Aula 02: Princípios da Segurança da Informação

Prof. Daniel Caetano

Objetivo: Apresentar alguns dos conceitos fundamentais que regem a Segurança da Informação, discutindo aspectos de segurança lógica e segurança física.

Bibliografia: FERREIRA, 2003; FERREIRA E ARAÚJO, 2006.

INTRODUÇÃO

Vários dos principais aspectos da segurança da informação dependem de que os sistemas saibam quem a pessoa que está solicitando determinadas informações, seja para registrar a operação sob sua responsabilidade, seja para verificar se aquela pessoa tem acesso ao conteúdo ou permissão para alterá-lo.

Uma outra situação em que é importante ter certeza de quem é a pessoa operando um sistema é quando ela envia uma mensagem ou assina um documento. Uma assinatura deve ter a propriedade de garantir a autoria daquela mensagem ou documento.

Em ambos os casos, pode-se espera que o indivíduo se identifique perante o sistema; por outro lado, não é possível tomar essa informação por verdadeira sem que seja feita uma conferência.

Além disso, uma vez que um profissional é promovido a um cargo de gerência de segurança da informação ou de sistemas, ele precisa ter em mente que são de sua responsabilidade não apenas a segurança contra hackers que ameaçam a informação através da rede de computadores, mas também envolve a segurança dos equipamentos, num sentido mais físico.

Cabe então a este profissional responder a algumas perguntas: "como proteger meus equipamentos?" ou "caso meus equipamentos sejam perdidos, como assegurar a recuperação dos dados?"

Nessa aula serão discutidos alguns desses aspectos, bem como será discutidas algumas formas de resolver o problema de conferir a identidade de um usuário. Serão discutidos também problemas de segurança lógica e física.

1. PROBLEMAS DE AUTENTICIDADE

Imagine que um dia você chegue no serviço e todos comecem a se despedir de você. Ao falar com seu chefe, você descobre que ele, tristemente, concordou com um pedido de demissão enviado por e-mail e **em seu nome**. Você de fato enviou um e-mail, mas era um relatório e não esse pedido de demissão que você não reconhece! Como resolver essa situação agora?

Esse não é o único problema que pode acontecer envolvendo a **identidade** de alguém. São vários os possíveis problemas. Por exemplo:

a) Alguém enviar uma mensagem em seu nome.
b) Alguém acessar um sistema em seu nome.
c) Alguém visualizar documentos que só você deveria.
d) Alguém interceptar mensagens que eram destinadas a você.

Dentre inúmeras outras.

Consertar esse tipo de situação pode ser bem difícil; na verdade, o ideal é que essas situações simplesmente não ocorram.

Sendo assim, em segurança da informação temos que garantir a **autenticidade** dos documentos e usuários, autores e receptores, permitindo garantir o **não-repúdio**.

A **autenticidade** é a característica daquilo que não foi adulterado. Sendo assim, se garantirmos a autenticidade, o autor da mensagem será quem diz ser, o conteúdo da mensagem será exatamente o que o autor criou, e o destinatário da mensagem será exclusivamente aquele que o autor pretende que seja.

Resumidamente, a autenticidade é garantida por três mecanismos:

1) Autenticação de Destino: Apenas o destinatário consegue ler a informação armazenada ou transmitida.
2) Integridade da Informação: Evitar que intermediário altere a informação:
3) Autenticação da Origem: Se a mensagem diz ser de um autor, ele deve ser, de fato, esse autor.

Garantindo-se todos esses requisitos, garante-se também o **não-repúdio**, isto é, o autor de uma mensagem (ou um comando, ou um acesso) não poderá negar que foi, de fato, o autor.

Como atingir a esses objetivos?

Bem, a coisa ganha contornos distintos dependendo se tratar de segurança lógica ou física. Vamos começar falando da segurança lógica.

2. CONTROLE DE ACESSO LÓGICO

Conceitos Chave:

- Segurança => Controle de Acesso
- Envolve: usuário + recurso
- Quem pode o quê?
  * Padrão: tudo é proibido, a menos que permitido
- Objetivos:
  * Proteger informações e transações
  * Monitoramento de acesso
- Procedimento:
  * Identificação: saber quem o usuário diz ser
    + UserID
  * Autenticação: comprovar que o usuário é quem diz ser
    + Password, Biometria, Cartão...
    + Algo que o usuário tem + Algo que o usuário sabe
- Permite responsabilização de usuários
- Dificuldades
  * UserIDs podem ser facilmente obtidos
  * Cartões podem ser roubados, mas são preferíveis
  * Senhas: longas, não óbvias, e não usadas em outros sistemas
    + Podem ser, ainda assim, roubadas.
  * Biometria: custo, variações
- Medida adicional: limitar tentativas de logon fracassadas

A segurança da informação, seja em qual nível for, sempre implicará em controle de acesso, seja ele físico (portões, muros etc.) ou lógico (login, logging etc.). O controle de acesso lógico deve sempre englobar o recurso que se pretende proteger e o usuário a quem se pretende dar privilégios de acesso.

