Uma Arquitetura de Segurança para Gerência de Redes

José Eduardo De Lucca[1]
Carlos B. Westphall[2]
Elizabeth S. Specialski[3]

UFSC - INE - CPGCC
Caixa Postal 476
88.040-970 - Florianópolis - SC

Resumo

Este artigo apresenta um levantamento dos riscos de segurança associados à Sistemas de Gerência de Redes e descreve uma Arquitetura de Segurança aplicável a tais sistemas que garante autenticação, integridade e confidencialidade nas comunicações entre entidades de gerência. Esta arquitetura permite a implantação dos serviços de modo transparente para o Sistema de Gerência hospedeiro.

1 Introdução

Nos dias de hoje, onde a interligação de computadores em rede é a tônica dos ambientes de produção, a confiabilidade destas redes e dos computadores interligados deve ser estrita. Esta confiabilidade está alicerçada em diversos pontos e dois dos mais importantes são o gerenciamento e a proteção dos elementos que compõem as redes.

Com a evolução da informática e da importância estratégica das atividades relacionadas com informática no desempenho de empresas e instituições em geral, os aspectos ligados à segurança passaram a representar papel importante no cotidiano das mesmas. A migração de ambientes centralizados (*time-sharing*) e de microcomputadores independentes para instalações interligadas por redes de computadores resultaram em novos e sérios problemas de segurança. A segurança tradicional em ambientes centralizados era basicamente física, com restrições de acesso às instalações e equipamentos. Dados fluindo pelas redes ou residindo temporariamente em nós intermediários são vulneráveis à interceptação, alteração ou destruição. Existem mais formas de executar uma tentativa de acesso a computadores conectados a uma rede do que a computadores isolados. Os problemas de gerenciamento de tais ambientes se completam com a tendência à grande

[1] Professor do INE (Depto de Informática) e mestrando do CPGCC (Curso de Pós-Graduação em Ciência da Computação) da UFSC (Universidade Federal de Santa Catarina). e-mail: delucca@inf.ufsc.br
[2] Professor do INE e do CPGCC da UFSC. e-mail: westphal@inf.ufsc.br
[3] Professora do INE e do CPGCC da UFSC. e-mail: beth@inf.ufsc.br

distribuição física dos recursos e usuários e aos diferentes níveis de segurança física encontrados em cada um destes locais.

Protocolos de Gerência de Redes e os canais de comunicação que transportam informação de gerência são potencialmente vulneráveis a atentados contra a segurança. Cuidados particulares devem, portanto, ser tomados para assegurar que tais protocolos e informações estejam protegidos. A definição de vulnerabilidades e dos riscos de segurança dos Sistemas de Gerência e a criação de ferramentas para tratar estes problemas fazem parte do conjunto de ações fundamentais para o funcionamento confiável das redes. A especificação de ferramantas, seu comportamento e seus inter-relacionamentos compõem uma Arquitetura de Segurança.

Na seção 2 será apresentada uma visão geral sobre aspectos de segurança em redes de compuadores. A seguir, na seção 3, o detalhamento dos problemas relativos à segurança restritos aos ambientes de Gerência de Redes, com análise das ameaças que podem atingir os mesmos. Na seção 4 são feitas considerações sobre os serviços necessários para garantir a proteção dos sistemas de Gerência de Redes e finalizando na seção 5 com a descrição de um modelo de Arquitetura de Segurança com os algoritmos necessários para implementação da mesma.

2 Segurança em Redes de Computadores

Existem diversos elementos sobre os quais podem incidir ameaças contra a segurança em um ambiente informatizado e em especial em um ambiente interligado por redes de computadores. Segurança em informática pode ser compreendido como a garantia ou confiança que os usuários tem em determinado sistema [PFL 89] [DOD 83]. Segurança aplicada no domínio das Redes de Computadores, então, deve garantir que o sistema não seja comprometido por ameaças cuja origem não esteja localizada, necessariamente, no computador local mas remotamente.

O que pode ser comprometido em um sistema informatizado? No limite, seria a indisponibilidade total do sistema, por algum motivo como equipamento avariado, código removido, cpu a 100% de carga, etc. Outras formas não tão facilmente detectáveis de comprometimento de um sistema (mas não menos preocupantes) são o fornecimento de resultados incorretos em um processamento ou a execução de outras atividades que não somente aquelas esperadas.

Existem muitas formas de comprometer sistemas porque normalmente existem muitos pontos expostos. Estes pontos de exposição podem ser classificados conforme estas seis categorias: hardware, software, informação/dados, pessoal, documentação e suprimentos.

No jargão de segurança os itens que se enquadram nas categorias acima são chamados ***ativos***. Os ativos de uma instalação que devem ser protegidos de ameaças, porque o *comportamento* apropriado desses ativos é que vai permitir o funcionamento dos sistemas. Uma alteração, destruição, erro ou indisponibilidade de algum destes ativos pode gerar um comprometimento do sistema. As ***vulnerabilidades*** dos ativos devem, portanto, ser estudadas e medidas de proteção adotadas para compensá-las.

Analisando os ativos apresentados estritamente do escopo de segurança em redes de computadores, apenas Hardware, Software e Informação são passíveis de serem protegidas por meios de o que se convenciona chamar de **Segurança Lógica**, em contraposição à Segurança Física[4]. A Segurança Lógica lança mão de software para garantir quatro princípios básicos: ***autenticação de usuário***, ***disponibilidade de recursos***, ***integridade das informações*** e ***confidencialidade das informações***.

2.1 Agressões e Falhas

Outra forma (complementar) de analisar os problemas de segurança é fazer uma classificação das ameaças entre ***agressões*** e ***falhas***, como referenciado em [COO 89]. Falhas são acontecimentos acidentais que, de uma forma ou de outra, põem em risco a segurança das instalações e dos sistemas. Exemplos de falhas são incêndios, inundações, terremotos, roedores que atacam a fiação e provocam curto-circuitos, acidentes ou erros humanos (derramamento de líquidos sobre equipamentos/mídia, manipulação incorreta de mídia, digitação de dados incorretos, ...) e falhas de hardware, de software e de comunicação. As falhas também são ameaças à segurança porque, como já foi definido, atentam contra a confiabilidade e/ou disponibilidade de um sistema. As agressões, por outro lado, são intencionais e hostis. São exemplos de agressões as ameaças de bombas, pressões/extorsão contra pessoas do *staff*, roubo, operação inadequada proposital de equipamentos, software propositadamente incorreto, vírus, invasões através de redes, (tentativas de) acesso a informações privativas/confidenciais, etc.

