REFERÊNCIAS

ARNOLD, T., HOPTON, D.,LEONARD, A., FROST, M. **Professional Software Testing With Visual Studio 2005 Team System: Tools For Software Developers And Test Engineers.** Wiley-India, 2007.

BRASIL. Constituição (1988).

BRASIL. Decreto nº 4.553, de 27 de dezembro de 2002.

CMMI. Capability Maturity Model Website. Disponível em: <http://www.sei.cmu.edu/cmmi/general/index.html>. Acesso em: 29 jul 2009.

CRINGLEY, R. X. **Accidental Empires: How the Boys of Silicon Valley Make Their Millions, Battle Foreign Competition and Still Can't Get a Date.** 2nd ed. USA: Penguin Books, 1996.

FARIS, T. H. **Safe and sound software: creating an efficient and effective quality system for software medical device organizations.** USA: American Society for Qualit, 2006.

FORTIFY. Application Security - Fortify Software. Disponível em: <http://www.fortify.com/>. Acesso em: 29 jul 2009.

HARRIS, S. **CISSP All-in-One Exam Guide.** 3rd ed. USA: McGraw-Hill Osborne Media, 2005.

ISC2. Certification CISSP. Disponível em: <http://www.isc2.org/cissp/default.aspx>. Acesso em: 16 maio 2009.

KOCK, N. F. **Systems analysis & design fundamentals: a business process redesign approach.** USA: SAGE, 2006.

MORIMOTO, C. E. **Redes, Guia Prático.** Porto Alegre, RS: GHD Press e Sul Editores, 2008.

NBR/ISO/IEC 17799. **Tecnologia da Informação: Código de prática para a gestão da segurança da informação.** Associação Brasileira de Normas Técnicas ABNT, 2002.

PAUL, M. The need for secure software. **Software Community (ISC)² Whitepapers.** Disponível em: <http://www.isc2.org/uploadedFiles/(ISC)2_Public_Content/Certification_Programs/CSSLP/CSSLP_WhitePaper.pdf>. Acesso em: 12 set 2009.

PRADHAN, D. **Fault-Tolerant System Design.** New Jersey: Prentice Hall, 1996.

RUSSELL, D., GANGEMI, G. T. **Computer Security Basics.** USA: O'Reilly, 1991.

SANTOS, G. P., SILVA, W. C., NALIN, M. Segurança da Informação: da Constituição e Atuação do Conselho Gestor de Segurança na Organização Militar. **Revista Científica da Escola de Administração do Exército,** Salvador, v. 1, n. 2, p. 6-19, 1º semestre de 2006.

SCHNEIER, B. **Applied Cryptography.** John Wiley & Sons, 1996.

SCHNEIER, B. **Secrets & Lies: Digital Security in a Networked World.** John Wiley & Sons, 2000.

SCHNEIER, B. **Applied cryptography: protocols, algorithms, and source code in C.** Wiley-India, 2007.

SÊMOLA, M. **Gestão da Segurança da Informação.** Editora Campus, 2003.

STALLINGS, W. **Data and Computer Communications.** Upper Saddle River: Prentice Hall, 2000.

STAMP, M. **Information security: principles and practice.** USA: John Wiley and Sons, 2005.

STEWART, J., TITTEL, E., CHAPPLE, M. **CISSP: Certified Information Systems Security Professional Study Guide.** 3rd ed. EUA: John Wiley and Sons, 2005. 759 p.

TANENBAUM, A. S. **Computer Networks.** 3rd ed. Upper Saddle River, NJ, USA: Prentice Hall, 1996**.**

TANENBAUM, A. S. **Redes de Computadores.** 4. ed. São Paulo: Elsevier, 2003. 945 p.

TIPTON, H. F., KRAUSE, M. **Information Security Management Handbook.** 4th ed. CRC Press, 2001. 626 p.

TIPTON, H. F., KRAUSE, M. **Information Security Management Handbook.** 6th ed. CRC Press, 2007.

WEBER, R. F. **Arquitetura de Computadores Pessoais.** Porto Alegre: Sagra Luzzato, 2000a.

WEBER, R. F. **Fundamentos de Arquiteturas de Computadores.** Porto Alegre: Sagra Luzzatto, 2000b.

WINDLEY, P. **Digital Identity.** USA: O'Reilly, 2005. 234 p.

YASCA. Yet Another Source Code Analyzer. Disponível: <http://www.yasca.org/>. Acesso em: 29 jul 2009.