De forma geral, um primeiro passo para uma boa política de controle de acesso é: **tudo é proibido a menos que expressamente permitido**. Isso está de acordo com a regra *praticidade = 1/ segurança* que foi mencionada anteriormente.

Assim, claramente o controle de acesso lógico reduz a praticidade do sistema. Mas qual é o objetivo central do controle de acesso? São, basicamente, dois os pontos de interesse:

- Proteger informações e transações de usuários não-autorizados;
- Monitoramento do acesso a recursos críticos para a empresa.

2.1. Procedimento do Controle de Acesso

O controle de acesso é feito, usualmente, através de dois processos: identificação e autenticação. O primeiro deles (identificação) permite ao sistema reconhecer qual usuário pretende acessar a informação, para identificar quais são suas permissões. O segundo (autenticação) permite ao sistema comprovar a identidade do usuário, visando impedir que uma pessoa se passe por outra. O processo completo de identificação e autenticação se chama "*logon*" ou "*login*".

O termo "*logon*" ou "*login*" significa aproximadamente algo como "criar uma entrada no *log*". *Log* é o nome em inglês para arquivos de registro de acesso. Mais detalhes sobre o arquivo de *log* serão apresentados mais adiante.

Usualmente, a identificação é feita por algum tipo de informação única para cada usuário, como um *número de funcionário* (*userid*, que deve ser único), que pode ser digitado manualmente ou fornecido através de um cartão, por exemplo.

Após a identificação, o sistema deve fazer a autenticação, para ter certeza de que o usuário que realiza o acesso é realmente quem diz ser. Assim, o usuário deve fornecer uma senha (password), por exemplo. Outras formas de autenticação são os sistemas de medição biométrica (como timbre de voz, exame de retina, leitura de digital etc.). É comum se afirmar que o login, ou seja, a identificação/autenticação, é feita por uma combinação entre algo que o usuário tem e algo que ele sabe, associado à sua identificação de usuário.

Biometria é uma área do conhecimento que estuda medidas únicas de seres vivos - em especial o ser humano, visando a obtenção de medidas que sejam únicas de indivíduo para indivíduo, de forma que esta medição possa ser usada para identificação e/ou autenticação de sistemas.

2.2. Dificuldades de Alguns Métodos de Identificação/Autenticação

Por permitir que todas as ações do usuário dentro do sistema sejam monitoradas e registradas, o *logon* é muito importante, pois permite que sejam apuradas as responsabilidades em casos de problemas de segurança. Entretanto, o *logon* precisa ser resistente às tentativas de invasão; caso um invasor utilize um *logon* de algum funcionário, a responsabilidade recairá sobre este funcionário.

Neste panorama, algumas tecnologias possuem alguns problemas. Cartões de identificação podem ser perdidos, mas *userids* que precisem ser digitados podem ser obtidos por outras pessoas ainda mais facilmente. Por esta razão, os cartões de identificação costumam ser a forma mais bem aceita de se identificar num sistema.

Para diminuir os riscos de uma tentativa de invasão, também a autenticação exige algumas providências de segurança. Usualmente são usadas senhas, o que é um bom método de autenticação, caso a senha não seja curta, óbvia e seu dono não a tenha escrito em algum lugar (incluindo aqui não tê-la usado em outros sistemas). Entretanto, senhas podem ser facilmente roubadas, o que tem levado a muitas empresas adotarem senhas conjuntamente com sistemas de medição biométrica para a autenticação de usuário, já que a medição biométrica costuma ser menos passível de falsificação, embora tenha seus problemas com falsos negativos e seu custo elevado.

De qualquer forma, usualmente são tomadas previdências adicionais com relação ao processo de autenticação, para frustrar qualquer tentativa de invasão: o número de tentativas incorretas de *logon* costuma (e deve) ser limitado. Usualmente considera-se que três tentativas incorretas é um bom valor para bloquear uma dada conta de usuário.

