIXO
	Ausência de proteção contra negação do serviço de tempo	BAIXO
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTO
	Ausência de servidor de tempo redundante	ALTO
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXO
	Ausência de enlace de comunicação redundante	MÉDIO
	Alta latência no enlace de comunicação	MÉDIO
	Ausência de proteção contra negação do serviço de tempo	MÉDIO
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTO
	Ausência de servidor de tempo redundante	ALTO

Quadro 13. Impacto das ameaças.

6.5 Determinação de Risco

A avaliação do grau de risco é determinada pela relação da probabilidade e do impacto das seções anteriores. Tal relação é apresentada no Quadro 14 e determina, por exemplo, que um grau de risco alto é a relação entre a probabilidade e impacto alto.

Vulnerabilidade/Ameaça	Impacto		
Probabilidade	BAIXO	MÉDIO	ALTO
BAIXO	BAIXO	BAIXO	MÉDIO
MÉDIO	BAIXO	MÉDIO	ALTO
ALTO	MÉDIO	ALTO	ALTO

Quadro 14. Exemplo de grau de risco.

Dessa forma, um par de vulnerabilidade e ameaça tem sua probabilidade e impacto com um determinado grau de risco. O Quadro 15 lista os pares de ameaças e vulnerabilidades de uma rede local, ordenado por grau de risco.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO
	Ausência de identificação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO
	Ausência de enlace de comunicação redundante	BAIXA	BAIXO	BAIXO
	Alta latência no enlace de comunicação	BAIXA	BAIXO	BAIXO
	Ausência de proteção contra negação do serviço de tempo	MÉDIA	BAIXO	BAIXO
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA	BAIXA	BAIXO
	Ausência de enlace de comunicação redundante	BAIXA	MÉDIO	BAIXO
	Alta latência no enlace de comunicação	BAIXA	MÉDIO	BAIXO
	Ausência de proteção contra negação do serviço de tempo	MÉDIA	MÉDIO	MÉDIO
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO

Quadro 15. Grau de risco em rede local.

O Quadro 16 lista os pares de ameaças e vulnerabilidades de uma rede de longa distância, ordenado por grau de risco.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO
	Ausência de identificação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO
	Ausência de enlace de comunicação redundante	ALTA	BAIXO	MÉDIO
	Alta latência no enlace de comunicação	ALTA	BAIXO	MÉDIO
	Ausência de proteção contra negação do serviço de tempo	ALTA	BAIXO	MÉDIO
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTA	ALTO	ALTO
	Ausência de servidor de tempo redundante	ALTA	ALTO	ALTO
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO
	Ausência de enlace de comunicação redundante	ALTA	MÉDIO	ALTO
	Alta latência no enlace de comunicação	ALTA	MÉDIO	ALTO
	Ausência de proteção contra negação do serviço de tempo	ALTA	MÉDIO	ALTO
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTA	ALTO	ALTO
	Ausência de servidor de tempo redundante	ALTA	ALTO	ALTO

Quadro 16. Grau de risco em rede de longa distância.

As ameaças e vulnerabilidades são base para a recomendação dos controles de segurança que norteiam a mitigação dos riscos. Com a determinação do grau de risco, é utilizado um critério de mitigação, gerado neste trabalho, para a aplicação dos possíveis controles dos protocolos de tempo na análise de risco do capítulo posterior.

No capítulo 8, na análise de risco dos cenários de sincronização de tempo, será selecionado um controle que endereça um possível ataque associado a um par de vulnerabilidades e ameaças. Para a mitigação obrigatória é exigido um controle obrigatório de acordo com o grau de risco do Quadro 17. Também, serão validadas a mitigação recomendada e opcional, se houver.

Grau de Risco	Mitigação
ALTO	OBRIGATÓRIA
MÉDIO	RECOMENDADA
BAIXO	OPCIONAL

Quadro 17. Critério para mitigação do risco.

7 LEVANTAMENTO DOS POSSÍVEIS CONTROLES

Neste capítulo são descritos os possíveis controles dos protocolos de tempo do escopo deste trabalho. Tais controles são classificados como técnicos, pois, de acordo com STONEBURNER; GOGUEN e FERINGA (2002), são aqueles incorporados dentro do *hardware, software* ou *firmware* de um determinado sistema. Os controles não-técnicos tratam de procedimento operacional ou procedimento relativo à política de segurança, o que, não é foco deste trabalho. Adicionalmente, nos controles técnicos são descritos somente os controles preventivos como, por exemplo, “controles de acesso, criptografia e autenticação” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 20). Pois, outros controles como, por exemplo, de detecção de intrusão descrita por STONEBURNER; GOGUEN e FERINGA (2002) não são aplicados aos protocolos de tempo.

Também, os possíveis controles são alinhados aos serviços e mecanismos da referência de segurança X. 800 (INTERNATION TELECOMMUNICATION UNION, 1990) apresentados no capítulo 3 para um processo de análise de risco mais consistente. Alguns exemplos são: a autenticação, o controle de acesso e a disponibilidade.

Por fim, através da análise de risco dos possíveis controles é possível indicar os protocolos e os controles mais adequados a cada cenário de sincronização de tempo.

7.1 Possíveis Controles NTP versão 3

Os controles de segurança oferecidos pelo protocolo NTP, versão 3, são: a autenticação, a confiabilidade, o controle de acesso, a disponibilidade e a integridade. Tais controles possibilitam a “proteção de falhas de implantação, operações impróprias e possível ataque malicioso de reenvio com ou sem modificação dos dados” (MILLS, 1992, p. 63).

Ainda, segundo Mills (1992), o protocolo prevê alguns controles de sanidade através das mensagens de controle descritas na seção 4.1.2 que inclui, por exemplo, uma verificação da porta e endereço UDP/IP de origem e destino. Além disso, o carimbo de tempo utilizado pelas mensagens evita alguns ataques de reenvio, pois é improvável prever carimbos de tempo futuros com a precisão requerida somente com observações passadas. Porém, essas funcionalidades não são proteções ideais mesmo permitindo alguma resistência a ataques de personificação e reenvio.

Por fim, o protocolo oferece a implantação de servidores redundantes, permitindo a disponibilidade e eventuais desvios de operação do serviço, evitando ação acidental ou intencional que causam eventos indesejados.

O Quadro 18 resume os controles existentes no NTP, versão 3, descritos com mais detalhes logo abaixo:

Controles	
Serviços	**Mecanismos**
Autenticação	Criptografia Simétrica
Confiabilidade	Relação 3m+1
Controle de acesso	Restrição de endereço IP do parceiro Comando *Restrict*
Disponibilidade	Servidores em modo simétrico ativo e passivo
Integridade	*Message Digest* – MD5 ou DES-CBC mode

Quadro 18. Mecanismos existentes no NTPv3. Fonte: (RYBACZYK, 2005).

7.1.1 Controles em modo simétrico ativo e passivo

Os possíveis controles em modo simétrico ativo e passivo são descritos a seguir com alguns exemplos para ilustrar tais controles:

a) Autenticação: através de uma associação persistente, a chave secreta é pré-distribuída e armazenada em um arquivo protegido em ambos servidores. É possível que tal arquivo seja alterado por meio externo ao protocolo NTP para uma distribuição segura da chave. “Para uma proteção robusta é necessário um protocolo de acordo de chaves independente do NTP” (MILLS, 1996, p. 18). A associação é iniciada por qualquer parceiro o qual possui a chave secreta *key* 1 e *key* 2 no arquivo “ntp.keys” conforme exemplo no Quadro 19;

ntp.keys
keys /etc/inet/ntp.keys trustedkey 1 2 peer saopaulo key 1 peer riodejaneiro key 2

Quadro 19. Exemplo de modo simétrico NTPv3. Adaptação: (DEETHS, 2001b).

b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;
c) Controle de acesso: restringir o acesso através dos parâmetros do comando *restrict* conforme seção 4.1.6. Além disso, limitar o acesso do parceiro através do endereço IP. Parâmetros recomendados: *Default, Ignore, Server, Nomodify, Nopeer, Noquery* e *Notrap;*
d) Disponibilidade: para evitar servidores de tempo falso, são necessárias parcerias com mais de 4 servidores. Também, utilizar autenticação para evitar mobilização de associações falsas e, conseqüentemente, ataques de negação de serviço;
e) Integridade: utilizar autenticação com chave secreta que, através do uso do código MAC, oferece a integridade das mensagens;

7.1.2 Controles em modo cliente/servidor

Os possíveis controles em modo cliente/servidor são descritos a seguir com alguns exemplos para ilustrar tais controles:

a) Autenticação: a associação permite o uso de chave secreta para autenticação dos servidores aos clientes. A associação é iniciada pelo cliente que possui a configuração da chave secreta no arquivo de configuração “ntp.conf”, conforme exemplo no Quadro 20;

ntp.conf
keys /etc/inet/ntp.keys server amazonas prefer key 1 server saofrancisco key 1 server parana key 4 trustedkey 1 4

Quadro 20. Exemplo de modo cliente NTPv3. Adaptação: (DEETHS, 2001b).

b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo

de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;

c) Controle de acesso: possível utilização do comando *restrict.* Porém, em um número grande de clientes, torna-se uma implantação complexa;
d) Disponibilidade: a disponibilidade do serviço é possível com a configuração de vários servidores de tempo, conforme Quadro 20. Porém, o serviço é frágil, pois não valida as requisições feitas pelos clientes. “Um servidor ordinariamente responde a qualquer requisição do cliente sem necessariamente autenticar as requisições ou conferir se são dados válidos (MILLS, 1996, p. 26);
e) Integridade: utilizar autenticação, pois se utiliza de código MAC.

7.1.3 Controles em modo *broadcast* e *multicast*

Os possíveis controles em modo *broadcast* e *multicast* são descritos a seguir com alguns exemplos para ilustrar tais controles:

a) Autenticação: associação iniciada pelo servidor *broadcast* o qual possui a especificação da chave secreta, conforme exemplo no Quadro 21.

ntp.keys
keys /etc/inet/ntp.keys *broadcast* 192.168.5.255 key 10 ttl 6

Quadro 21. Exemplo de modo servidor *broadcast* NTPv3. Adaptação: (DEETHS, 2001b).

Em modo *multicast*, a configuração é idêntica, mas utiliza o endereço de *multicast* conforme Quadro 22;

ntp.keys
keys /etc/inet/ntp.keys *broadcast* 224.0.1.1 key 12 ttl 6

Quadro 22. Exemplo de modo servidor *multicast* NTPv3. Adaptação: (DEETHS, 2001b).

b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;

c) Controle de acesso: não existe nesse modo;
d) Disponibilidade: um computador cliente em modo *broadcast* ou *multicast* possui apenas um parâmetro de configuração *broadcastclient* ou *multicastclient* no arquivo “ntp.conf”, conforme exemplo no Quadro 23 e Quadro 24 respectivamente. Dessa maneira, um cliente sincroniza com qualquer servidor nesse modo de operação. Deeths (2001b) afirma que ”é importante utilizar autenticação quando configurado o modo *broadcast*”;

ntp.conf
broadcastclient

Quadro 23. Exemplo de modo cliente *broadcast* NTPv3. Adaptação: (DEETHS, 2001b).

ntp.conf
multicastclient

Quadro 24. Exemplo de modo cliente *multicast* NTPv3. Adaptação: (DEETHS, 2001b).

e) Integridade: utilizar autenticação, pois se utiliza de código MAC.