Não é possível abordar todos os problemas a partir do enfoque de Segurança Lógica. Os problemas relacionados às falhas dizem respeito à outros aspectos que não Segurança Lógica (manutenção e segurança física, p.ex.). Na lista de agressões também se encontram diversas ameaças que não são tratáveis por medidas de segurança lógica, como ameaça de bomba e roubo.

Então, sob esta ótica, as ameaças que dizem respeito à segurança em redes de computadores são agressões perpetradas por pessoas não autorizadas (as quais serão chamadas *invasores*) que objetivam obter benefícios indevidos ou prejudicar o funcionamento dos sistemas.

2.2 Acesso à Informação e à Capacidade de Processamento

Também é possível analisar as ameaças potenciais que os sistemas em rede estão sujeitos a partir das vantagens que se pode obter com a invasão de sistemas. Algumas vantagens[5] seriam o acesso a informações, a obtenção de "ciclos de máquina", o acesso à serviços e à outras redes, o acesso a software, ganho de espaço de armazenamento e

---

[4] *Segurança Física é a segurança tradicional de informática, centrada em restrições de acesso físico às instalações e equipamentos, prevenção de acidentes de trabalho e planos de recuperação de desastres como incêndios e inundações. Maiores informações podem ser encontradas em [COO 89] e [PFL 89].*

[5] *Vantagens aqui devem ser entendidas como um ou mais dos seguintes "motivadores": aspecto financeiro, sabotagem/espionagem (industrial, p.ex.), vingança, curiosidade, desafio, diversão.*

destruição/modificação de informações (ganhos indiretos, em função de prejuízos a terceiros)

Em suma, o que está em "disputa" neste contexto de proteção de Sistemas em Rede pode ser resumido nestes dois itens:

1. A ***informação*** em si: o acesso, a destruição e a modificação de informação e o acesso a serviços; e
2. O acesso à capacidade de ***processamento*** de informação e ao equipamento: roubo de ciclos de máquina, acesso à serviços, redes e software, e uso da capacidade de armazenamento.

Por informação deseja-se representar muitas coisas: dados para processamento, tecnologia, know-how, conhecimento científico, informações econômico-financeiras, estratégias e políticas, projetos, etc. Computadores podem manter informações confidenciais sobre pessoas, sobre objetivos militares e movimentos de tropas, informações vitais para empresas ou governos, saldos bancários, e assim por diante. O valor destas e de outras informações é alto, apesar de ser muito difícil, na maioria dos casos estabelecer o valor intrínseco de determinada informação. Uma abordagem possível nestes casos é determinar que o valor de determinada informação é igual ao custo de obtenção de determinados dados (como por exemplo o resultado de anos de pesquisas em laboratório sintetizado em artigos) ou ainda da recuperação ou reconstrução das informações perdidas. Outro tipo de informação é a que diz respeito a pessoas (ou mesmo entidades) onde o acesso destas informações podem configurar um atentado à privacidade.

Então, apesar de as informações possuírem um alto valor, é freqüentemente difícil medi-lo (pela subjetividade da questão). Pode-se estabelecer apenas que o detentor da informação conhece o valor da mesma. A capacidade de acesso a informação, bem como a capacidade de alterá-la ou destrui-la, representa então poder, que é protegido pelos legítimos detentores da mesma e que é buscado (de forma ilegítima) pelos invasores.

O acesso ao hardware e ao software (e o decorrente acesso à capacidade de processamento) também representa poder, já que a utilização dos mesmos permite o processamento de informações. O acesso ilegítimo à capacidade de processamento pode ser apenas roubo de tempo de processamento, mas esse tipo de ato pode levar a conseqüências sérias, como o aumento do custo para usuários legítimos ou, em caso extremo, a negação de serviço para usuários legítimos, uma vez que a cpu e/ou a memória estão ocupadas realizando tarefas estranhas à instalação. Outras práticas ilegítimas seriam o acesso a serviços não disponíveis na instalação de origem, o acesso não autorizado a software, uso de capacidade de armazenamento, ou ainda para acesso à outras redes, usando o sistema invadido como dissimulação da origem da agressão. Um exemplo típico de roubo de tempo de cpu é a utilização de máquinas para decifrar informações criptografadas (como arquivos de senhas) para ter acesso a novas informações: uma agressão (roubo de ciclos) que alimentará outra agressão (a invasão de outros sistemas).

As agressões referentes à informação e à capacidade de processamento podem ser perpetradas basicamente de três formas: por escuta ou monitoração da rede; por invasão ao sistema; e por mascaramento.

A **escuta/monitoração** do canal é tarefa simples e mesmo com recursos pouco sofisticados é possível alcançar tal feito. Exemplos de formas de se conseguir monitoração de redes vão desde o uso de analisadores de protocolos (recurso caro) até a modificação do software de um computador comum para atuar como escuta. Existem ainda equipamentos próprios para escuta (passiva) que se valem de emanações eletromagnéticas dos cabos e conectores. O comprometimento da segurança de um nó intermediário em redes *store-and-forward* ou de *gateways* e roteadores leva à exposição de informações a terceiros. Então, toda informação que circula por redes pode ser interceptada e, se medidas de segurança não tiverem sido adotadas, esta informação se torna não confidencial. Pouco se pode fazer a nível de software para impedir este tipo de agressão. O uso de criptografia deve ser considerado pois, apesar de não impedir o ataque, é uma forma de reforçar o sigilo das comunicações.

A **invasão** de sistemas com o objetivo de ganhar acesso a informações e a recursos computacionais é uma das agressões mais comuns e necessita de pouco aparato além de bom conhecimento e muita persistência por parte do perpetrante da ação. As vulnerabilidades relativas à invasão de sistemas podem ser geradas de muitas formas; por exemplo pela não instalação de senhas por parte de usuários ou por falhas de implementação de softwares. Os riscos associados são os mesmos relacionados para a escuta do canal e mais a possibilidade de negação de serviços para usuários legítimos em função de invasores estarem usufruindo de serviços de forma não autorizada. A negação de serviço pode aparecer de várias formas: cpu com alta carga, espaço de armazenamento não disponível, serviços (como canais de comunicação) sobrecarregados, software eliminado ou afetado por vírus, equipamentos desabilitados, etc. Mas, grande parte desta vulnerabilidade é responsabilidade do sistema operacional hospedeiro, reduzindo a responsabilidade dos mecanismos de segurança das redes. Na verdade, esta forma de agressão normalmente se transforma ou em escuta ou em mascaramento após concretizada a invasão.