Três tentativas é um valor considerado razoável para serviços de importância, que são usados com relativa frequência e que, em geral, envolvem responsabilidade ou movimentações financeiras. Caso não sejam estas as características da aplicação, é razoável ampliar o número de tentativas para 9 ou 10 antes de bloquear um usuário.

2.3. Gerenciamento de Usuários e Controle de Log

Conceitos Chave:

- Auditoria => apuração de falhas e responsabilidades
- Análise de Logs: muito importante
  * Logs precisam registrar TUDO que o usuário fez
  * Logs precisam registrar QUEM fez tudo
- Administradores de Sistema
  * Implementar cadastro/autorizações de usuários
  * Equipe de Administradores... tomar cuidados
    + Comunicação
    + Controle de Alterações
    + UserIDs diferentes para cada administrador
  * Gerenciamento de Logs
    + Sincronia de Relógios da Rede
    + Armazenamento de Logs - protegido dos usuários
    + Rotação de Logs (Backup após análise)
  * Logs: Locais x Remotos x Mistos
  * Auditorias Frequentes

Normalmente, se a segurança do sistema for bem planejada e for bem administrada, a maioria das falhas de segurança e identificação de responsabilidades são possíveis através de auditoria. Um dos principais instrumentos de auditoria são os arquivos de registro de acesso e uso do sistema, os chamados logs.

Em muitos casos, a análise dos logs é o único instrumento que possibilita essas identificações e, por esta razão, é de extrema importância que os logs fiquem protegidos da ação direta dos usuários. É preciso, também, garantir que os logs registrem de fato tudo que foi feito e qual foi o usuário que realizou cada uma das ações.

Em geral, para que isso seja conseguido, existe uma pequena equipe de administradores de sistema que cuidam de implementar o cadastro e as autorizações a usuários selecionados por níveis superiores. Para que esta equipe funcione bem, algumas regras são necessárias:

- Comunicação (registro de alterações feitas, problemas encontrados, etc.)
- Controle de Alterações (registro de autoria das modificações, para contato futuro)
- Um *userid* para cada administrador.

Considerando que o gerenciamento de usuários é adequado, também é função dos administradores cuidar do gerenciamento de logs. O primeiro e mais importante fato é cuidar da sincronia dos relógios das diferentes máquinas, como já foi citado anteriormente, de forma a permitir o rastreamento das ações dos usuários que ocorrem sequencialmente nas diversas máquinas.

A segunda medida é cuidar do adequado armazenamento dos logs. Uma primeira medida é garantir uma partição especial para os logs locais, para evitar os problemas já citados. Outra medida é a rotação dos logs, transportando logs mais antigos (já revisados) para mídias de armazenamento como DVDs, liberando espaço para logs mais recentes.

Em alguns sistemas, entretanto, a manutenção de logs locais não é adequada, dado que estão sujeitos a serem destruídos. Nestes casos, é interessante usar um equipamento dedicado a armazenar o log de tudo que é feito em outras máquinas. Esta medida tem algumas limitações, como banda de transmissão, problemas para registrar ações do usuário local caso a rede caia etc. Algumas vezes é usado um misto de ambos os sistemas.

É importante ressaltar que os logs devem ser monitorados periodicamente, e a frequência com que isso é feito deve ser tão maior quanto mais crítico for o acesso ao sistema. Qualquer evento estranho deve ser devidamente investigado, de forma a averiguar sua origem e normalidade.

2.4. Assinaturas Digitais

Conceitos Chave:

- Requisitos da Assinatura Digital
  * Receptor deve poder verificar a identidade alegada do transmissor
  * O transmissor não pode repudiar o conteúdo da mensagem
  * O receptor/intermediário não tenha como alterar/forjar a mensagem

Os mecanismos vistos anteriormente são bons para que o usuário seja identificado ao acessar um sistema, para que esse sistema saiba se ele pode ou não realizar determinadas operações ou mesmo se ele pode acessar algum documento. São bons também para identificar o responsável por algum problema. Por outro lado, não são muito bons para garantir a transmissão de mensagens íntegras.

Para garantir a transmissão de mensagens autênticas e o não-repúdio, precisaremos recorrer às assinaturas digitais. Como elas funcionam?