7.2 Possíveis Controles NTP versão 4

Mesmo com a especificação do NTP, versão 4, em fase *work in progress* pelo IETF (2007), o protocolo já está disponível para a sua utilização. Essa versão “introduz novos métodos de descobrir os servidores e, automaticamente, selecionar o mais preciso entre eles” (MILLS, 2006a, p. 16). Também, uma mudança significativa no serviço de autenticação foi adicionada na nova especificação.

Na configuração do protocolo NTP, versão 3, a autenticação com chave secreta permite aos “dispositivos confiarem em seus parceiros e considerá-los legítimos” (RYBACZYK, 2005, p. 83). Porém, há uma deficiência na distribuição e no armazenamento seguro dessas chaves. Rybaczyk (2005) afirma que:

> Para a configuração de chave criptográfica privada ser efetiva e não oferecer simplesmente uma falsa sensação de segurança aos administradores, a chave deve ser entregue de forma segura para cada dispositivo participante e, subseqüentemente, ser armazenada de forma segura. (RYBACZYK, 2005, p.84).

O protocolo NTP, versão 4, suporta a mesma criptografia simétrica para manter compatibilidade com a versão 3. Adicionalmente, oferece uma segurança mais robusta através de um novo protocolo denominado *Autokey*. Essa solução endereça, principalmente, a questão de distribuição das chaves privadas.

O Quadro 25 resume os controles existentes no NTP, versão 4, descritos com mais detalhes logo abaixo:

Controles	
Serviços	**Mecanismos**
Autenticação	Criptografia Simétrica ou Assimétrica
Confiabilidade	Utilizar a relação 3m+1
Controle de acesso	Restrição de endereço IP do parceiro Comando *Discard* Comando *Restrict*
Disponibilidade	Através do algoritmo de *clustering* e pacote KoD
Integridade	*Message Digest* – MD5 ou modo DES-CBC e *Autokey*
Irretratabilidade	Assinatura Digital

Quadro 25. Mecanismos existentes no NTPv4.

7.2.1 Controles em modo simétrico ativo e passivo

Os possíveis controles em modo simétrico ativo e passivo são descritos a seguir com alguns exemplos para ilustrar tais controles:

a) Autenticação: além da autenticação com criptografia simétrica descrita na seção 4.1.4, é possível configurar o modo simétrico através do *autokey* descrita na seção 4.2.4. A associação é iniciada por qualquer parceiro o qual possui o parâmetro da chave no arquivo “ntp.keys”, conforme exemplo no Quadro 26.

Ntp.conf
peer 192.168.15.15 driftfile /etc/ntp/drift keys /etc/ntp/ntp.keys keydir /usr/local/etc #Esse parâmetro é uma linha crypto privatekey /etc/ntp/ntpkey publickey /usr/local/etc/ntpkey_peer-1.example.org dh /usr/local/etc/ntpkey_dh leap /usr/local/etc/ntp_leap

Quadro 26. Exemplo modo parceiro NTPv4. Adaptação: (PALKO, 2001).

b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo

de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;

c) Controle de acesso: restringir o acesso através dos parâmetros do comando *restrict* conforme seção 4.2.7. Além disso, limitar o acesso do parceiro através do endereço IP. Parâmetros recomendados: *default, ignore, server, nomodify, nopeer, noquery, notrap e notrust;*
d) Disponibilidade: igualmente ao protocolo NTP, versão 3, são recomendados mais de 4 servidores. Também, utilizar o serviço de autenticação;
e) Integridade: utilizar o serviço de autenticação *Autokey* descrito no item “a” desta seção;
f) Irretratabilidade: é possível utilizar um dos esquemas de identidade da seção 4.2.11 para garantir a identidade do parceiro.

7.2.2 Controles em modo cliente/servidor

Os possíveis controles em modo cliente/servidor são descritos a seguir com alguns exemplos para ilustrar tais controles:

a) Autenticação: de maneira idêntica ao NTP, versão 3, a associação é iniciada pelo cliente que possui a configuração da chave secreta. Porém, no protocolo NTP, versão 4, é possível utilizar uma chave de sessão denominada *autokey* conforme exemplo no Quadro 27.

ntp.conf
server 192.168.10.20 autokey server 192.168.11.21 autokey driftfile /etc/ntp/drift keys /etc/ntp/ntp.keys #Esse parâmetro é uma linha crypto privatekey /etc/ntp/ntpkey publickey /usr/local/etc/ntpkey_client.example.org dh /usr/local/etc/ntpkey_dh leap /usr/local/etc/ntp_leap

Quadro 27. Exemplo modo cliente NTPv4. Adaptação: (PALKO, 2001).

b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;
c) Controle de Acesso: igualmente ao NTP, versão 3, porém com a possibilidade de utilizar o parâmetro *notrust* do comando *restrict,* é possível trocar

mensagem autenticada somente;

d) Disponibilidade: a disponibilidade do protocolo NTP, versão 4 é mais robusta se utilizado o serviço de KoD, descrito na seção 4.2.10, que possibilita limitar e bloquear o acesso de um cliente com excesso de requisições;
e) Integridade: utilizar o serviço de autenticação *autokey* descrito no item “a” desta seção;
f) Irretratabilidade: é possível utilizar um dos esquemas de identidade da seção 4.2.11 para garantir a identidade do parceiro.

7.2.3 Controles em modo *broadcast* e *multicast*

Os possíveis controles em modo *broadcast* e *multicast* são descritos a seguir:

a) Autenticação: idêntico ao protocolo NTP, versão 3, a associação é iniciada pelo servidor *broadcast*, que possui a especificação da chave secreta em autenticação simétrica. É possível ainda utilizar o *autokey*;
b) Confiabilidade: utilizar mais de quatro servidores redundantes pois o algoritmo de *cluster* do protocolo possui contramedidas próprias para eliminar um servidor de tempo impreciso;
c) Controle de acesso: inexistente;
d) Disponibilidade: de maneira idêntica ao NTP, versão 3, um cliente sincroniza com qualquer servidor nesse modo de operação. Assim, é importante utilizar autenticação quando configurado o modo *broadcast* segundo Deeths (2001b);
e) Integridade: utilizar o serviço de autenticação *autokey* descrito no item “a” da seção 7.2.2.

7.3 Possíveis Controles SNTP versão 4

O protocolo SNTP suporta os mesmos controles do protocolo NTP, versão 4, exceto o serviço de disponibilidade que apresenta uma restrição por parte do modo de operação simétrico, esse não disponível nesse protocolo.

O Quadro 28 resume os controles existentes no SNTP, que são descritos com mais detalhes logo abaixo:

Controles	
Serviços	**Mecanismos**
Autenticação	Criptografia Simétrica ou Assimétrica
Confiabilidade	Utilizar a relação 3m+1
Controle de acesso	Restrição de endereço IP do parceiro Comando *Discard* Comando *Restrict*
Disponibilidade	Restrito no uso de servidores individuais pois não oferece o modo de operação simétrico
Integridade	*Message Digest* – MD5 ou modo DES-CBC e *Autokey*
Irretratabilidade	Assinatura Digital

Quadro 28. Mecanismos existentes no SNTPv4.

Os controles do SNTP são os mesmos do NTP, versão 4, tanto para o modo de operação cliente/servidor quanto para o modo *broadcast*/*multicast*. Assim, serão utilizados os controles nas seções pertinentes às recomendações.

7.4 Possíveis Controles PTP

A especificação (EIDSON; FISHER; WHITE, 2002) define o protocolo PTP para sincronização na ordem abaixo de microssegundo, porém não estão definidos os mecanismos de segurança do protocolo (KONSTANTIN; TSANG, 2006).

Uma análise de segurança das fragilidades do protocolo foi realizada por Konstantin e Tsang (2006) para sugerir as contramedidas de segurança do protocolo e atentar sua importância à comunidade. Como resultado, “fornecer a assistência aos desenvolvedores e usuários da tecnologia baseada no PTP em identificar os

requisitos de segurança e o desenvolvimento dos mecanismos de segurança necessários para o protocolo” (KONSTANTIN; TSANG, 2006, p. 2).

O Quadro 29 resume as recomendações de segurança para o protocolo PTP baseado na análise (KONSTANTIN; TSANG, 2006).

Controles	
Serviços	**Mecanismos Recomendados**
Autenticação	Autenticação centralizada ou encadeada e *port-security*
Confidencialidade	Não identificado como necessário
Controle de acesso	Autenticação centralizada ou encadeada e *port-security*
Disponibilidade	Autenticidade das mensagens, criptografia e limitação através de *port-security*
Integridade	Criptografia e limitação através de *port-security*

Quadro 29. Recomendações para o PTP. Fonte: (KONSTANTIN; TSANG, 2006).

O resultado apresentado por Konstantin e Tsang (2006) sugere que o protocolo PTP é carente para garantir a integridade da mensagem transmitida e validar a autenticidade do remetente, porque falha contra ameaças de modificação, personificação, atraso, reenvio e negação de serviço.

8 ANÁLISE DE RISCO DOS CENÁRIOS DE SINCRONIZAÇÃO DE TEMPO

Através do processo de determinação dos riscos do capítulo 6, foi possível identificar as ameaças e vulnerabilidades dos cenários de sincronização de tempo e determinar o grau de risco nos ambientes de redes locais e de longa distância. Os possíveis controles dos protocolos de tempo, descritos no capítulo 7, serão a base para a seleção dos controles indicados no processo de mitigação dos riscos nesse capítulo.

Em cada cenário analisado são tratados três fatores: a análise de risco, os possíveis controles existentes e, dentre eles, a seleção dos controles para mitigar os riscos. Tais fatores, descritos nas seções subseqüentes, serão objetos para a identificação e recomendações finais.

Cada cenário pode exigir controles específicos para determinadas vulnerabilidades presentes. Tais controles podem ser suportados intrinsicamente pelo protocolo de tempo utilizado. Também, podem existir e depender de uma configuração específica. Ou, pode não ser suportado pelo protocolo de tempo utilizado.

Dessa forma, esse capítulo consolida as informações sobre os protocolos de tempo, os cenários de sincronização de tempo, os riscos e os controles para indicar uma solução de instalação segura ao serviço de sincronização de tempo.

8.1 Análise de Risco do Cenário de Sincronização de Tempo entre Servidores em Rede Local

A Figura 40 ilustra o cenário de sincronização entre servidores de tempo utilizando um ambiente de rede local. Nesse cenário, o principal objetivo é fornecer o tempo de uma referência local aos estratos mais altos.

O modo de operação típico é o cliente/servidor ou mestre/escravo. O servidor de tempo, representado no estrato “n”, é a referência de tempo utilizando seu relógio local. Ele fornece mensagens para a sincronização aos demais servidores

localizados no estrato “n+1”. Esses servidores podem sincronizar outros servidores e clientes finais posteriormente.

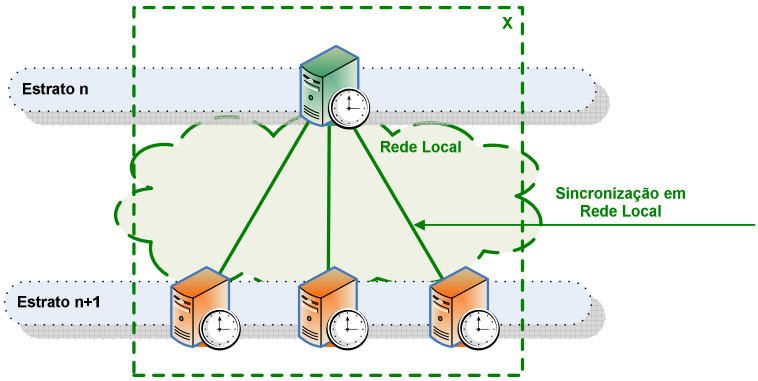

Figura 40. Exemplo de sincronização de tempo entre servidores em rede local.