O terceiro item, **mascaramento**, consiste na tentativa de personificação de uma terceira entidade em uma comunicação. O objetivo é o mesmo que os anteriores: acesso a informações ou a recursos computacionais. O mascaramento pode ser conseguido por invasão simples (como visto acima) ou por meios muito mais sofisticados como a alteração de pacotes que fluem na rede ou ainda forjando pacotes. Estando mascarado de uma entidade comunicante legítima da rede, o software "clandestino" pode ter acesso a informações sensíveis ou a recursos importantes e até provocar eventos anonimamente. Fica claro que este tipo de agressão é complexa o que pressupõe a necessidade de o invasor ser conhecedor profundo de protocolos de comunicação utilizados e sugere um alto interesse pelas vantagens advindas da invasão. Disto conclui-se que, quanto mais sofisticada é a agressão, mais sofisticados têm que ser os mecanismos de defesa.

A seguir serão vistos aspectos relacionando a necessidade de segurança especificamente em sistemas de gerenciamento de redes.

3 Gerência de Redes e Segurança

Gerência de Redes é uma aplicação distribuída onde processos de gerência (agentes e gerentes) trocam informações com o objetivo de monitorar e controlar a rede. O

processo gerente envia solicitação ao processo agente que por sua vez responde às solicitações e também transmite notificações referentes aos objetos gerenciados que residem em uma base de informação de gerenciamento (MIB) [WES 92] [BRI 93].

Toda e qualquer informação produzida pelo Sistema de Gerência, em um determinado instante, está ou em uma MIB ou trafegando pela rede (em uma comunicação típica entre um agente e um gerente ou entre dois gerentes) ou ainda poderá ser deduzida (reproduzida) com informações parciais oriundas destas duas fontes. Toda informação produzida pelo Sistema de Gerência é útil para a manutenção da rede em operação com confiabilidade. Sem dúvida, os Sistemas de Gerência facilitam a administração das redes seja pela automatização de algumas atividades seja por permitir maior controle sobre os recursos da rede ou ainda por fornecer informações (estatísticas, p.ex.) que permitirão ajustes, correções ou adaptações às necessidades dos usuários.

Entretanto, neste ponto também é possível observar que o próprio Sistema de Gerência e as informações por ele geradas são de extrema valia para indicar pontos vulneráveis à ataques, ter acesso e controlar indevidamente recursos da rede, manipular informações, em suma, realizar atividades prejudiciais à rede, aos sistemas e/ou aos usuários.

Sob certa ótica, é possível até afirmar que uma rede com Sistema de Gerência formal implantado é *menos* segura do que a mesma rede sem o Sistema de Gerência. Isto porque, quando há gerência, há mais vulnerabilidades, há mais pontos onde é possível desferir um ataque; e, sendo assim, há mais possibilidades de comprometimento da rede e de seus sistemas. Aqui estão alguns exemplos:

- Se um agente emite um alarme acerca de falha em um mecanismo de segurança e este alarme é interceptado por um invasor; então está-se fornecendo uma informação valiosa para que um intruso possa realizar outras agressões.
- Uma notificação de alarme forjada por um intruso pode levar a alguma ação (por parte do gerente "iludido") que libere informações ou serviços a usuários que não teriam autorização em situações normais.
- Uma entidade infiltrada que se mascara de gerente pode ter acesso à informações sensíveis mantidas na MIB, inclusive com poder de alteração (como desativação de serviços de segurança ou alteração de registros de contabilização).
- Um agente mascarado pode fornecer acesso à recursos da rede para usuários não autorizados e/ou indisponibilizar tais recursos para usuários legítimos; ou ainda forjar informações com o intuito de forçar o gerente para a alocação de mais ou melhores recursos.

Estas e muitas outras vulnerabilidades não existiriam se não existisse um Sistema de Gerência. Ressalve-se que também são possíveis ataques que resultariam nos mesmos "benefícios" (sempre existirão formas de tentar burlar a segurança), mas a Gerência acrescenta pontos passíveis destes ataques aos já existentes; e por isso pode-se concluir que um Sistema de Gerência de Redes torna a rede mais insegura por um lado, ao mesmo tempo que cria mecanismos de controle que serão úteis também na manutenção da segurança da rede.

3.1 Ameaças sobre Sistemas de Gerência

As ameaças que serão abordadas dizem respeito às agressões que podem ser perpetradas por intrusos na rede ou por usuários que tentam obter mais recursos ou informações do que autorizados. Alguns exemplos destas agressões estão apresentadas acima e que, de acordo com definições já apresentadas, podem ser classificadas em :

- Mascaramento
- Monitoração ou Escuta Passiva
- Escuta Ativa

A seguir são apresentados com mais detalhes estas ameaças às quais estão expostos os Sistemas de Gerência de Redes.

3.1.1 Mascaramento

É a pretensão de uma entidade de se fazer passar por outra de modo a ter acesso a informações, ganhar novos privilégios, afetar os sistemas, etc. São evidentes as vantagens que uma entidade pode obter ao se mascarar em outra. A primeira delas é o anonimato, tornando difícil a descoberta da origem da agressão. Outras vezes, a intenção é "incriminar" outro usuário por atos ilícitos.

Um fato é certo: para criar uma entidade mascarada, o agressor deve ter acesso à rede, mas pode ser um acesso autorizado (lícito) ou não. Então, uma primeira barreira contra este tipo de agressão é um Sistema de Controle de Acesso à rede o mais confiável possível. Controle de acesso envolve identificação, autenticação e autorização, além de uma política de segurança e consciência por parte dos usuários da importância da segurança para a rede e seus sistemas. Por **identificação** entende-se uma estrutura de nomes que garanta a identificação única para cada entidade da rede. Mas não basta identificação porque as entidades podem não ser confiáveis ao se identificar, sendo necessário então a confirmação da identidade: **autenticação**, ou seja, a validação de que uma entidade é quem ou aquilo que diz ser. A **autorização** permite indicar se determinada entidade (identificada e autenticada) possui acesso legítimo (autorizado) a determinado recurso ou operação e deve evitar o acesso caso contrário.

Mas não se pode pensar em Controle de Acesso somente no momento do primeiro acesso em uma sessão (*login*) mas também em outras atividades durante a sessão, de forma continuada, sob pena de abordar o problema de maneira muito pobre.

No que diz respeito a entidades de Gerência, o controle de acesso é um ponto crucial, justamente pelos problemas que podem ser causados se um agressor conseguir forjar uma entidade e esta seja "aceita" como legítima pelas entidades pares comunicantes. Os protocolos de gerência são, por natureza, simples e, portanto, a criação de entidades que simulam agentes ou gerentes não é difícil.

É então importante para a segurança em um Sistema de Gerência que cada entidade componente do mesmo esteja devidamente identificada e autenticada e tenha os direitos de acesso definidos e controlados. Para tanto, faz-se necessária a especificação e

implantação de Serviços de Identificação/Autenticação específicos para entidades comunicantes, e de Confidencialidade de Acesso aos recursos (no caso, o acesso à MIB).