Bem, sinteticamente, para que documentos possam ser trocados pela rede substituindo os documentos físicos, é necessário um sistema que respeite os seguintes requisitos:

1) O receptor possa verificar a identidade alegada do transmissor
2) O transmissor não possa repudiar o conteúdo da mensagem
3) O receptor/intermediário não tenha como alterar/forjar ele mesmo a mensagem

A forma mais comum é um sistema de **criptografia de chave pública**. Nesse sistema, há **duas chaves: a privada e a pública**. A chave privada tem esse nome porque apenas o autor da mensagem a possui; a chave pública está disponível para todos, em um local público e confiável.

Simplificadamente, o autor gera um número – chamado **hash** – que é único para a mensagem que ele pretende enviar. Esse número é, então, codificado com a chave privada do autor e enviado para o destinatário, junto com a mensagem. No destinatário, esse número só poderá ser decifrado com a chave pública do autor, e o destinatário poderá verificar se o número enviado pelo autor corresponde ao hash da mensagem, que o destinatário também consegue gerar. Se o hash gerado pelo destinatário e o enviado pelo autor forem os mesmos, podemos confirmar que a mensagem não foi alterada – o hash permanece igual – e que o autor é quem diz ser – pois foi possível decifrar o hash com a chave pública dele.

Agora que compreendemos a segurança lógica em boa parte de sua dimensão, vamos falar um pouco também da segurança física.

3. SEGURANÇA FÍSICA x LÓGICA

Conceitos Chave:

- Aspectos Lógicos x Físicos
  - * Dado em Si x Meio Portante
  - * Integridade Lógica x Integridade Física
- Segurança Lógica
  - * Processo lógico do controle de acesso
    - + Identificação e Autenticação
    - + Registro em logs
    - + Controle de Permissões de Acesso
  - * Evitar que a informação seja alterada/apagada indevidamente
  - * Evitar que estranhos entrem na sala do servidor (controle da porta, p.ex.)
- Segurança Física
  - * Aspectos físicos do controle de acesso
  - * Dão suporte aos mecanismos lógicos
    - + Se a identificação/autenticação for falha, quem barra o sujeito?
      - = A porta
      - = O muro
      - = A grade
  - * Ligada apenas à integridade física
    - + Filosofia: "Destruição" Física implica "Destruição" Lógica

Sempre que se fala em informação, há dois aspectos a serem considerados: os lógicos e os físicos. Pode-se falar em manter a integridade lógica, ou seja, da informação em si ou em manter a integridade física da informação, ou seja, do meio portante (equipamentos e mídias, por exemplo).

Assim, cabe apresentar os conceitos de segurança lógica e segurança física. A segurança lógica é aquela que tem sido apresentada com mais ênfase no momento, relativa ao processo lógico do controle de acesso (como *login* e senha, *log* de acesso etc.) e é usada para garantir tanto a integridade lógica (mudança do conteúdo dos documentos) quanto a integridade física (destruição física dos equipamentos e/ou documentos).

A segurança física, por outro lado, lida com os aspectos físicos do controle de acesso (como muros, portas, câmeras, sistemas de fechadura eletrônicos etc.). Embora seja possível dizer que a destruição ou roubo de um documento provoque um dano ao seu conteúdo lógico (que pode ter deixado de existir), não é comum fazê-lo. Em geral se faz

ligação da segurança física apenas à integridade física da informação (ou seja, do equipamentos e mídias).

3.1. Segurança Lógica na Integridade Física

Conceitos Chave:
- Papel Chave no Controle de Acesso Físico
  * "Não há equipamento seguro se o intruso tiver acesso físico ao eqpto."
  * 72% dos ataques são causados por funcionários (FBI)
    + 20% são causados por terceiros autorizados pela empresa
    + 8% são causados por agentes externos (pessoas sem permissões)
- Limitar e Registrar o acesso físico
  * Quem é, o que Possui/Sabe
- Controle de Acesso Físico Automatizado => Segurança Lógica
  * Software que faz o controle de acesso
  * Características desejáveis de um sistema deste tipo
    + Proteção contra ataques forçados (força bruta/corte de energia)
    + Atualização do Sistema (número de usuários e privilégios)
    + Registro de Acessos (data, hora, usuário, local, no. de tentativas)
    + Autenticação por Senha (smartcard + senha)
    + Bloqueio de Múltiplos Acessos (entrar duas vezes sem sair?)
    + Flexibilidade (controle centralizado de acesso)
    + Monitoração (log de uso indevido, falhas...)
    + Sistema de Backup (sistemas sobressalentes, base de dados...)
    + Proteção dos Equipamentos (segurança máxima!)