8.1.1 Análise de Risco

Todos os servidores são tratados igualmente na análise de risco, pois os dispositivos devem possuir os mesmos controles para a mitigação de risco. A fim de atender o objetivo de sincronia segura na hierarquia de tempo.

O Quadro 30 resume a análise de risco dos servidores de tempo desse cenário.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco	Mitigação
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO	OPCIONAL
	Ausência de enlace de comunicação redundante	BAIXA	MÉDIO	BAIXO	OPCIONAL
	Alta latência no enlace de comunicação	BAIXA	MÉDIO	BAIXO	OPCIONAL
	Ausência de proteção contra negação do serviço de tempo	MÉDIA	MÉDIO	MÉDIO	RECOMENDADA
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO	OBRIGATÓRIA

Quadro 30. Análise de risco para sincronização de tempo entre servidores em rede local.

8.1.2 Relação dos Possíveis Controles

Os possíveis controles são listados no Quadro 31 e representam os serviços e mecanismos existentes nos protocolos de tempo analisados.

Ameaças Específicas	Vulnerabilidades	Risco	Controles Possíveis				
			Serviço	Mecanismos			
				NTPv3	NTPv4	SNTPv4	PTP
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de enlace de comunicação redundante	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Alta latência no enlace de comunicação	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de proteção contra negação do serviço de tempo	MÉDIO	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD	Inexistente
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Confiabilidade	3m+1	3m+1	3m+1	Inexistente

Quadro 31. Controles possíveis na sincronização de tempo entre servidores em rede local.

8.1.3 Seleção dos Possíveis Controles

Para a mitigação dos riscos, serão selecionados os controles apropriados através de um critério de seleção dos controles de segurança. Pressupõe a mitigação "obrigatória" como o mínimo fator de escolha do protocolo de tempo. Também, a mitigação "recomendada" elimina ou reduz o risco do par de ameaças e vulnerabilidade analisado.

Os protocolos selecionados foram: protocolo NTP, versão 3, NTP, versão 4, e o SNTP, pois atendem a mitigação obrigatória através de controles pertinentes ao cenário de sincronismo entre servidores de tempo, conforme Quadro 32.

O protocolo PTP, ainda, não possui controles para a mitigação "obrigatória". Dessa forma, não foi um protocolo selecionado.

Ameaças Específicas	Vulnerabilidades	Mitigação	Controles Selecionados			
			Serviço	Mecanismos		
				NTPv3	NTPv4	SNTPv4
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Disponibilidade	Redundância	Redundância	Redundância
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de enlace de comunicação redundante	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Alta latência no enlace de comunicação	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de proteção contra negação do serviço de tempo	RECOMENDADA	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Confiabilidade	3m+1	3m+1	3m+1

Quadro 32. Controles selecionados para sincronização de tempo entre servidores em rede local.

8.1.4 Resultados

Nesse cenário de sincronização de tempo, com o típico modo de operação cliente/servidor devido à disposição dos estratos, conclui-se o uso obrigatório da autenticação através do uso de chave secreta presente no protocolo NTP, versão 3. Ou, caso a escolha seja o uso dos protocolos NTP, versão 4, e SNTP, a autenticação deve ser configurada através do protocolo *Autokey* que utiliza esquema de chave pública.

Também, foi identificado o uso obrigatório do controle de acesso através da restrição do endereço IP dos parceiros e dos parâmetros: *Default, Ignore, Server, Nomodify, Nopeer, Noquery* e *Notrap* do comando *Restrict*.

A ameaça de subversão de um servidor legítimo obriga o uso de servidores redundantes. A instalação de quatro ou mais servidores de referência de tempo, conforme Figura 41 é o modelo mais adequado. Esse novo cenário de sincronização entre servidores de tempo garante uma estrutura de sincronização robusta, garantindo a confiabilidade e disponibilidade do serviço.

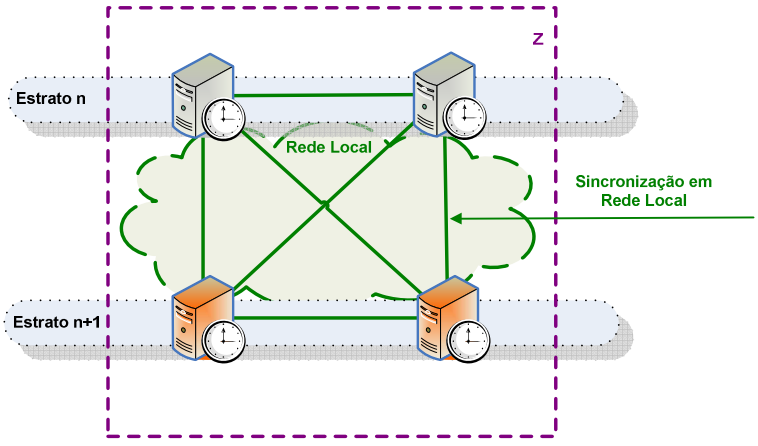

Figura 41. Sincronização de tempo entre servidores com redundância.

Por fim, para a ameaça de sobrecarga do serviço, a disponibilidade é atendida com uma chave secreta no protocolo NTP, versão 3, e com o *Autokey* nos protocolos NTP, versão 4, e SNTP. Além disso, é recomendada a configuração do comando KoD presente nesses dois protocolos a fim de limitar a ação de sobrecarga indevida do parceiro.

8.2 Análise de Risco do Cenário de Sincronização de Tempo entre Servidores em Rede de Longa Distância

A Figura 42 exemplifica um cenário de sincronização entre servidores de tempo utilizando um ambiente de rede de longa distância. Nesse cenário, o principal objetivo é fornecer a referência de tempo aos estratos mais altos.

O modo de operação típico é o cliente/servidor. Um servidor de tempo localizado, por exemplo, em escritório central sincroniza os servidores do próximo estrato localizados, por exemplo, em escritórios filiais através de uma rede de longa distância do tipo *Frame Relay* ou MPLS. Esse servidor é a referência de tempo local, utilizando seu relógio, para os servidores participantes no serviço de sincronismo. Por fim, os servidores localizados nas filiais, nesse exemplo, podem sincronizar os clientes finais.

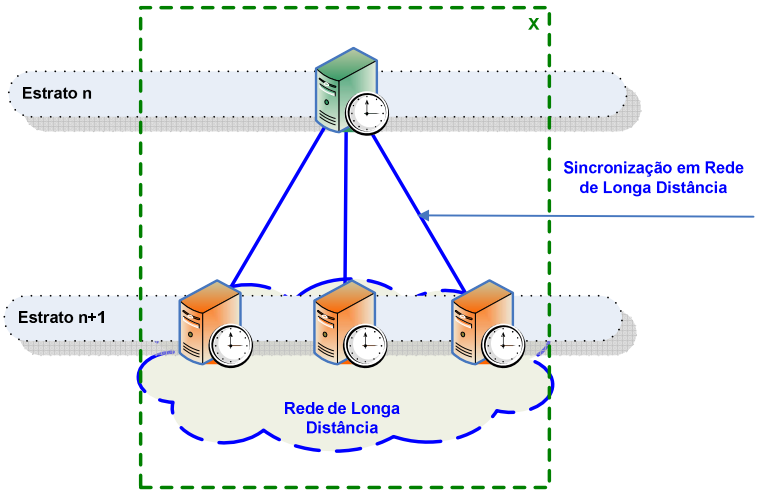

Figura 42. Sincronização de tempo entre servidores em rede de longa distância.

8.2.1 Análise de Risco

De forma idêntica ao cenário anterior, a análise de risco considera todos os servidores de tempo. O Quadro 33 descreve o resumo dessa análise.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco	Mitigação
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	ALTA	ALTO	ALTO	OBRIGATÓRIA
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO	OPCIONAL
	Ausência de enlace de comunicação redundante	ALTA	MÉDIO	ALTO	OBRIGATÓRIA
	Alta latência no enlace de comunicação	ALTA	MÉDIO	ALTO	OBRIGATÓRIA
	Ausência de proteção contra negação do serviço de tempo	ALTA	MÉDIO	ALTO	OBRIGATÓRIA
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	ALTA	ALTO	ALTO	OBRIGATÓRIA

Quadro 33. Análise de risco para sincronização de tempo entre servidores em rede de longa distância.

8.2.2 Relação dos Possíveis Controles

Os possíveis controles são listados no Quadro 34 e representam os serviços e mecanismos existentes nos protocolos de tempo analisados.

Ameaças Específicas	Vulnerabilidades	Risco	Controles Possíveis				
			Serviço	Mecanismos			
				NTPv3	NTPv4	SNTPv4	PTP
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de enlace de comunicação redundante	ALTO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Alta latência no enlace de comunicação	ALTO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de proteção contra negação do serviço de tempo	ALTO	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD	Inexistente
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Confiabilidade	3m+1	3m+1	3m+1	Inexistente

Quadro 34. Controles possíveis na sincronização de tempo entre servidores em rede de longa distância.

8.2.3 Seleção dos Possíveis Controles

Foram utilizados os mesmos critérios do cenário de sincronização entre servidores de tempo em rede local para a seleção dos controles de segurança. Ou seja, a mitigação “obrigatória” é o mínimo fator para a escolha dos protocolos de tempo e seus controles. Dessa maneira, o Quadro 35 apresenta os protocolos e os controles selecionados.

Ameaças Específicas	Vulnerabilidades	Mitigação	Controles Selecionados			
			Serviço	Mecanismos		
				NTPv3	NTPv4	SNTPv4
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Disponibilidade	Redundância	Redundância	Redundância
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de enlace de comunicação redundante	OBRIGATÓRIA	Disponibilidade	Redundância	Redundância	Redundância
	Alta latência no enlace de comunicação	OBRIGATÓRIA	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de proteção contra negação do serviço de tempo	OBRIGATÓRIA	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict

Quadro 35. Controles selecionados para sincronização de tempo entre servidores em rede de longa distância.

Nota-se que a presença de linhas de comunicação de longa distância eleva o grau de risco de alguma vulnerabilidades. Conseqüentemente, o grau de mitigação também muda nesse caso.

8.2.4 Resultados

Nesse cenário, as recomendações são mais rígidas ao cenário de sincronização entre servidores de tempo em ambiente de rede local. Ou seja, conclui-se que é obrigatório o uso da autenticação através do uso de chave secreta no protocolo NTP, versão 3. Caso sejam utilizados os protocolos NTP, versão 4, e SNTP, a autenticação deve ser realizada através do *Autokey*.

Além disso, o controle de acesso é uso obrigatório com a restrição dos endereços IP e os parâmetros do comando *Restrict*: *Default, Ignore, Server, Nomodify, Nopeer, Noquery* e *Notrap.*

Também, vulnerabilidades relacionadas com a disponibilidade obrigam a instalação de quatro ou mais servidores de referência de tempo, conforme Figura 43. Esse novo cenário de sincronização entre servidores de tempo evitam interrupções do serviço. Considerar dois ou mais servidores de tempo em cada localidade física evita a vulnerabilidade de ausência de de servidor redundante.