3.1.2 Escuta Passiva

Neste caso, há apenas coleta de informações que transitam na rede. Apesar de, em um primeiro momento, os riscos que representa a escuta passiva parecerem pequenos, é possível recolher muitas informações úteis para o comprometimento de uma rede. Um exemplo são as informações que dizem respeito à segurança da rede ou sobre falhas, que fluem entre agentes e gerentes da rede. Estas informações podem ser senhas de usuários, informações trocadas entre entidades para autenticação, informações sobre configuração, informações sobre falha de algum mecanismo de segurança, etc.

Quando informações sensíveis como as citadas devem transitar pela rede, é fundamental que sejam adotadas medidas para evitar que tais informações sejam acessadas indevidamente. Para tanto é necessário definir um Serviço de Confidencialidade de Comunicação.

É fácil perceber que grande parte das informações que são trocadas entre entidades de um Sistema de Gerência são sensíveis e portanto devem ser protegidas.

3.1.3 Escuta Ativa

A escuta ativa difere da escuta passiva por não apenas coletar informações que fluem pela rede, mas também por alterá-las de alguma forma, seja no conteúdo, na seqüência, no tempo ou pela destruição ou criação de mensagens; de forma a realizar ou induzir ações não autorizadas ou criar condições para ações não autorizadas ou ainda encobrir atos ilícitos praticados.

A barreira criada pelo controle de acesso citado acima não é efetiva contra esta ameaça uma vez que a atuação pode se dar sobre mensagens legítimas de entidades autenticadas e autorizadas. A autenticação das entidades comunicantes, como citado, visa a garantir que não há entidades mascaradas mas não impede que sejam criadas mensagens espúrias em nome de uma entidade legítima. Outros casos não abordados pelos serviços de autenticação e autorização dizem respeito à destruição de mensagens, atrasos forçados em mensagens, reordenação de mensagens e repetição de mensagens em outro momento.

Duas medidas de proteção se tornam então necessárias: autenticação da origem das mensagens e garantia da integridade das mensagens. Sem estes dois serviços a rede continuará aberta a ataques.

Os Sistemas de Gerência de Redes estão sujeitos a todas estas ameaças porque estão baseadas na separação das funções de gerência com distribuição das informações, sendo necessária a comunicação entre entidades de gerência. Deve-se então acrescentar ao Serviço de Identificação/Autenticação de entidades a tarefa de autenticar a origem, a forma e o momento do envio das mensagens. Além disso, um Serviço de Integridade de mensagens deve ser estabelecido e será o responsável pela garantia de que uma mensagem não sofreu alterações em seu caminho desde a origem ao destinatário, envolvendo as tarefas de evitar alteração de informações, re-sequenciamento e a simples destruição.

A autenticação, por sua vez, também depende da integridade das mensagens para algumas tarefas. Por exemplo, de nada adianta validar a origem de uma mensagem que foi alterada por uma escuta ativa ou se durante uma autenticação de entidade as mensagens podem ser afetadas de modo a validar uma entidade mascarada. Então há uma interdependência entre os serviços e todos devem estar em atividade para que se possa dar confiabilidade à rede.

4 Segurança sobre Gerência de Redes

Como foi mostrado no item 3, a Gerência de Redes está baseada na comunicação entre entidades agentes e gerentes de segurança e em uma base de informações de gerência (MIB). Toda informação produzida e manipulada pelo Sistema de Gerência é útil para a manutenção da rede em operação com confiabilidade e com bom desempenho. Mas, da mesma forma que traz benefícios, abre vulnerabilidades muito perigosas para todo o sistema gerenciado, pois se o simples acesso às informações de gerência já pode significar grande vantagem para um agressor quanto mais é a possibilidade de, por meios escusos, gerar solicitações de alteração na configuração, manipulação de informações de contabilização e desempenho ou mesmo desativar serviços de segurança.

Ambientes de Gerência de Redes necessitam então de serviços de segurança para garantir a confiabilidade daqueles, uma vez que ter domínio sobre o gerenciamento da rede é o mesmo que deter o domínio sobre **toda** a rede, já que são nestes ambientes que estão localizadas as facilidades de gerência de configuração, falhas, desempenho, contabilização e da própria segurança.

Sendo assim, passa-se a seguir à especificação de uma Arquitetura de Segurança para um Ambiente de Gerência de Redes genérico. Neste ambiente genérico interagem as seguintes entidades:

- *agentes*: atuam diretamente sobre objetos da rede (objetos gerenciáveis), alterando seu estado, detectando falhas, acumulando informações ao longo do tempo, emitindo relatórios, etc. Interage com os gerentes (abaixo) atendendo solicitações ou emitindo avisos. Mantém atualizada e consistente uma base de informações acerca dos objetos que gerencia e o acesso a esta base só pode ser realizado pelo agente.
- *gerente*: centraliza informações oriundas dos agentes e é responsável pela gerência de um conjuntos de objetos gerenciáveis (via agentes), valendo-se de serviços de gerenciamento que são submetidos aos agentes. Interagem também com outros gerentes.
- *objeto gerenciável*: representa um recurso da rede que é monitorado e controlado por um agente.

4.1 Requisitos de Proteção

No contexto de um Sistema de Gerência, as ameaças que cabem ser analisadas, dentre todas as ameaças à segurança em uma rede de computadores, são as seguintes:

a) acesso não autorizado à informação de gerência que flui pela rede;
b) acesso não autorizado à informação de gerência mantida na MIB;
c) alteração e re-sequenciamento de mensagem de gerenciamento; e
d) geração de mensagens de gerenciamento por terceiros (entidades que não fazem parte da arquitetura de segurança).

Os Serviços de Segurança que precisam estar disponíveis para contrapor estas ameaças, conforme visto acima, são:

1. Confidencialidade (contra (a) e (b));
2. Integridade (contra (c)); e
3. Autenticação (contra (d)).

A proposta de mecanismos de segurança para implementação destes serviços são apresentados a seguir.

Para suportar o ***Serviço de Confidencialidade*** (ou privacidade) é necessário o uso de criptografia. Há dois tipos básicos de criptografia em uso hoje em dia: por chave secreta e por chave pública [PFL 89]. A adoção da segunda alternativa - um sistema de chaves públicas[6] - é a mais natural em função da eficiência no processo de distribuição das chaves, evitando a necessidade de um transporte e difusão *off-line* das chaves entre as entidades cooperantes (o que, muitas vezes, é impossível em se tratando de softwares), além de também se adaptar melhor aos outros itens da Arquitetura de Segurança como será mostrado adiante. Um contratempo é a menor eficiência no processo de "encriptação". O uso de criptografia é a única forma de garantir que uma mensagem que esteja trafegando pela rede e seja interceptada não forneça informações valiosas para o agressor. A mensagem poderá ser interceptada, mas dificilmente será decodificada sem que a chave esteja disponível.