APÊNDICE A
Material Didático sobre Desenvolvimento de Aplicações Seguras

A.1 Introdução

A Segurança da Informação, apesar do nome moderno, é uma preocupação muito antiga. Na Roma Antiga, o imperador Júlio César já se preocupava com o problema, enviando mensagens cifradas para os seus generais, a fim de preservar a confidencialidade de suas ordens. O código utilizado para criptografar as mensagens ficou conhecido como a Cifra de César e, atualmente, é reconhecido como um dos mais antigos algoritmos de criptografia de que se tem registro histórico (TANENBAUM, 1996).

Nas décadas de 40 a 70 do século XX, os computadores eram gigantes de grande porte, denominados *mainframes*, que ocupam salas inteiras (WEBER, 2000b). Esses computadores não eram conectados uns com os outros e trabalhavam de forma isolada. O único meio de acesso ao computador era, portanto, físico e, diga-se de passagem, altamente controlado e restrito. Somente técnicos e pessoas autorizadas tinham acesso ao computador. Devido ao alto preço de aquisição, custo de manutenção e complexidade de operação, apenas governos e grandes empresas possuíam computadores então. Mas mesmo nessa época pioneira, os computadores já faziam aquilo que é de interesse para a segurança da informação: automatizar processos. No contexto funcional e prático da Ciência da Computação, o que os computadores fazem é exatamente isso, ou seja, realizar de forma automática e mais rápida os mesmos processos que antes eram feitos de forma manual. Dessa forma, todos os problemas e cuidados inerentes aos processos e suas informações, passam para a esfera computacional.

Na década de 70, surgem os computadores pessoais (WEBER, 2000a). A redução do tamanho físico dos computadores foi possível graças ao invento do transistor, que substituiu a válvula dos primeiros computadores. Com o desenvolvimento dos circuitos integrados, que passaram a agregar milhares (atualmente milhões) de transistores em alguns centímetros quadrados de cerâmica e silício, a redução do tamanho e aumento do poder computacional deu um salto ainda maior. Com a redução de tamanho e de preço, os computadores popularizaram-se entre a empresas e, posteriormente, com a criação do computador pessoal, popularizaram-se também entre os cidadãos comuns. Agora, a preocupação com a segurança da informação não se restringe mais apenas aos governos e a grandes empresas, mas passa a fazer parte do cotidiano de empresas de todo porte, que automatizam seus negócios; e do cidadão comum, também, que passa digitalizar as

suas informações pessoais.

Ainda na década de 70, começam também as primeiras experiências com redes de computadores, ou seja, criam-se formas de conectar os computadores uns com os outros, de modo que eles possam se comunicar, trocando informações. Pode-se dizer que, tão importante quanto a revolução dos computadores, foi a revolução da redes de computadores, pois esta potencializou o emprego daquele (STALLINGS, 2000). Mas com o aumento das possibilidades, aumentou-se, também, os riscos e ameaças à segurança da informação. Assim, os problemas com a segurança da informação potencializam-se pois, agora, inúmeras pessoas passam a ter acesso ao computador através da rede.

Um dos centros de pesquisa pioneiros no desenvolvimento das redes de computadores pessoais foi o *Palo Alto Research Center* (PARC) da empresa Xerox. Esse centro de pesquisa possuía, já na década de 70, uma rede funcional de computadores pessoais comunicando-se entre si, trocando arquivos e compartilhando impressoras (CRINGLEY, 1997). A rede desenvolvida pela Xerox era tão sofistica a ponto de possuir um sistema de envio e recebimento de mensagens pessoais; somente após mais de duas décadas é que o resto do mundo veio a conhecer um sistema semelhante, atualmente conhecido como *e-mail*. Além disso, o Xerox PARC ainda desenvolveu o primeiro sistema operacional com interface gráfica (MORIMOTO, 2008), que viria a inspirar Steve Jobs e Steve Wozniack, da *Apple*, a desenvolver, para os computadores *Macintosh*, o *MacOs*; este, por sua vez, serviria de inspiração a Bill Gates, da *Microsoft*, para desenvolver o sistema operacional *Windows*, para os computadores IBM PC e compatíveis. O importante de toda essa história é que, nesse contexto acelerado de pesquisa e inovação, a preocupação com a segurança não era a maior das prioridades. De fato, muitos protocolos e sistemas foram desenvolvidos sem nenhuma preocupação com a segurança.