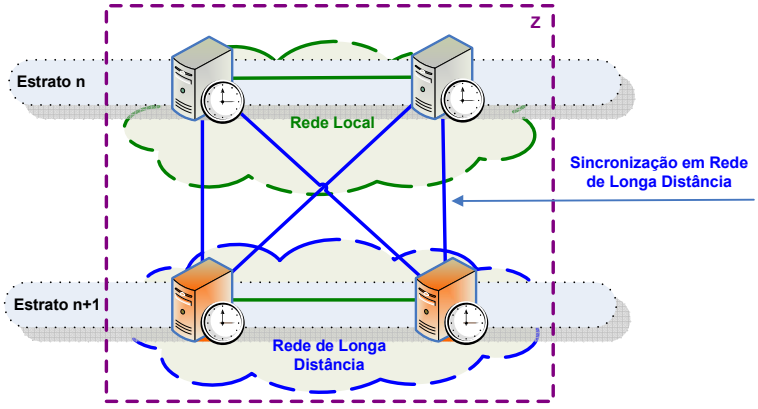

Figura 43. Sincronização de tempo com redundância em rede de longa distância.

Por fim, para a ameaça de sobrecarga do serviço, a disponibilidade é atendida com uma chave secreta no protocolo NTP, versão 3, e com o *Autokey* nos protocolos NTP, versão 4, e SNTP. Além disso, é recomendada o uso obrigatório da configuração do comando KoD presentes nos protocolos NTP, versão 4, e SNTP para limitar a ação de sobrecarga indevida do parceiro.

8.3 Análise de Risco do Cenário de Sincronização de Tempo entre Servidor e Cliente em Rede Local

A Figura 44 ilustra o cenário de sincronização entre um servidor de tempo e o cliente final utilizando um ambiente de rede local.

Nesse cenário é possível o modo de operação cliente/servidor, *broadcast* ou *multicast* e o *manycast*. Normalmente, quando há um número grande de clientes, um servidor, em modo *broadcast* ou *multicast*, sincroniza os clientes finais. Também, é possível configurar os clientes em modo *manycast* quando utilizado os protocolos NTP, versão 4, e SNTP. Nesse exemplo, o servidor de tempo localizado no estrato "n" fornece a sincronização para os clientes que são dependentes exclusivamente desse servidor.

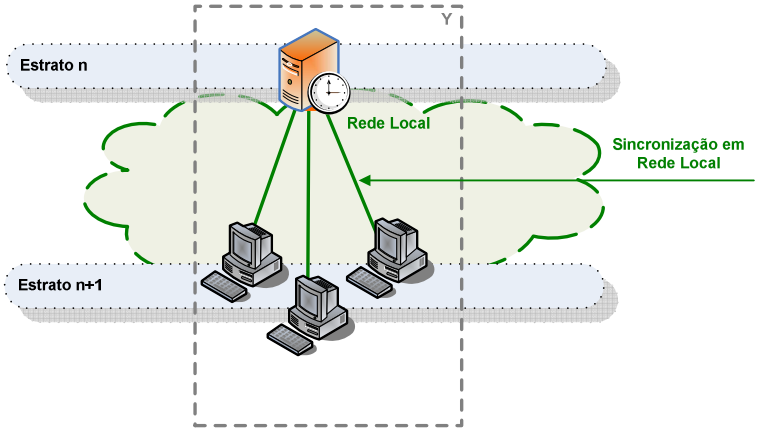

Figura 44. Sincronização de tempo entre servidores e clientes.

8.3.1 Análise de Risco

O principal dispositivo é o servidor de tempo, pois, ele é a referência de tempo para os clientes finais e o ponto de falha mais crítico. A análise de risco foi feita sob a visão de um cliente final.

Dessa maneira, a análise de risco é sobre esse dispositivo, conforme Quadro 36.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco	Mitigação
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO	RECOMENDADA
	Ausência de identificação do servidor de tempo	MÉDIA	MÉDIO	MÉDIO	RECOMENDADA
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO	OPCIONAL
	Ausência de enlace de comunicação redundante	BAIXA	BAIXO	BAIXO	OPCIONAL
	Alta latência no enlace de comunicação	BAIXA	BAIXO	BAIXO	OPCIONAL
	Ausência de proteção contra negação do serviço de tempo	MÉDIA	BAIXO	BAIXO	OPCIONAL
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO	OBRIGATÓRIA

Quadro 36. Análise de risco para sincronização de tempo entre servidores e clientes.

8.3.2 Relação dos Possíveis Controles

Os possíveis controles são listados no Quadro 37 e representam os serviços e mecanismos existentes nos protocolos de tempo analisados.

Ameaças Específicas	Vulnerabilidades	Risco	Controles Possíveis				
			Serviço	Mecanismos			
				NTPv3	NTPv4	SNTPv4	PTP
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	MÉDIO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de identificação do servidor de tempo	MÉDIO	Identificação	chave secreta	PC, TC, IFF, GC E MV	PC, TC, IFF, GC E MV	Inexistente
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de enlace de comunicação redundante	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Alta latência no enlace de comunicação	BAIXO	Disponibilidade	Redundância	Redundância	Redundância	Inexistente
	Ausência de proteção contra negação do serviço de tempo	BAIXO	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD	Inexistente
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Confiabilidade	3m+1	3m+1	3m+1	Inexistente

Quadro 37. Controles possíveis na sincronização de tempo entre servidores e clientes.

8.3.3 Seleção dos Possíveis Controles

Também, nesse cenário, foi utilizado o mesmo critério dos cenários anteriores para a seleção dos controles de segurança que estão descritos no Quadro 38.

Ameaças Específicas	Vulnerabilidades	Mitigação	Controles Selecionados			
			Serviço	Mecanismos		
				NTPv3	NTPv4	SNTPv4
Desvio significativo de sincronismo em um cliente	Ausência de autenticação do servidor de tempo	RECOMENDADA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de identificação do servidor de tempo	RECOMENDADA	Identificação	chave secreta	PC	PC
Perda de sincronismo em um cliente	Ausência de servidor de tempo redundante	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de enlace de comunicação redundante	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Alta latência no enlace de comunicação	OPCIONAL	Disponibilidade	Redundância	Redundância	Redundância
	Ausência de proteção contra negação do serviço de tempo	OPCIONAL	Disponibilidade	chave secreta	Chave pública e KoD	Chave pública e KoD
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Confiabilidade	3m+1	3m+1	3m+1

Quadro 38. Controles selecionados para sincronização de tempo entre servidores e clientes.

8.3.4 Resultados

Nesse cenário, conclui-se o uso obrigatório da autenticação através do uso de chave secreta no protocolo NTP, versão 3. Caso sejam utilizados os protocolos NTP, versão 4, e SNTP, a autenticação deve ser realizada através do *Autokey*. Principalmente, devido a possibilidade de explorar a ameaça de subversão de um servidor legítimo.

É recomendado o uso do esquema de identificação nos protocolos NTP, versão 4, e SNTP para o modo de operação *manycast,* pois, nesse modo de operação, os clientes desconhecem a identidade dos servidores autorizados de forma antecipada.

As vulnerabilidades: ausência de enlace de comunicação redundante e alta latência no enlace de comunicação entre os servidores, são minimizadas com a instalação de dois ou mais servidores de referência de tempo. Porém, a ameaça de subversão de um servidor legítimo obriga o uso de quatro ou mais servidores de tempo, conforme Figura 45. Esse novo cenário de sincronização entre servidores de tempo garante a confiabilidade do serviço e a sua disponibilidade.

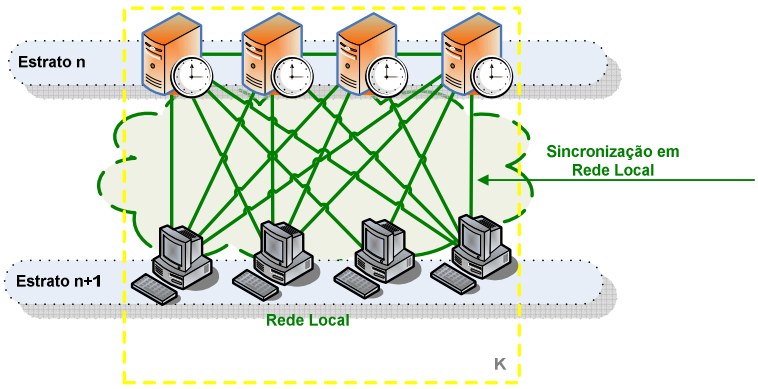

Figura 45. Sincronização de tempo entre servidores e clientes com redundância em rede local.

Por fim, para a ameaça de sobrecarga do serviço, a disponibilidade é atendida com uma chave secreta no protocolo NTP, versão 3, e com o *Autokey* nos protocolos NTP, versão 4, e SNTP. Além disso, é opcional a configuração do comando KoD presentes nos protocolos NTP, versão 4, e SNTP, para limitar a ação de sobrecarga indevida do parceiro.

8.4 Análise de Risco do Cenário de Sincronização de Tempo entre Servidores Simétrico em Rede Local

A Figura 46 ilustra o cenário de sincronização entre servidores de tempo utilizando um ambiente de rede local.

Nesse exemplo, um típico modo de operação é o da associação simétrica. Há um servidor primário ativo que sincroniza o tempo com um servidor primário passivo. Isso pode ser configurado na família de protocolos NTP, normalmente, no mesmo estrato para garantir uma referência de tempo precisa aos demais participantes do serviço de sincronização de tempo.

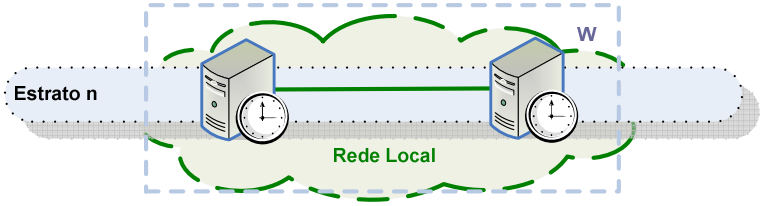

Figura 46. Sincronização de tempo entre servidores em modo simétrico.

8.4.1 Análise de Risco

Os servidores de tempo são tratados igualmente na análise de risco, pois devem possuir os mesmos controles para a mitigação de risco, conforme Quadro 39.

Ameaças Específicas	Vulnerabilidades	Prob.	Impacto	Risco	Mitigação
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXA	BAIXO	BAIXO	OPCIONAL
	Ausência de enlace de comunicação redundante	BAIXA	MÉDIO	BAIXO	OPCIONAL
	Alta latência no enlace de comunicação	BAIXA	MÉDIO	BAIXO	OPCIONAL
	Ausência de proteção contra negação do serviço de tempo	MÉDIA	MÉDIO	MÉDIO	RECOMENDADA
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	MÉDIA	ALTO	ALTO	OBRIGATÓRIA
	Ausência de servidor de tempo redundante	MÉDIA	ALTO	ALTO	OBRIGATÓRIA

Quadro 39. Análise de risco para sincronização de tempo entre servidores em modo simétrico.

8.4.2 Relação dos Possíveis Controles

Os possíveis controles são listados no Quadro 40, bem como os protocolos de tempo.

Ameaças Específicas	Vulnerabilidades	Risco	Controles Possíveis				
			Serviço	Mecanismos			
				NTPv3	NTPv4	SNTPv4	PTP
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	Inexistente	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Disponibilidade	Redundância	Redundância	Inexistente	Inexistente
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	BAIXO	Disponibilidade	Redundância	Redundância	Inexistente	Inexistente
	Ausência de enlace de comunicação redundante	BAIXO	Disponibilidade	Redundância	Redundância	Inexistente	Inexistente
	Alta latência no enlace de comunicação	BAIXO	Disponibilidade	Redundância	Redundância	Inexistente	Inexistente
	Ausência de proteção contra negação do serviço de tempo	MÉDIO	Disponibilidade	chave secreta	Chave pública e KoD	Inexistente	Inexistente
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	ALTO	Autenticação	chave secreta	chave secreta ou pública	Inexistente	Inexistente
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict	Inexistente	Inexistente
	Ausência de servidor de tempo redundante	ALTO	Confiabilidade	3m+1	3m+1	Inexistente	Inexistente

Quadro 40. Controles possíveis na sincronização de tempo entre servidores em modo simétrico.