Da mesma forma, o acesso à MIB pode ser até aberto pois, se as informações lá contidas estarão cifradas, elas não serão úteis para invasores, uma vez que estes não terão tempo hábil para decifrá-las antes que ocorram alterações nas mesmas (e invalidando assim todo o trabalho realizado até ali).

A alteração de mensagens ou re-sequenciamento (re-submissão de mensagem antiga) é uma séria ameaça pois esta mensagem pode "passar" no teste de autenticação (uma vez que é uma mensagem originalmente montada e expedida por uma entidade autorizada) e, com isso causar danos ao sistema. Por isso o ***Serviço de Integridade*** deve estar atento para evitá-las. Duas providências se fazem necessárias:

i) para evitar que uma mensagem alterada seja considerada válida, a ação a ser tomada é a cifragem de um campo que contenha o *checksum* de toda a mensagem. A chave que deve ser utilizada para isso é a chave privada do remetente da mensagem (a chave privada do esquema de chave pública). Com isso se garante a integridade da

---

6 Um sistema de chaves públicas prevê a existência de duas chaves simétricas: o que uma chave cifra o seu par decifra e vice-versa. Uma das chaves é mantida em segredo (chave privada) e a outra é divulgada (chave pública - daí o nome do sistema) através de um serviço de diretório, por exemplo. Maiores detalhes podem ser encontrados em [NEC 90] e [PFL 89]

mensagem, pois um agressor não terá como alterar a mensagem, gerar um novo *checksum* e criptografá-lo pois não possuirá a chave correta. Já o destinatário pode verificar a integridade simplesmente usando a chave pública do remetente para conferir o checksum calculado com o decifrado. Qualquer alteração da mensagem é imediatamente detectada. Este esquema é semelhante ao proposto em [OMU 90] e [GAL 91].

ii) para evitar o re-sequenciamento, o que deve ser feito é a inclusão de um campo que indicará a ordem da seqüência da mensagem. Este campo deverá conter um valor dentro de uma seqüência determinada a cada comunicação entre cada par de entidades (ou seja, a cada mensagem, o remetente incluirá o valor da seqüência e indicará qual valor deverá ser usado na próxima comunicação entre estas duas entidades). Este campo (ou melhor, estes dois campos) também devem ser criptografados com a chave privada do remetente. A lei de formação da seqüência não é importante e pode ser implementada diferentemente em cada uma das partes. A abordagem freqüentemente adotada para este problema é a de sincronização de relógios entre todos os computadores do Sistema de Gerência e o decorrente uso de *timestamps* para garantir o momento do envio da mensagem [GAL 91]. A abordagem aqui proposta é muito mais simples (tanto para implementação quanto para validação) e não menos eficiente, uma vez que exige apenas uma negociação preliminar acerca do início da seqüência e a cada interação uma especificação acerca da próxima comunicação.

O ***Serviço de Autenticação*** deve garantir que a origem das mensagens de gerenciamento são de entidades legítimas para evitar a execução de ações indevidas ou o acesso a informações por terceiros. Uma observação atenta à providência referente a alteração de mensagens citada acima (item *i*) pode levar a conclusão que a própria integridade oferece meios de aferir a autenticidade das mensagens, uma vez que somente o interlocutor autêntico conhecerá sua chave privada e com isso poderá gerar os campos criptografados de acordo com o esperado. A autenticação, então, está automaticamente incluída no Serviço de Integridade. Esta vantagem é resultado da forma como foram analisados e equacionados os problemas de segurança.

A abordagem sugerida para a solução dos problemas tem ainda a vantagem de permitir a instalação independente entre confidencialidade e os outros dois serviços (integridade e autenticação). Esta vantagem provém do fato de que, qualquer que seja o sistema de criptografia a ser empregado, a cifragem das mensagens completas sempre representa uma sobrecarga ao sistema e a confidencialidade pode ser dispensável em determinadas situações, obtendo-se nestes casos, ganhos de performance.

Também o sistema de chaves públicas adotado é uma vantagem por ser muito mais inteligente do que o sistema de chave única (ou secreta), já que dispensa um segundo modo de comunicação entre as entidades, sendo seguro até para troca de chaves sobre meios reconhecidamente inseguros.

Um grau de segurança adicional é conseguido com o uso de criptografia sobre a MIB. Empregando o conceito de que a MIB somente poderá ser acessada por um único agente, toda a informação poderá ser guardada criptografada com a chave pública

deste agente. Desta forma, só o mesmo agente pode ter acesso às informações geradas ou manipuladas por ele próprio.

5 Arquitetura de Segurança para Gerência de Redes

A seguir será apresentada a Arquitetura de Segurança proposta, seguida da apresentação detalhada dos algoritmos utilizados para incorporar segurança em um Sistema de Gerência de Redes genérico.

5.1 Modelo da Arquitetura de Segurança

Cada agente e gerente do Sistema de Gerência deve possuir uma *"Interface de Segurança"* que deve garantir que as mensagens recebidas pelos agentes e gerentes são realmente internas ao Sistema (autênticas) e que não foram alteradas (íntegras). Além disso, pode ser desejável a confidencialidade da comunicação entre as entidades do Sistema e esta característica também deve ser garantida pela Interface de Segurança. Esta interface atuará como uma "clearing house" entre cada par comunicante, impedindo que informações de gerência sejam acessadas, alteradas ou forjadas por entidades não autorizadas.

Os serviços diretamente implementados pela Interface de Segurança são:

- **Serviço de Autenticação**, garantindo a origem autêntica das mensagens;
- **Serviço de Integridade**, que impede o processamento de mensagens adulteradas ou forjadas;
- **Serviço de Confidencialidade de Comunicação**, tornando as mensagens inescrutináveis por terceiros, enquanto úteis;
- **Serviço de Confidencialidade de Acesso**, que garante a proteção às informações de gerência mantidas na MIB.

Todos os Serviços acima devem estar presentes nas Interfaces de Segurança dos agentes e dos gerentes componentes do Sistema de Gerência, à exceção do último, cuja presença somente é necessária nas entidades agente, pois diz respeito apenas a atividades destes.

Acessoriamente, são facilmente conseguidos como "efeito-colateral" da implantação dos serviços acima os seguintes:

- **Serviço de Controle de Acesso**, em função da Confidencialidade de Acesso: se apenas o proprietário da MIB pode "compreender" os dados lá mantidos, o problema de acesso está equacionado.
- **Serviço de Não-Repudiação**, resultado da implantação do Serviço de Autenticação: uma vez garantida a origem da mensagem, também não há como o remetente negar a autoria da mesma pois somente ele poderia gerar uma mensagem com campos criptografados pela chave privada dele (este é um mecanismo derivado da assinatura digital, porém mais poderoso).