Na área de segurança lógica, além da usual preocupação com o acesso aos dados através de redes, existe grande preocupação também com o controle de acesso físico (obviamente, em combinação com os aspectos da segurança lógica).

Alguns autores chegam a dizer que "não há equipamento seguro se o intruso tiver acesso físico ao equipamento". Segundo o FBI, 72% dos ataques (fraudes, roubos, sabotagens, etc.) são causados por funcionários da própria empresa. Cerca de 20% são causados por terceiros autorizados pela empresa a manipular as informações e apenas cerca de 8% dos ataques são causados por agentes externos (por redes ou por pessoas sem permissões de acesso).

Assim, além do usual papel de bloquear acessos indesejáveis aos dados através de terminais ou rede, o controle de acesso tem também a função de limitar o acesso físico. Assim como no controle de acesso mencionado quando a Integridade Lógica foi apresentada, mais uma vez surgem os elementos: "quem é o indivíduo", "o que ele possui"

e/ou "o que ele sabe". É importante relembrar que os sistemas de controle de acesso devem se basear ao menos em dois destes elementos.

Mas se estamos falando de acesso físico, porque "Segurança Lógica"? Porque a maioria do acesso físico de segurança é, hoje, automatizado. E existe um software por trás da automação destes dispositivos físicos de controle de acesso. Ou seja: este software e seu funcionamento são os aspectos lógicos envolvidos.

Os sistemas de controles de acesso físico automatizado devem ter as seguintes características:

- Proteção contra ataques forçados (força bruta, corte de energia etc.).
- Atualização do sistema (maior número de usuários, mudanças de privilégios etc.).
- Registro de acessos (log de data, hora, local, usuário, tentativas frustradas).
- Autenticação por senha (preferencia um sistema de smartcard + senha)
- Bloqueio de múltiplos acessos (quem já está dentro não pode entrar novamente).
- Flexibilidade (controle centralizado das permissões de acesso de cada elemento das instalações (elevadores, portões etc.)).
- Monitoração (monitoração, com geração de log, de uso indevido das instalações, violações, mal-funcionamento, falta de energia).
- Sistema Backup (sistemas sobressalentes para situações críticas de falha... cuidados com a base de dados!).
- Proteção dos Equipamentos (segurança máxima para o sistema que administra o controle de acesso físico).

Muitas destas características são similares às já comentadas quando o assunto era o controle de acesso para manutenção da integridade lógica, mas algumas são distintas. É importante ressaltar que nem todas as empresas precisam de sistemas tão complexos, sendo necessária uma avaliação caso a caso.

3.2. Segurança Física

Conceitos Chave:

- Segurança Física sem Segurança Lógica => Cadeado => Ok
- Segurança Lógica sem Segurança Física => Pula Muro => Não Ok
- Investimento => Segurança Física
- Controle de Acesso Físico:
  * Grades, muros, portas
  * Guardas
  * Crachás
  * Sistemas de Portas Duplas
- Segurança Física é só Controle de Acesso?
  * Proteção contra agentes naturais ou criminosos!
  * Dificultar espionagem

De nada adianta um segurança lógica perfeita em um sistema de controle de acesso se a segurança física for falha. Por exemplo: se o sistema de identificação e autenticação for perfeito mas o funcionário puder entrar em uma dada sala ignorando solenemente o tal sistema, ele terá falhado completamente.

Assim, uma boa parte do investimento do controle de acesso está na segurança física. Alguns dos tipos do controle de acesso físico são:

- Grades, muros, portas (limites das regiões restritas, monitoradas)
- Guardas (garantir o controle de acesso em pontos estratégicos - como as entradas - checagem de visitantes).
- Crachás (identificação dos funcionários e visitantes. Quanto menos informações, melhor).
- Sistemas de Portas Duplas (obrigar a identificação, evitando que intrusos "entrem junto" com pessoas autorizadas).

Entretanto, o aspecto de segurança física engloba mais que o controle de acesso. É preciso que as informações estejam protegidas fisicamente contra agentes naturais ou criminosos (fogo, explosões, inundações, corte de energia etc.).

Além disso, as instalações onde serão armazenadas informações sensíveis devem ser projetadas de forma a dificultar espionagem, até mesmo com isolamento, no caso de informações especiais.

4. BIBLIOGRAFIA

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, F. N. F; ARAÚJO, M. T. **Política de Segurança da Informação: Guia Prático de Elaboração e Implementação**. Rio de Janeiro: Ciência Moderna, 2006.