Nesse modo, o protocolo SNTP não tem a opção de configuração simétrica.

8.4.3 Seleção dos Possíveis Controles

Para atender os riscos com mitigação “obrigatória”, foram selecionados os protocolos NTP, versão 3, NTP, versão 4, conforme Quadro 41, pois possuem controles pertinentes a esse cenário de sincronismo entre servidores de tempo no modo simétrico.

Ameaças Específicas	Vulnerabilidades	Mitigação	Controles Selecionados		
			Serviço	Mecanismos	
				NTPv3	NTPv4
Desvio significativo de sincronismo em um servidor	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Disponibilidade	Redundância	Redundância
Perda de sincronismo em um servidor	Ausência de servidor de tempo redundante	OPCIONAL	Disponibilidade	Redundância	Redundância
	Ausência de enlace de comunicação redundante	OPCIONAL	Disponibilidade	Redundância	Redundância
	Alta latência no enlace de comunicação	OPCIONAL	Disponibilidade	Redundância	Redundância
	Ausência de proteção contra negação do serviço de tempo	RECOMENDADA	Disponibilidade	chave secreta	Chave pública e KoD
Subversão de um servidor legítimo	Ausência de autenticação do servidor de tempo	OBRIGATÓRIA	Autenticação	chave secreta	chave secreta ou pública
			Controle de Acesso	Restrição IP e Restrict	Restrição IP e Restrict
	Ausência de servidor de tempo redundante	OBRIGATÓRIA	Confiabilidade	3m+1	3m+1

Quadro 41. Controles selecionados para sincronização de tempo entre servidores em modo simétrico.

8.4.4 Resultados

Nesse cenário conclui-se que é obrigatório o uso da autenticação através do uso de chave secreta no protocolo NTP, versão 3. Caso seja utilizado o protocolo NTP, versão 4, a autenticação deve ser realizada através do *Autokey*. Também, o controle de acesso é de uso obrigatório com a restrição dos endereços IP e os parâmetros do comando *Restrict*: *Default, Ignore, Server, Nomodify, Nopeer, Noquery* e *Notrap.*

Os controles para as vulnerabilidades ausência de enlace de comunicação redundante e alta latência no enlace de comunicação entre os servidores são opcionais. Porém, a ameaça de subversão de um servidor legítimo obriga o uso de quatro ou mais servidores de tempo para garantir a confiabilidade do serviço.

Por fim, para a ameaça de sobrecarga do serviço, a disponibilidade é recomendada com o uso de chave secreta no protocolo NTP, versão 3, e com o *Autokey* no protocolo NTP, versão 4.

8.5 Conclusão dos Resultados

Na análise de risco de dois cenários de sincronização de tempo em rede local:

- Cenário de Sincronização de Tempo entre Servidores;
- Cenário de Sincronização de Tempo entre Servidores Simétrico.

Foi destaque o uso “obrigatório” dos serviços de segurança: autenticação, o controle de acesso e a confiabilidade, devido a ameaça de subversão de um servidor legítimo e a possibilidade de desvio significativo de sincronismo de um servidor de tempo terem contribuído com os maiores riscos. A ausência de proteção contra negação do serviço de tempo teve grau “recomendado” para o uso dos controles apropriados. Por último, as vulnerabilidades: ausência de enlace de comunicação redundante e alta latência no enlace de comunicação entre os servidores, tiveram o grau “opcional” para a mitigação de risco.

No terceiro cenário de sincronização de tempo em rede local:

- Cenário de Sincronização de Tempo entre servidor e cliente.

Os serviços de segurança de uso “obrigatório” identificados foram: a autenticação, o controle de acesso e a confiabilidade, principalmente, devido a ameaça de subversão de um servidor legítimo ter contribuído com maior risco. A vulnerabilidade de ausência de identificação do servidor de tempo foi classificada de risco médio, sendo assim “recomendada” a mitigação de risco com o serviço de identificação do servidor. As demais vulnerabilidades tiveram a classificação de risco baixo, sendo assim “opcional” o uso dos controles de segurança.

De maneira geral, na análise em ambiente de rede local, o serviço de segurança confiabilidade está associado à ameaça de subversão de um servidor legítimo em rede local e a vulnerabilidade ausência de servidor de tempo redundante exige mais de quatro servidores legítimos através da relação 3m+1. No Quadro 42, esta vulnerabilidade é apresentada de forma separada justamente para explicitar o controle relativo ao serviço de confiabilidade.

Na análise de risco do cenário de sincronização de tempo em rede de longa distância:

- Cenário de Sincronização de Tempo entre Servidores

As ameaças de desvio significativo do sincronismo do servidor de tempo e a perda do sincronismo de um servidor contribuíram com risco alto na análise desse cenário. Assim, os serviços de segurança de uso “obrigatório” são: autenticação, o controle de acesso e a disponibilidade. O uso de servidor redundante para a ameaça de perda de sincronismo teve indicação “opcional”, mas seu risco tem mitigação através do risco alto pelas ameaças descritas anteriormente.

Por fim, os protocolos de tempo selecionados que atendem a mitigação de risco com controles adequados são os protocolos NTP, versão 3, NTP, versão 4, e o SNTP. Este último não é aplicável no cenário de sincronização entre servidores de tempo no modo simétrico em rede local. O protocolo PTP, ainda em aprovação, não há controles intrínsicos especificados para a instalação de sincronização de tempo visando a proteção das ameaças deste trabalho.

A consolidação deste trabalho é apresentada no Quadro 42, onde os controles para uma instalação segura do serviço de sincronização de tempo estão indicados da seguinte maneira: em vermelho o uso dos controles “obrigatórios”, em amarelo os controles “recomendados” e os verdes os controles “opcionais”.

Vulnerabilidade	Sincronização entre servidores de tempo						Sincronização cliente / servidor (*broadcast*, *multicast* e *manycast*)			Sincronização entre servidores de tempo simétrico		Cenário
	Rede Local			Rede Longa Distância			Rede Local			Rede Local		Ambiente de Rede
	NTPv3	NTPv4	SNTPv4	NTPv3	NTPv4	SNTPv4	NTPv3	NTPv4	SNTPv4	NTPv3	NTPv4	Protocolos Selecionado
Ausência de autenticação do servidor de tempo	Chave secreta Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Chave secreta Restrição IP e *Restrict*	Chave secreta ou pública Restrição IP e *Restrict*	Controles Selecionados
Ausência de identificação do servidor de tempo	NA			NA			Chave secreta	PC	PC	NA		
Ausência de servidor de tempo redundante (Mais que 2)	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	
Ausência de servidor de tempo redundante (Mais que 4)	3m+1	3m+1	3m+1	NA			3m+1	3m+1	3m+1	3m+1	3m+1	
Alta latência no enlace de comunicação	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	
Ausência de enlace de comunicação redundante	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	Redundância	
Negação do serviço de tempo	Chave secreta	Chave pública e KoD	Chave pública e KoD	Chave secreta	Chave pública e KoD	Chave pública e KoD	Chave secreta	Chave pública e KoD	Chave pública e KoD	Chave secreta	Chave pública e KoD	

Quadro 42. Protocolos e controles selecionados para os cenários de sincronização de tempo.

Controle: Obrigatório Recomendado Opcional NA – Não se aplica

9 CONSIDERAÇÕES FINAIS

A precisão do tempo é uma característica importante na ordem temporal dos eventos em sistemas computacionais distribuídos. Um serviço de sincronização de tempo requer inúmeros controles para um funcionamento adequado e deve oferecer robustez às aplicações que dependem de um tempo preciso e estável.

Um dos principais elementos para o funcionamento desse serviço são os protocolos de tempo e os controles de segurança agregados às suas funcionalidades, pois são protocolos que utilizam os serviços oferecidos pela camada de transporte da pilha TCP/IP e, conseqüentemente, impactados pela suas fragilidades.

Este trabalho foi direcionado a fim de endereçar as questões de segurança do serviço de sincronização de tempo em determinados cenários de uso.

Através de uma análise de risco foi possível selecionar os protocolos de tempo mais apropriados aos cenários de sincronização de tempo. Também, foram identificados e recomendados os possíveis controles que deveriam estar presentes em tais protocolos para a mitigação dos riscos apresentados neste estudo.

Este trabalho apresentou a importância da precisão e exatidão do tempo em sistemas computacionais distribuídos para determinadas aplicações que necessitam do serviço de sincronização do tempo. Também, contribui para o enriquecimento sobre o tema através de recomendações para uma instalação segura considerando alguns riscos em determinados cenários de uso.

9.1 Conclusões

Este trabalho analisou os riscos em determinados cenários de sincronização de tempo para a identificação dos possíveis controles e uma seleção daqueles aplicavéis na mitigação de riscos. Os controles selecionados dos protocolos de tempo foram consolidados a fim de apresentar sua aplicação nos diversos cenários de sincronização e ambiente de rede, além dos modos de operação dos protocolos de tempo.

Tal consolidação, resumida no Quadro 42, beneficia os projetistas e administradores de redes no projeto do serviço de sincronização de tempo. Através de uma abordagem pragmática e sem complexidade, este trabalho colabora na escolha do protocolo de tempo, nos modos de operação e na indicação dos controles obrigatórios, recomentados e opcionais para uma instalação segura. É possível a existência de controles irrelevantes na mitigação de riscos que não foram indicados na consolidação deste trabalho.

Além da instalação padrão do serviço de sincronização de tempo e observando o Quadro 42, nota-se a necessidade de configuração adicional dos controles selecionados nos protocolos de tempo, alguns deles obrigatórios e outros recomendados, para uma operação segura.

De maneira indireta este trabalho contribui para ressaltar a importância de um processo estruturado de análise de risco a fim de identificar as ameaças e vulnerabilidades para determinar os riscos e concluir quais controles são os mais adequados para a mitigação de riscos.

9.2 Contribuições

Este trabalho contribui para ressaltar a importância do sincronismo de tempo seguro em sistemas computacionais distribuídos nas áreas de tecnologia da informação. Outro benefício é determinar alguns cenários de sincronização de tempo sob a ótica da segurança, visando à mitigação dos possíveis riscos.

É, também, uma contribuição do presente trabalho orientar os administradores de redes sobre a importância da utilização de controles existentes nos protocolos de tempo, com o objetivo de proteger e prevenir determinados tipos de ameaças e vulnerabilidades.

De forma mais ampla, este trabalho visou à apresentação da importância da precisão e exatidão do tempo para determinadas aplicações que necessitam de tal serviço.

Assim, o trabalho pode servir como referência para a comunidade de TI sobre os controles necessários para uma instalação e operação segura do serviço de sincronização de tempo.

9.3 Limitações

O serviço de sincronização de tempo é pouco difundido e a literatura existente sobre o tema é dispersa. Apesar dos protocolos para esse serviço existirem há muitos anos, somente a família de protocolos NTP persistiu até os dias atuais. Ademais, pouco têm sido escrito sobre a exatidão de tempo em sistemas computacionais distribuídos e sobre a rastreabilidade a algum órgão brasileiro oficial (Observatório Nacional).