Além dos serviços citados, é de grande importância que as Interfaces de Segurança mantenham registros das ocorrências em *logs* para que seja possível a realização de auditorias, como atividade de gerenciamento de segurança. Nos casos de tentativa de burla da segurança (detecção de mensagens alteradas ou re-apresentação de pacotes fora da seqüência, p.ex.) as Interfaces devem levantar alarmes de segurança para o Sistema de Gerência.

Interface de Segurança é, portanto, uma redoma que encapsula totalmente cada agente e cada gerente do Sistema de Gerência, de forma que toda comunicação entre estas entidades se dê somente através da Interface. Esta abordagem permite que a instalação da Interface seja transparente para os agentes e gerentes, ou seja, nada é alterado nos agentes e gerentes para que a Arquitetura de Segurança seja implantada. As comunicações entre entidades, porém, passarão sempre por filtros (as Interfaces de Segurança) em cada um dos lados desta comunicação (figura 1), para verificação de integridade e autoria e para garantir privacidade.

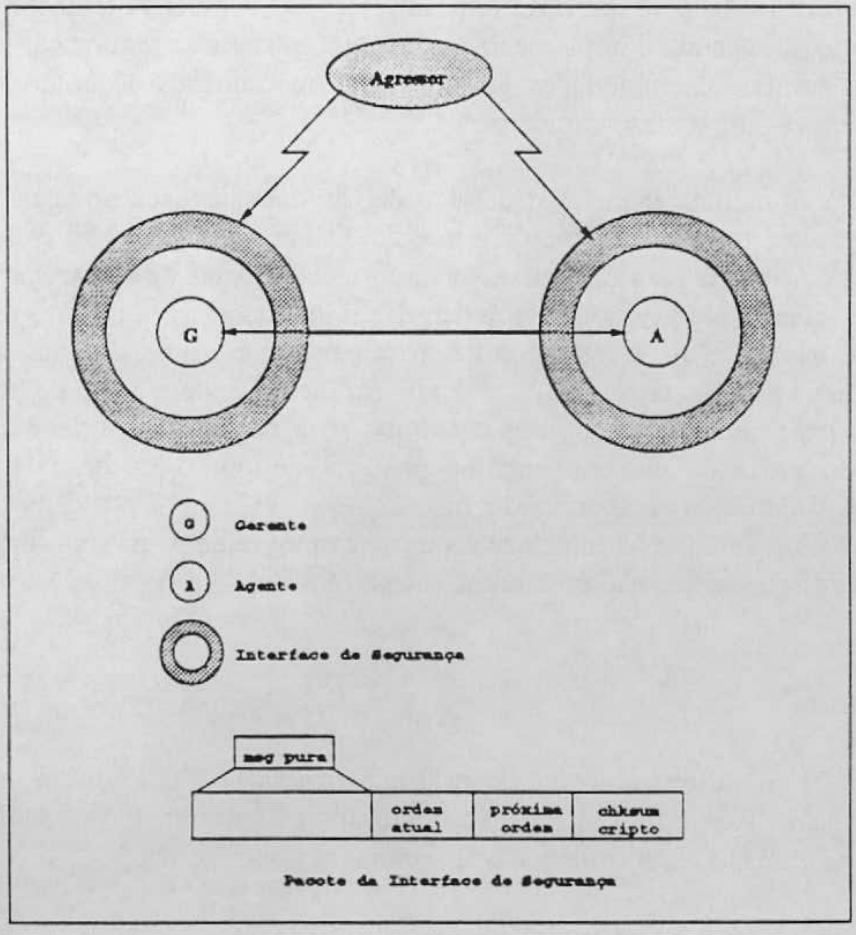

Figura 1: Interface de Segurança

Somente trafegarão na rede (no escopo de Sistemas de Gerência) pacotes de comunicação entre Interfaces de Segurança que encapsulam pacotes de agentes e gerentes, com todos os mecanismos de segurança para evitar possíveis agressões. A interface de

segurança emissora é responsável pela incorporação dos mecanismos no pacote original e a interface do lado receptor é responsável pelas verificações e liberação ou não de pacotes.

O acesso às informações de gerência guardadas na MIB também deve ser restrito. Existem duas formas de prover tal restrição: pela instalação de um mecanismo de controle de acesso próprio ou a criação de um mecanismo de confidencialidade, onde as informações armazenadas na MIB estariam cifradas. A estratégia de estabelecer um Serviço de Confidencialidade no acesso à MIB, garantindo que um e somente um agente (o seu criador e mantenedor) terá acesso direto às informações lá contidas, se apresenta como a mais interessante. Três itens motivam esta escolha:

- o mecanismo de confidencialidade já está disponível para outros serviços de segurança (Confidencialidade de Comunicação), eliminando a necessidade de construção de um novo mecanismo de segurança, o controle de acesso;
- elimina a necessidade de criação de uma Interface de Segurança também para a MIB, centralizando nos agentes a implementação dos mecanismos de segurança;
- não possui certas vulnerabilidades presentes nos mecanismos de controle de acesso, como a abertura para o mascaramento.

A forma de implantar o Serviço de Confidencialidade no acesso à MIB é o uso de criptografia em todos os acessos à mesma. O agente responsável pela MIB possui uma chave que é utilizada para cifrar todas as informações antes de armazená-las e decifrar as informações quando do acesso. A cifragem das informações contidas na MIB pode ser feita com a mesma chave que o agente utiliza para garantir a privacidade das comunicações ou com uma chave própria para a tarefa, podendo ser inclusive com o uso de uma técnica de chave secreta, mais eficiente em termos de tempo para criptografar e decriptografar. Isto porque o acesso à MIB é completamente independente de todo o processo de comunicação entre entidades. Tal mecanismo permite inclusive que o acesso em si possa ser realizado sem restrições, mas uma vez que as informações estão criptografadas, não há liberação efetiva das mesmas para aqueles que não possuírem as chaves.

5.2 Algoritmos

Os algoritmos utilizados para a implementação das Interfaces de Segurança são divididos em Algoritmos para Autenticação e Integridade e Algoritmos para Confidencialidade. Estes algoritmos estão apresentados a seguir:

5.2.1 Algoritmos para Autenticação e Integridade

Para se conseguir a garantia de autenticidade e integridade das mensagens que são trocadas entre as entidades componentes do Sistema de Gerência, cada Interface de Segurança deve implementar (indistintamente para agentes e gerentes) os algoritmos para o envio e o recebimento de mensagens a seguir (as figuras 2 e 3 apresentam os diagramas de estados dos algoritmos), além de uma negociação preliminar para troca de informações que

serão necessárias para o desenrolar das comunicações, como as chaves públicas das duas interfaces e a determinação do primeiro valor que será utilizado para garantir a ordem das mensagens.

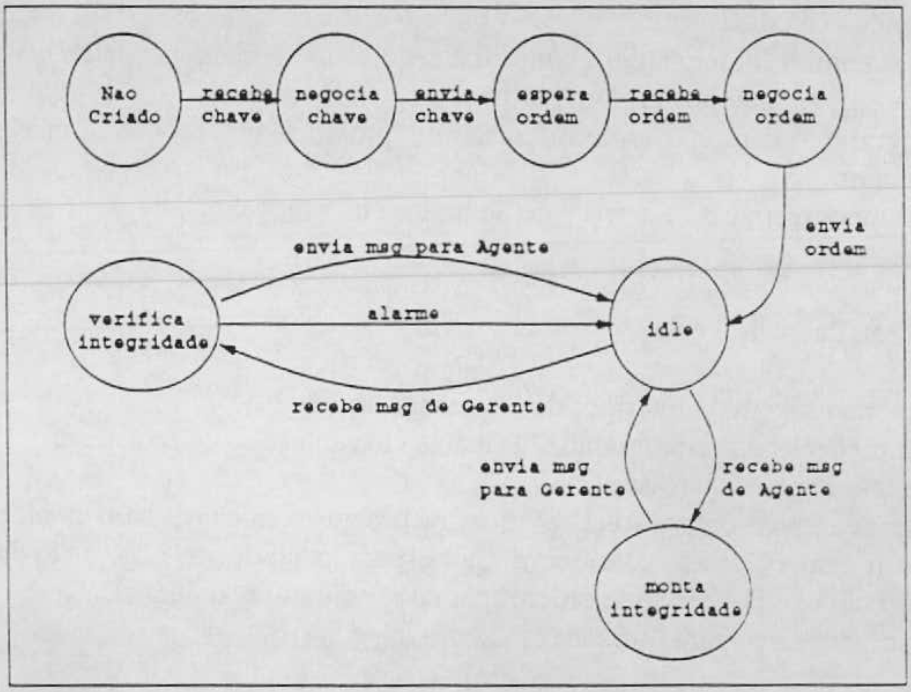

Figura 2: Integridade e Autenticação no Agente

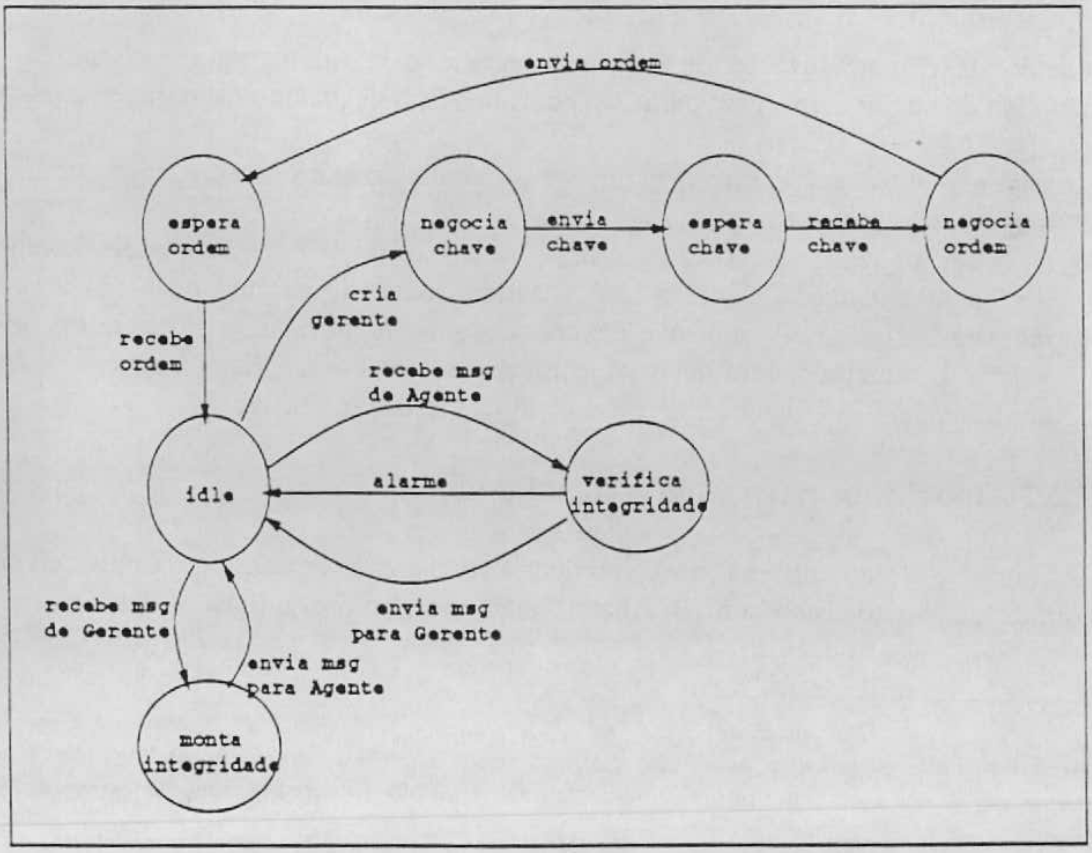

Figura 3: Integridade e Autenticação no Gerente

- Envio de mensagens

1. Recebe mensagem da Entidade "pura"[7]
2. Calcular checksum da mensagem e criptografá-lo com chave privada própria, agregando-o na mensagem
3. Agregar campo "ordem atual", conforme negociado previamente entre as partes
4. Gerar e agregar campo "próxima ordem"
5. Criptografar campos "ordem atual" e "próxima ordem" com chave pública do destinatário
6. Enviar mensagem para Interface de Segurança homóloga

- Recepção de mensagens

1. Recebe mensagem da Interface de Segurança homóloga
2. Decifrar checksum criptografado, usando a chave pública do remetente
3. Calcular e conferir checksum
4. Decifrar campos "ordem atual" e "próxima ordem" com chave privada própria
5. Conferir campo "ordem atual" com valor esperado, conforme negociado previamente
6. Armazenar campo "próxima ordem" para uso em futura comunicação
7. Enviar mensagem para Entidade "pura"

- Negociação Preliminar

Quando da disponibilização de um novo agente para um gerente, este último toma a iniciativa de enviar mensagem para "negociação". Esta negociação se dará em 2 passos:

1. Devem ser trocados entre o gerente e o agente em questão suas chaves públicas, por iniciativa do gerente.
2. Deve ser realizada a negociação sobre o valor inicial que conterá a ordem das mensagens para a manutenção da integridade e autenticidade. O gerente deve enviar mensagem indicando o primeiro valor que deverá ser usado na primeira mensagem operacional. O valor da primeira ordem deve ser confirmada pelo agente. Estas mensagens devem ser confidenciais, já utilizando as chaves públicas trocadas a priori.