Este estudo aconteceu juntamente com a evolução das especificações dos protocolos SNTP (MILLS, 2006c), versão 4, NTP (BURBANK; et al, 2007), versão 4 e o PTP (EIDSON; FISHER; WHITE, 2002). Os dois últimos ainda em situação de *work in progress* a serem aprovadas pelas entidades IETF e IEEE, respectivamente.

Durante esta pesquisa, foram publicados os únicos livros referentes sobre o tema: (RYBACZYK, 2005), (MILLS, 2006a) e o livro *Measurement, Control, and Communication Using IEEE 1588* disponível em 2006.

Assim, este trabalho também pode ser considerado um ponto de partida para futuros estudos sobre a sincronização de tempo. Seria importante um estudo de caso para analisar a real eficácia dos controles de segurança apresentados neste trabalho, principalmente, após a publicação das referências definitivas.

9.4 Trabalhos Futuros

Alguns temas para trabalhos futuros a serem explorados como continuidade deste trabalho:

a) Controles de segurança dos protocolos de tempo: Um estudo de caso;
b) Criptoanálise dos algoritmos utilizados pelo protocolo *Autokey*;
c) Análise dos Serviço de Segurança utilizando PTP;
d) Viabilidade do serviço TLS/SSL para protocolos de tempo;
e) Impacto de um serviço de DNS inseguro nos protocolos de tempo.

REFERÊNCIAS

ALLAN, D.; ASHBY, N.; HODGE, C. **The science of timekeeping:** Application Note 1289. EUA: Hewlett Packard,1997. Disponível em <http://www.allanstime.com/Publications/DWA/Science_Timekeeping/TheScienceOfTimekeeping.pdf>. Acesso em 26 de maio de 2007.

BIPM - BUREAU INTERNATION DES POIDS ET MESURES. **Approximation to UTC**. França: BIPM, 2006. Disponível em <http://www1.bipm.org/en/scientific/tai/time_server.html>. Acesso em 26 de maio de 2007.

BURBANK, J. et al.. **Network Time Protocol Version 4 protocol and algorithms specification:** draft-ietf-ntp-ntpv4-proto-04. IETF, 2007. Disponível em <http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-proto-04>. Acesso em 26 de maio de 2007.

DEERING, S. **Host extensions for IP multicasting**. IETF, 1989. Disponível em <http://www.ietf.org/rfc/rfc1112.txt>. Acesso em 26 de maio de 2007.

DEERING, S.; HIDEN, R**. Internet Protocol, Version 6 (IPv6) specification**. IETF: 1998. Disponível em <http://www.ietf.org/rfc/rfc2460.txt>. Acesso em 26 de maio de 2007.

DEETHS, D.; BRUNETT, G. **Using NTP to control and synchronize system clocks – part I.** Introduction to NTP. Sun BluePrints, 2001a. Disponível em <http://www.sun.com/blueprints/0701/NTP.pdf>. Acesso em 26 de maio de 2007.

DEETHS, D.; BRUNETT, G. **Using NTP to control and synchronize system clocks – part II.** Basic NTP administration and architecture. Sun BluePrints, 2001b. Disponível em <http://www.sun.com/blueprints/0801/NTPpt2.pdf>. Acesso em 26 de maio de 2007.

EIDSON, J.; FISHER, M.; WHITE, J. **IEEE-1588 standard for a precision clock synchronization protocol for networked measurement and control systems**. IEEE, 2002. 34th Annual Precise Time and Time Interval (PTTI) Meeting.

FEDERAL INFORMATION PROCESSING STANDARDS. **DES modes of operation:** Publication 81. NIST, 1980. Disponível em <http://www.itl.nist.gov/fipspubs/fip81.htm>. Acesso em 26 de maio de 2007.

GUREWITZ, O.; CIDON, I.; SIDI, M. **Network time synchronization using clock offset optimization**. IEEE, 2003. Proceeding of the 11th IEEE International Conference on Network Protocols (ICNP'03) 1092-1648/03

GUSELLA, R.; ZATTI, S. **The accuracy of the clock synchronization achieved by TEMPO in Berkeley UNIX 4.3BSD. IEEE Transactions on Software Engineering, IEEE, v. 15, n. 7**, Jul. 1989. Disponível em <http://digitalassets.lib.berkeley.edu/techreports/ucb/text/CSD-87-337.pdf>. Acesso em 26 de maio de 2007.

INMETRO. **Vocabulário internacional de termos fundamentais e gerais de metrologia:** VIM**.** Rio de Janeiro: INMETRO, 1995. Disponível em <http://www.inmetro.gov.br/noticias/eventos/MetQuim_palestras/Vocabul%E1rio%20Internacional%20de%20Metrologia_Jos%E9%20Carlos%20Valente_Inmetro.pdf>. Acesso em 26 de maio de 2006.

ITU - INTERNATION TELECOMMUNICATION UNION. **Security architecture for Open Systems Interconnection for CCITT applications:** recommendation X.800. Geneva: CCITT, 1991. Disponível em <http://fag.grm.hia.no/IKT7000/litteratur/paper/x800.pdf>. Acesso em 26 de maio de 2007.

INTERNET SYSTEMS CONSORTIUM. **NTP public services project**. ISC, 2005. Disponível em <http://ntp.isc.org/bin/view/Servers/StratumOneTimeServers>. Acesso em 26 de maio de 2006.

LAMPORT, L. **Time, clocks, and the ordering of events in a distributed system**. c**ommunication of the ACM: v. 21, n. 7, p. 558-565**, jul. 1978. - Disponível em <http://research.microsoft.com/users/lamport/pubs/time-clocks.pdf>. Acesso em 26 de maio de 2007.

LOMBARDI, M. **NIST time and frequency services.** EUA: NIST, 2002. NIST Special Publication 432, 2002. Disponível em <http://tf.nist.gov/timefreq/general/pdf/1383.pdf>. Acesso em 26 de maio de 2007.

KENT, S.; ATKINSON, R**. IP Encapsulating Security Payload (ESP)**. IETF: 1998. Disponível em <http://www.ietf.org/rfc/rfc2406.txt>. Acesso em 26 de maio de 2007.

KONSTANTIN, B., TSANG, J. **A security analysis of the precise time protocol:** short paper. Canada: Laboratory for Education and Research in Secure Systems Engineering University of British Columbia, 2006. - Disponível em <http://konstantin.beznosov.net/professional/works/doi/view.php?105>. Acesso em 17 de agosto de 2007.

MILLS, D. **Network Time Protocol (NTP)**. IETF, 1985. Disponível em <http://www.ietf.org/rfc/rfc958.txt>. Acesso em 26 de maio de 2007.

MILLS, D. **NTP Network Time Protocol (Version 3) specification, implementation and analysis**. IETF, 1992. Disponível em <http://www.ietf.org/rfc/rfc1305.txt>. Acesso em 26 de maio de 2007.

MILLS, D. **Proposed authentication enhancements for the Network Time Protocol Version 4.** Technical Report 96-10-3. Delaware: University of Delaware,1996. Disponível em <http://www.ee.udel.edu/~mills/database/reports/secure/securea.pdf>. Acesso em 26 de maio de 2007.

MILLS, D. **Computer network time synchronization: the Network Time Protocol**. EUA: CRC Press, 2006a.

MILLS, D. **The Autokey security architecture, protocol and algorithms.** Network Working Group Technical Report 6-1-1**.** Delaware: University of Delaware, 2006b. Disponível em <http://www.eecis.udel.edu/~mills/database/reports/stime1/stime.pdf>. Acesso em 26 de maio de 2007.

MILLS, D. **Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI**. IETF, 2006c. Disponível em <http://www.ietf.org/rfc/rfc4330.txt>. Acesso em 26 de maio de 2007.

MOCKAPETRIS, P. **Domain names: concepts and facilities**: IETF, 1983. Disponível em <http://www.ietf.org/rfc/rfc882.txt>. Acesso em 26 de maio de 2007.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST-F1 cesium fountain atomic clock**. EUA: NIST, 2006. Disponível em <http://tf.nist.gov/cesium/fountain.htm>. Acesso em 26 de maio de 2007.

PALKO, R. **Securing time:** the autokey protocols. EUA: SANS Institute, 2001. Disponível em <http://www.sans.org/reading_room/whitepapers/protocols/371.php>. Acesso em 26 de maio de 2007.

PARTRIDGE, C.; MENDEZ, T.; MILLIKEN, W. **Host anycasting service**. IETF, 1993. Disponível em <http://www.ietf.org/rfc/rfc1546.txt>. Acesso em 26 de maio de 2007.

POSTEL, J. **Daytime protocol.** IETF, 1983. Disponível em <http://www.ietf.org/rfc/rfc867.txt>. Acesso em 26 de maio de 2007.

POSTEL, J.; HARRENSTIEN, K. **Time protocol. Information sciences institute**: IETF, 1983. Disponível em <http://www.ietf.org/rfc/rfc868.txt>. Acesso em 26 de maio de 2007.

REDE NACIONAL DE PESQUISAS. **Implementando o serviço NTP na sua rede local**. Rio de Janeiro: RNP, 2000. Disponível em <http://www.rnp.br/_arquivo/cais/manual_ntp_v1b.pdf>. Acesso em 26 de maio de 2007.

RIVEST, R. **The MD5 Message-Digest algorithm**. IETF, 1992. Disponível em <http://www.ietf.org/rfc/rfc1321.txt>. Acesso em 26 de maio de 2007.

RIVEST, R.; SHAMIR, A.; ADLEMAN, L. **A method for obtaining digital signatures and public-key cryptosystems**. Communications of the ACM: V. 21 (2), p.120–126, 1978. Disponível em <http://people.csail.mit.edu/rivest/RivestShamirAdleman-AMethodForObtainingDigitalSignaturesAndPublicKeyCryptosystems.pdf>. Acesso em 26 de maio de 2007.

RYBACZYK, P. **Expert network time protocol:** an experience in time with NTP**.** Berkeley: Apress, 2005.

SHIREY, R**. Internet security glossary**. IETF: 2000. Disponível em <http://www.ietf.org/rfc/rfc2828.txt>. Acesso em 26 de maio de 2007.

SILVA, IVAN M. **Manual técnico versão 2.0. ON (DSH) Resinc/HLB.** Brasil: Observatório Nacional, 2002. Disponível em <http://pcdsh01.on.br/rbshlb.pdf>. Acesso em 26 de maio de 2007.

SPURGEON, C. **Ethernet: o guia definitivo**. Tradução de Daniel Vieira. Rio de Janeiro: Editora Campus, 2000.

STALLINGS, W. **Cryptography and network security:** principles and practices. New Jersey: Prentice Hall, 2003.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. **Risk management guide for information technology systems:** special publication SP800-30. EUA: NIST, 2002. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>. Acesso em 26 de maio de 2007.

TANENBAUM, ANDREW S. **Computer networks:** fourth edition. New Jersey: Prentice Hall, 2003.

WEIBEL, H. **High precision clock synchronization according to IEEE 1588 implementation and performance issues**. Zurich: Zurich University of Applied Sciences Institute of Embedded Systems (InES). Disponível em <http://ines.zhwin.ch/uploads/media/embedded_World_05_Contribution_final_02.pdf >. Acesso em 26 de maio de 2007.

WHITE, G. **Security+ certification:** all-in-one exam guide. Califórnia: McGrawHill/Osborne, 2003.

GLOSSÁRIO

Ameaça: um perigo possível que pode explorar uma vulnerabilidade e ocasionar uma potencial violação de segurança.

Chave privada: é o componente secreto de um par de chaves criptográficas utilizadas na criptografia assimétrica.

Chave pública: é o componete público de um par de chaves criptográficas utilizadas na criptografia assimética.