5.2.2 Algoritmos para Confidencialidade

Conforme apresentado, há dois momentos onde é necessária a confidencialidade: na comunicação e no acesso à MIB. Abaixo estão os algoritmos utilizados neste casos.

---

[7] *Por entidade "pura" se entende agente ou gerente do Sistema de Gerência sem os mecanismos de segurança aqui descritos, ou seja, conforme originalmente implementados. Toda comunicação entre entidades puras agora se dá através da Interface de Segurança apresentada.*

5.2.2.1 Confidencialidade na Comunicação

A confidencialidade na comunicação deve ser garantida quando requisitada. As atividades relativas à confidencialidade devem ser realizadas sobre uma mensagem já preparada pelos mecanismos de Integridade e Autenticação, sendo realizada, portanto, um nível abaixo. A Interface de Segurança deve, então, implementar o algoritmo abaixo:

- Envio de mensagem

1. Recebe mensagem da Entidade "pura"
2. Agregar mecanismos de Integridade/Autenticação (5.2.1)
3. Criptografar mensagem com chave pública do destinatário
4. Enviar mensagem para Interface de Segurança par

- Recepção de mensagem

1. Recebe mensagem da Interface de Segurança par
2. Decifrar mensagem, usando chave privada própria (5.2.1)
3. Verificar Integridade/Autenticação
4. Enviar mensagem para Entidade "pura"

5.2.2.2 Confidencialidade no Acesso à MIB

Para a confidencialidade das informações contidas na MIB, é necessário apenas que a Interface de Segurança dos Agentes contemple o seguinte:

- Acesso à Informação da base

1. Recebe solicitação de acesso da Entidade "pura"
2. Busca na MIB a informação desejada, que estará criptografada
3. Decifra a informação, com a chave privada própria
4. Envia informação para Entidade "pura"

- Manutenção de Informação

1. Recebe solicitação de manutenção de informação da Entidade "pura"
2. Criptografa informação com chave pública própria
3. Armazena/Altera informação na MIB

6 Conclusão

Foi apresentada aqui uma Arquitetura de Segurança genérica para aplicação em Sistemas de Gerência de Redes. Tal arquitetura é extremamente flexível uma vez que permite sua aplicação em todos os Sistemas de Gerência baseados em entidades agentes e gerentes e, ao mesmo tempo, não exige que tais entidades sofram alterações para suportá-la, tornando transparente a sua instalação. Também permite que os Serviços de Segurança disponibilizados por ela sejam seletivamente implantados, conforme necessidades de cada instalação e restrições de desempenho.

Apesar de possuir uma estrutura simples e não incluir grande sobrecarga ao sistema como um todo, são oferecidos pela arquitetura os serviços de autenticação, integridade, confidencialidade (de comunicação e de acesso), não-repudiação e controle de acesso. As novidades da abordagem utilizada dizem respeito à utilização de sequenciamento constante (a cada mensagem trocada entre entidades é realizada uma verificação da origem - autenticação), a ampliação do conceito de assinatura digital (que permite não só validar a origem mas também a integridade das mensagens) e ao controle de acesso à MIB ser feito através do serviço de confidencialidade (que não impede o acesso mas não revela as informações senão para o legítimo proprietário).

A princípio, a arquitetura oferece um ambiente confiável para Sistemas de Gerência de Redes; mas como tudo relacionado com segurança[8], somente após muitos testes e análises e a submissão da implementação a sistemas em produção, vulneráveis a ataques de toda ordem, é que será possível a sua validação. Além disso, a validação estará fortemente associada com os algoritmos de criptografia utilizados pelos diversos serviços integrantes da arquitetura; muito mais do que em relação à arquitetura.

Bibliografia

[BAL 92] BALL, L. L. *Cost-Efficient Network Management*, McGraw-Hill, 1992.

[BRI 92] BRISA, *Gerenciamento de Redes: Uma Abordagem de Sistemas Abertos*, Makron Books, 1993.

[COL 89] COLLINS, W. *OSI Management Services Elements, Protocols and Application Layer Structure (ALS)*, Proc. of Integrated Network Management I, 1989.

[COO 89] COOPER, J. A., *Computer and Communications Security*, McGraw-Hill, 1989.

[DOD 83] USA DEPARTMENT OF DEFENSE COMPUTER SECURITY CENTER, *Trusted Computer System Evaluation Criteria - Orange Book*, CSC-STD-001-83, EUA, 1983.

---

[8] *Algoritmos de criptografia e segurança em geral nunca são considerados totalmente confiáveis. O máximo que se afirma acerca de um mecanismo de segurança é que "até aquele momento" não existem ou não foram publicadoas formas de se sobrepujar os mesmos.*

[GAL 91] GALVIN, J. M. & McCLOGHRIE, K. & DAVIN, J.R., *Secure Management of SNMP Networks*, Prof. of Integrated Network Management II, 1991.

[ISO 89] ISO/TC 97, *IS-ISO 7498-2: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*, 1989.

[KAR 91] KARILLA, A. T., *Open Systems Security: An Architectural Framework*, Helsink, Finlândia, 1991. (Tese de Doutorado)

[KLE 88] KLERER, S. M, *The OSI Management Architecture: an Overview*, IEEE Network, vol.2, n° 2, pp 20-29, março 1988.

[NEC 90] NECHVATAL, J., *Public Key Cryptography*, National Institute of Standards and Technology - NIST, EUA, 1990.

[OMU 90] OMURA, J., *Novel Applications of Cryptography in Digital Communications*, IEEE Communications Magazine, pp 21-34, maio 1990.

[PFL 89] PFLEEGER, C. P., *Security in Computing*, Prentice-Hall, 1989.

[ROT 93] ROTEMBERG, M., *Communications Privacy Implications for Network Design, Comm. of the ACM*, vol 36, n° 8, pp 87-95, agosto 1993.

[SEV 89] SEVCIK, P. J. & KORN, L. K., *A Network Monitoring and Control Security Architecture*, Proc. of Integrated Network Management I, 1989.

[SOU 92] SOUZA, R., *Arquitetura e Gerência de Segurança no OSI*, Anais OSI/92, São Paulo, 1992.

[TAN 91] TANEMBAUM, A. *Computer Networks*, 2a. ed., Prentice-Hall, 1991.

[WES 92] WESTPHALL, C. B. & ASSOUL, S. *Management Architecture for Networks of the Future*. IEEE/IFIP Distributed Systems: Operation and Management. Munich, Alemanha, 1992.