Chave secreta: um componente secreto compartilhado entre um emissor e um receptor utilizado na criptografia simétrica.

Confidencialidade: é uma propriedade do dado de não estar disponível ou não ser divulgada à indivíduos, entidades ou processos não autorizados.

Confiabilidade: é a habilidade de um sistema operar uma determinada função sob condições estipuladas por um período de tempo.

Disponibilidade: é uma propriedade do sistema ou recurso do sistema ser acessível e consumida sob demanda por uma entidade autorizada de acordo com sua especificação e desempenho.

Estrato: camada na hierarquia de sincronização de tempo representada por “n” e “n+1”.

Exatidão: é a medida ou cálculo obtido de medições com resultados iguais ou similares em referência à algum ponto, é o grau de veracidade.

Função *hash*: um algoritmo que computa um valor baseado no objeto do dado.

Hash: O valor obtido da função *hash*.

Integridade: é a propriedade que o dado não foi alterado, destruido ou perdido de maneira não autorizada ou acidental.

Impacto: resultado de um evento adverso que gera perda ou degradação de qualquer um, ou uma combinação de qualquer um dos seguintes objetivos de segurança: integridade, disponibilidade e confidencialidade.

Irretratabilidade: é uma propriedade para proteção contra a negação no envolvimento na comunicação.

Precisão: é a medida ou cálculo obtido de inúmeras medições com resultados iguais ou similares entre si, é o grau de reprodutividade.

Probabilidade: é um indício de algo acontecer.

Rastreabilidade: é a habilidade de interrelacionar cronológicamente entidades identificáveis unicamente de maneira significante.

Redundância: é uma maneira de se obter um sistema com alta disponibilidade.

Resiliência: é a capacidade de resistir a situações adversas.

Risco: uma expectativa de perda expressa como a probabilidade que uma particular ameaça explorará uma particular vulnerabilidade resultando um particular dano.

Vulnerabilidade: uma falha ou fraqueza no projeto do sistema, implantação ou operação e gerenciamento que pode ser explorada para violar a política de segurança do sistema.

APÊNDICE A - Processo de Avaliação de Risco

No contexto Internet, Shirey (2000) afirma que é considerado um risco a expectativa de perda expressa como a probabilidade de uma ameaça explorar uma vulnerabilidade particular, ocasionando um dano. Similarmente, segundo Stoneburner, Goguen e Feringa (2002) o “risco é uma função entre a probabilidade e o impacto de uma dada ameaça explorar uma vulnerabilidade potencial e resultar um evento adverso na organização”.

A avaliação de risco é uma das etapas do processo de uma metodologia de gerenciamento de risco. Organizações utilizam a avaliação de risco com o objetivo de determinar a extensão das potenciais ameaças e os riscos associados. “Esse processo ajuda a identificar os controles apropriados para reduzir ou eliminar os riscos” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 8). Uma descrição da avaliação de riscos é realizada por Shirey (2000):

> Um processo que identifica sistematicamente valores de recursos dos sistemas e ameaças para aqueles recursos, quantificando perdas expostas (exemplo: perda potencial) baseado na freqüência estimada e custos de ocorrências e, opcionalmente, recomenda como alocar recursos para contramedidas e também minimizar exposições totais (SHIREY, 2000, p. 143).

É possível que, mesmo depois de aplicar todas as contramedidas disponíveis, permaneça algum risco residual (SHIREY, 2000). Isso pode ser tratado em um processo de mitigação de riscos com a aceitação ou não dos riscos residuais.

Stoneburner, Goguen e Feringa (2002) afirmam que a avaliação de risco deve “determinar a probabilidade de eventos adversos futuros, as ameaças aos sistemas de TI em conjunto com as vulnerabilidades potenciais e com os controles apropriados”. O processo de avaliação de riscos proposto na publicação especial SP800-30 (STONEBURNER; GOGUEN; FERINGA, 2002), baseia-se em nove passos, conforme Figura 47.

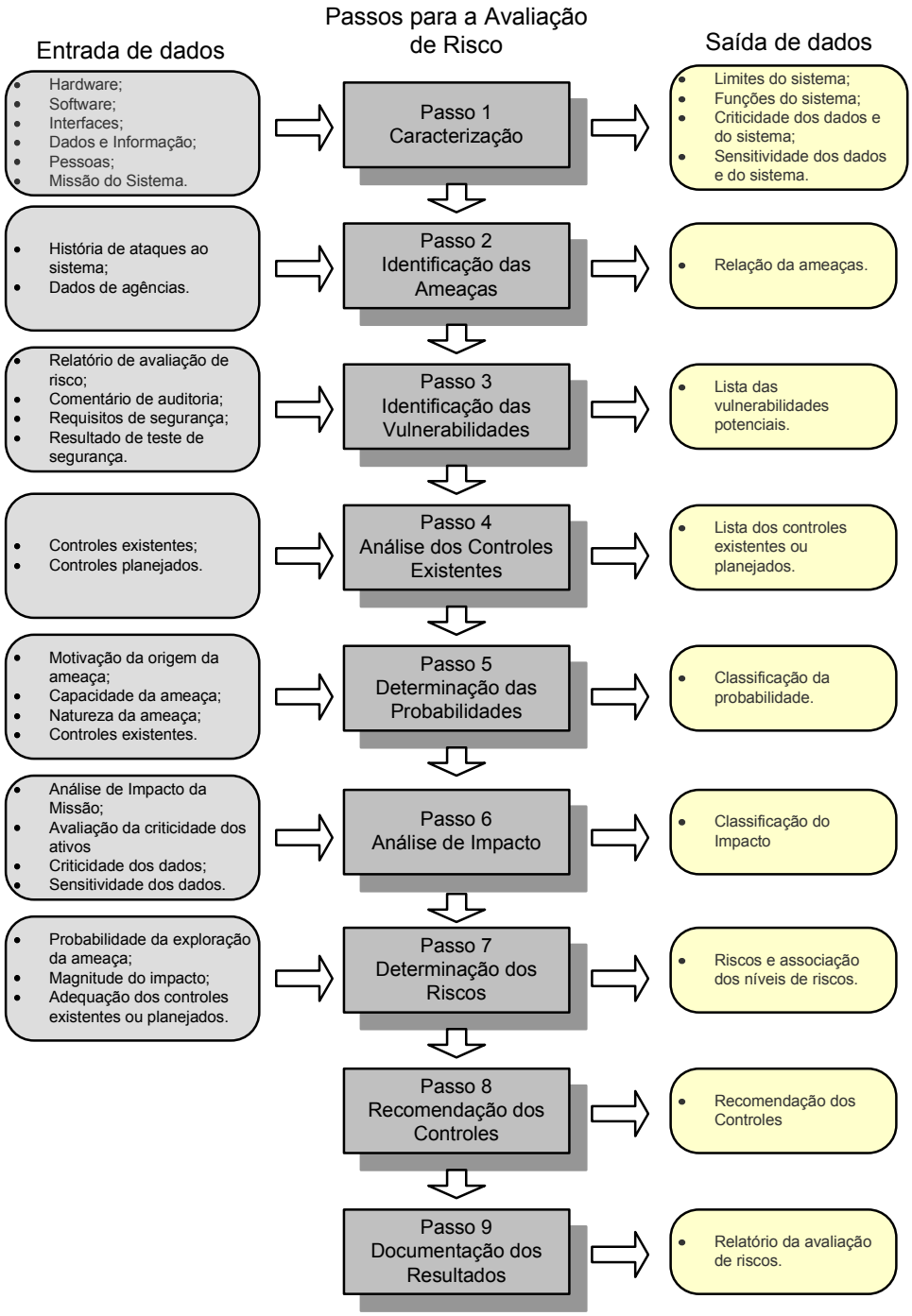

Figura 47: Processo de Avaliação de Riscos. Fonte: STONEBURNER; GOGUEN; FERINGA (2002)

Esse é um método estruturado na identificação do escopo, das ameaças, vulnerabilidades, probabilidades, dis impactos e controles para uma avaliação de riscos dos sistemas de TI.

Passo 1 - Caracterização do Sistema

O primeiro passo é “definir o escopo do esforço” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 10) e a identificação dos limites dos sistemas. Esse passo estabelece o contexto da avaliação de risco e fornece as informações que constituem os ambientes de redes, as configurações, os modos operacionais e outras características do sistema.

O entendimento do ambiente do sistema é crucial para a identificação dos riscos. Assim, deve existir a coleta de informações relativas ao sistema servindo como base de estudo na avaliação de riscos. Em um sistema em operação, as informações coletadas são aquelas existentes em um ambiente já configurado. Porém, para sistemas em fase de projeto ou em fase de desenvolvimento, Stoneburner, Goguen e Feringa (2002) recomendam:

> Para um sistema que está em fase inicial ou projeto, informações do sistema podem ser derivadas dos documentos de requisitos ou de projetos. Para um sistema de tecnologia da informação em desenvolvimento, é necessário definir regras chave de segurança e planejar atributos para o futuro sistema de TI (STONEBURNER; GOGUEN; FERINGA, 2002, p. 11).

Documentos de especificação e os planos de segurança podem fornecer informações úteis. Além disso, alguns exemplos da publicação especial SP800-30 (STONEBURNER; GOGUEN; FERINGA, 2002) são: requisitos funcionais do sistema, topologia de rede, controles técnicos, entre outros.

Passo 2 - Identificação de Ameaça

Shirey (2000) afirma que uma ameaça é “um perigo possível que pode explorar uma vulnerabilidade e ocasionar uma potencial violação de segurança.”

Uma ameaça só apresenta risco quando existe uma vulnerabilidade particular associada a um sistema, implantação ou operação a ser acionada ou explorada. Para Stoneburner, Goguen e Feringa (2002), “a vulnerabilidade é uma falha ou fraqueza que pode ser acionada acidentalmente ou explorada intencionalmente”.

Uma classificação comum das ameaças são baseadas na sua origem e são divididas em três tipos (STONEBURNER; GOGUEN; FERINGA, 2002):

a) Ameaças naturais: enchente, terremoto, tornado, avalanche, tempestade e outros eventos;
b) Ameaças humanas: evento originado por comportamento humano que pode ser intencional, por exemplo, acesso não-autorizado. E, comportamento não-intencional, por exemplo, erro operacional;
c) Ameaças ambientais: falha no fornecimento de energia elétrica, contaminação química, vazamento de líquido inflamável, entre outros.

Em uma avaliação de risco, é importante considerar todas as possibilidades de ameaças que podem causar danos ao ambiente e ao sistema.

Ameaças naturais, geralmente, são consideradas de acordo com a probabilidade de uma ameaça acontecer na localidade em questão, mas o risco é determinado pelo impacto que uma determinada ameaça pode causar.

As ameaças humanas intencionais são aquelas com intuito de realizar ataques deliberados. “Um ataque deliberado pode ser uma tentativa maliciosa de conseguir acesso não-autorizado aos sistemas de TI com o objetivo de comprometer a integridade dos dados, disponibilidade ou confidencialidade dos sistemas” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 13). E, as ameaças humanas não-intencionais são aquelas ocasionadas por erros operacionais, configurações inapropriadas, implantações deficientes, entre outros.

Ameaças ambientais são aquelas que causam danos ao ambiente das instalações do sistema que, normalmente, têm um tempo maior de interrupção ou interdição.

Além da classificação da ameaça por origem, em SHIREY (2000) há a classificação da ameaça por conseqüência e os tipos de ameaças utilizados em determinados ataques, conforme Quadro 43:

Conseqüência da Ameaça	Classes de Ameaça	Tipos de Ameaça
Divulgação	Exposição	Exposição Deliberada *Scavenging* Erro Humano Falha de *Hardware* ou *Software*
	Intercepção	Roubo *Wiretapping (passive)* *Emanations analysis*
	Inferense	Análise de Tráfego Análise de Sinal
	Intrusão	Intrusão Invasão Engenharia Reversa Análise Criptográfica
Fraude	Personificação	Personificação Lógica Maliciosa
	Falsificação	Substituição Inserção
	Repudiação	Falsa Negação de Origem Falsa Negação por Recepção
Interrupção	*Incapacitation*	Lógica Maliciosa Destruição Física Erro Humano Falha de *Hardware* ou *Software* Desastre Natural
	Corrupção	Lógica Maliciosa Destruição Física Erro Humano Falha de *Hardware* ou *Software* Desastre Natural
	Obstrução	Interferência Inundação
Apropriação	Apropriação Indevida	Roubo de Serviço Roubo de Funcionalidade Roubo de Dados
	Mau uso	*Tamper* Lógica Maliciosa Violação de Permissão

Quadro 43. Classificação de Ameaças. Fonte: (SHIREY, 2000)

Passo 3 - Identificação de Vulnerabilidade

A identificação de vulnerabilidade é essencial para a análise de ameaça, pois o risco existe quando há a associação entre ameaça e vulnerabilidade. Porém, nem toda ameaça resulta em um ataque:

> A maioria dos sistemas tem vulnerabilidades de algum tipo, mas isto não significa que os sistemas são frágeis. Nem toda ameaça resulta em um ataque e nem todo ataque é bem sucedido. O sucesso depende do grau da vulnerabilidade, da força do ataque e da efetividade das contramedidas em uso (SHIREY, 2000, p. 189).

Um dos métodos recomendados por Stoneburner, Goguen e Feringa (2002) na identificação da vulnerabilidade do sistema "é o uso de fontes[9] de vulnerabilidade, teste[10] de desempenho da segurança do sistema e o desenvolvimento de uma lista de requisitos de segurança".

Ainda, de acordo com os autores, o método é diferente dependendo da fase do projeto. Em um sistema na fase inicial de um projeto, "a procura de vulnerabilidade deve focar na política de segurança da organização, no procedimento de segurança planejado, na definição de requisito do sistema e na análise de segurança do produto de fornecedores ou de desenvolvedores (ex.: relatórios técnicos)" (STONEBURNER; GOGUEN; FERINGA, 2002, p. 16).

9 Fontes de Vulnerabilidade: <http://www.securityfocus.com>, <http://www.cert.org> , <http://www.us-cert.gov/>, <http://www.rnp.br/cais/alertas/>. <http://secunia.com/>, <http://cve.mitre.org/ >

10 Não haverá implantação neste trabalho. Maiores informações uma metodologia de teste de desempenho de segurança consultar NIST SP-800-42 *Network Security Testing Overview*.

Passo 4 - Análise dos Controles

A análise de controles deve identificar os controles existentes apresentados nas seções sobre esse tema. Segundo Stoneburner, Goguen e Feringa (2002), controles de segurança são constituídos de métodos técnicos e não-técnicos, conforme descritos a seguir:

> Controles técnicos são salvaguardas que são incorporados dentro de *hardware*, *software* ou *firmware* (ex.: mecanismos de controle de acesso, mecanismos de identificação e autorização, métodos criptográficos, software de detecção de intrusão). Controles não-técnicos são gerenciamento e controles de operação como, políticas de segurança, procedimentos operacionais e segurança pessoal, física e ambiental (STONEBURNER; GOGUEN; FERINGA, 2002, p. 20).

Além disso, eles afirmam que os métodos técnicos e não técnicos são classificados em duas categorias: controle preventivo e controle de detecção:

> Os controles preventivos são os que atuam de forma a inibir as tentativas de violação as políticas de segurança, incluem, por exemplo, obrigações de controles de acesso, criptografia e autenticação. Os controles de detecção alertam as violações ou as tentativas de violação das políticas de segurança. Incluem, por exemplo, trilhas de auditoria, métodos de detecção de intrusão e *checksums* (STONEBURNER; GOGUEN; FERINGA, 2002, p. 20).

Passo 5 - Determinação de Probabilidade

Caso uma ameaça explore ou acione uma vulnerabilidade potencial há uma classificação para a probabilidade desse evento. Essa probabilidade pode ser uma medida quantitativa ou qualitativa. Stoneburner, Goguen e Feringa (2002) sugerem uma classificação qualitativa com nível alto, médio ou baixo no processo de avaliação de riscos. O Quadro 44 descreve esses três níveis com mais detalhes:

Grau da Probabilidade (Ameaça-Vulnerabilidade)	Definição
ALTA	A origem da ameaça é altamente motivada e suficientemente capaz de exercer o ataque. E, controles para prevenir a vulnerabilidade são ineficientes.
MÉDIA	A origem da ameaça é motivada e capaz de exercer o ataque. Mas controles estão no local para prevenir o ataque à vulnerabilidade.
BAIXA	Falta motivação ou capacidade para exercer o ataque. Ou, controles estão no local para prevenir, ou impedem significativamente, o ataque à vulnerabilidade.

Quadro 44. Grau da Probabilidade Qualitativa. Fonte: (STONEBURNER; GOGUEN; FERINGA, 2002)

Além disso, para determinar a probabilidade alguns fatores são considerados: a motivação e capacidade da origem da ameaça, a natureza da vulnerabilidade e, por fim, a existência e a efetividade dos controles existentes.

Passo 6 - Análise de Impacto

Uma ameaça bem sucedida acionando ou explorando uma vulnerabilidade gera um impacto adverso, o qual “em termos de perda ou degradação de qualquer um, ou uma combinação de qualquer um dos seguintes objetivos de segurança: integridade, disponibilidade e confidencialidade” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 22).

Abaixo, uma descrição de cada um dos objetivos de segurança e suas conseqüências ou impactos:

a) Integridade: requisito, necessário, a fim de proteger a informação contra modificação imprópria. Perda de Integridade ocorre quando mudanças não-autorizadas são realizadas em dados ou sistemas por ações intencionais ou acidentais. O uso de informações contaminadas pode resultar em decisões incorretas ou fraudes. Também, violação de integridade pode ser o primeiro passo para um ataque bem sucedido contra a disponibilidade e confidencialidade do sistema;
b) Disponibilidade: é a propriedade de um sistema ou dos recursos de um sistema estar acessível e utilizável por uma entidade autorizada. A perda de disponibilidade pode resultar em perda de produtividade e/ou perda de efetividade operacional, impedindo os usuários de exercer, suas funções;
c) Confidencialidade: requisitos necessários para proteger a informação de divulgação não-autorizada. A perda de confidencialidade pode resultar em perda de sigilo de qualquer natureza, perda de imagem, embaraço público e ações legais contra a organização.

A mensuração de impactos pode ser medida de forma quantitativa e/ou qualitativa. “Medidas quantitativas são perdas de receitas, custo de reparos de sistemas ou grau de esforço requerido a fim de corrigir problemas ocasionados por uma ameaça bem sucedida” (STONEBURNER; GOGUEN; FERINGA, 2002, p. 22). Impactos de outros tipos, como perda de confidencialidade, perda de credibilidade ou perda de imagem

são difíceis de ser mensurados por unidades específicas. Assim, podem ser qualificados na magnitude do impacto como sendo: altos, médios ou baixos.

Na análise de impacto deste trabalho, as medidas quantitativas não são possíveis devido à natureza do conteúdo ser generalizada. Não há medidas com valores de referência já definidos. Dessa maneira, são tratadas apenas as medidas qualitativas conforme Quadro 45:

Magnitude do Impacto	Definição
ALTO	(1) Pode resultar em perdas de altos valores dos principais recursos ou ativos tangíveis. (2) Pode resultar de forma significativa violação, dano ou impedir a missão da organização, reputação ou de interesses. (3) Pode resultar em ferimentos humanos graves, inclusive morte.
MÉDIO	(1) Pode resultar em perdas de valores de recursos ou ativos tangíveis. (2) Pode resultar na violação, dano ou impedir a missão da organização, reputação ou de interesses. (3) Pode resultar em ferimentos humanos graves.
BAIXO	(1) Pode resultar em perdas de alguns de recursos ou ativos tangíveis. (2) Pode afetar a missão da organização, reputação ou de interesses.

Quadro 45. Magnitude do Impacto. Fonte: (STONEBURNER; GOGUEN; FERINGA, 2002)

Passo 7 - Determinação de Risco

A avaliação do grau de riscos de um determinado par de ameaça e vulnerabilidade, segundo Stoneburner; Goguen e Feringa (2002), pode ser expressa pelas funções:

a) a probabilidade de tentativa de uma dada ameaça valer-se de uma dada vulnerabilidade;
b) a magnitude do impacto devido a uma ameaça bem sucedida valer-se de uma vulnerabilidade;
c) a adequação dos controles planejados ou existentes para reduzir ou eliminar os riscos.

Sendo assim, na mensuração dos riscos, são necessárias uma escala e uma matriz de riscos como sugerida na publicação especial SP800-30 (STONEBURNER; GOGUEN; FERINGA, 2002).

A matriz de riscos é derivada da multiplicação da probabilidade da ameaça e de seu impacto. Tal matriz é exemplificada através da Tabela 4, que descreve como os níveis de risco são derivados dos níveis alto, médio e baixo.

Ameaça	Impacto		
Probabilidade	BAIXO (10)	MÉDIO (50)	ALTO (100)
ALTO (1.0)	**BAIXO** (10x1.0=10)	**MÉDIO** (50x1.0=50)	**ALTO** (100x1.0=100)
MÉDIO (0.5)	**BAIXO** (10x0.5=5)	**MÉDIO** (50x0.5=25)	**MÉDIO** (100x0.5=50)
BAIXO (0.1)	**BAIXO** (10x0.1=1)	**BAIXO** (50x0.1=5)	**BAIXO** (100x0.1=10)

Tabela 4. Exemplo de Matriz de Riscos (Probabilidade x Impacto). Fonte: (STONEBURNER; GOGUEN; FERINGA, 2002).

É possível determinar uma forma mais racional para os níveis de risco, assumindo valores para cada grau. Por exemplo, para o grau de probabilidade alta, é assumido valor 1.0; para grau médio, é dado o valor 0.5 e, para o grau baixo, é assinalado o valor 0.1. De forma análoga, para o grau de impacto alto, é dado o valor de 100; para grau médio, 50 e, para o grau baixo, o valor 10. Assim, é criada uma escala de

risco, onde o grau de risco alto é representado por valores maiores que 50. No grau de risco médio, os valores estão entre 10 e 50 e, para o grau de risco baixo, os valores estão abaixo de 10.

Nessa escala de riscos valores não significam a negligência de controles em qualquer grau. Essa classificação é uma forma de priorizar os controles de maneira a atender os níveis de risco mais críticos e, em seguida, os riscos menos críticos em processo de mitigação de riscos. Sobre maiores detalhes do processo de mitigação de riscos consultar a publicação especial SP800-30 (STONEBURNER; GOGUEN; FERINGA, 2002).

Passo 8 - Recomendação de Controles

O principal objetivo da recomendação dos controles é eliminar ou reduzir os riscos a um grau de segurança aceitável para o funcionamento dos sistemas envolvidos. No processo de análise de risco, todos os possíveis controles são relacionados, mas nem todos precisam ser implantados a fim de reduzir perdas.

A decisão sobre a implantação ou não dos controles faz parte de um processo de mitigação de risco, o qual não é objeto de estudo deste trabalho.