Na década de 80, a popularização dos computadores e de suas redes vai aumentando progressivamente. Nesse período, existem várias redes diferentes, mas que não estão conectadas umas a outras. É a era das redes locais ou LANs (*Local Area Network*), onde cada empresa tinha a sua rede, que ligava os seus computadores e servidores. Para as pessoas físicas, existiam as chamadas BBS (*Boletim Board System*), empresas que disponibilizavam uma rede privada para interligar diferentes usuários de suas casas ou escritórios.

Na década de 90, a popularização da informática explode com a Internet. A rede mundial de computadores interliga quase todas as redes que antes estavam isoladas umas das outras, agregando-as em uma grande rede global. Praticamente todas as empresas e negócios montam a sua página na Internet. Muitas empresas, inclusive, ganham mercado modernizando o seu negócio para atuar especificamente na rede mundial de computadores; enquanto diversas outras empresas surgem em

função da Internet. Mas, ao usar a *World Wide Web* (WWW) para conduzir os seus negócios, as empresas passam a depender dela também. Assim como as pessoas comuns que, cada vez mais, passam a depender da Internet para fazer aquilo que mais as caracteriza como seres humanos: comunicar-se umas com as outras.

Assim, com todo esse contexto em mente, constata-se que os computadores foram gradualmente automatizando os processos de negócios das empresas, tornando-se cada vez mais importantes para o funcionamento das corporações. Atualmente, os computadores são indispensáveis para as empresas, pois as mesmas simplesmente param caso os seus sistemas corporativos não funcionarem. Da mesma forma, para cada pessoa física, individualmente, o computador começou como uma curiosidade ou brinquedo sofisticado para, atualmente, ser indispensável para o trabalho, o estudo e a comunicação pessoal. E quanto maior a dependência do computador para as empresas e pessoas, maior o risco que ambas correm. De acordo com Sêmola (2003, p. 39), "os riscos são inerentes e proporcionais aos índices de dependência que a empresa tem da informação e da complexidade da estrutura que suporta os processo de automação, informatização e compartilhamento de informações". Portanto, uma falha de segurança em um sistema corporativo pode, potencialmente, prejudicar diretamente os negócios de uma empresa.

A.2 CIA + A³

Um dos conceitos mais bem difundidos em termos de boas práticas em segurança da informação é a dupla conhecida como CIA + A³ ou CIA AAA (leia-se "*CIA Triple-A*"). As siglas, em inglês, significam: *Confidentiality Integrity Availability, Authentication Authorization and Auditing*. Trata-se de um conjunto de conceitos importantíssimos de segurança da informação que, traduzidos para o português, significam: Confidencialidade Integridade Disponibilidade, Autenticação Autorização e Auditoria. Cada um desses conceitos será analisado detalhadamente a seguir.

A.2.1 CIA

Confidencialidade, Integridade e Disponibilidade (traduzido do inglês CIA - *Confidentiality Integrity Availability*) são os elementos fundamentais para a segurança da informação. Todos esses elementos possuem significado e implicações próprias e, por isso, serão estudados em detalhes a

seguir.

A.2.1.1 *Confidentiality*

Confidencialidade é a capacidade de proteger a informação de tal forma que ela possa ser acessada e compreendida apenas pela a pessoa ou entidade a qual se destina. Uma das técnicas mais utilizadas para a obtenção da confidencialidade é o uso da criptografia (SCHNEIER, 1996). Um algoritmo criptográfico embaralha a informação de tal forma que ela torna-se ilegível. Esse processo, obviamente, é reversível mediante a apresentação de uma chave. No caso do algoritmo criptográfico trabalhar com uma única chave, ele é chamado de algoritmo simétrico. Por outro lado, se o algoritmo realizar a sua computação com duas chaves distintas, o algoritmo é chamado de assimétrico. Uma análise detalhada dos algoritmos de criptografia é bastante extensa e merece uma dedicação específica para que possa ser dada a devida atenção que o assunto merece pela sua importância dentro da área de Segurança da Informação.

Existem outras técnicas, além do uso de criptografia, de obter-se confidencialidade. A mais simples de todas é simplesmente omitir ou ocultar a informação sigilosa, exibindo somente parte da informação como um todo; adicionalmente, deve-se tomar o cuidado para que a informação parcial seja exibida apenas quando extremamente necessário. Por exemplo, ao ocorrer um problema de pagamento com uma compra efetuada pela Internet ou pelo telefone, com o uso de cartão de crédito, o sistema corporativo que lida com esse problema deve apresentar o seguinte comportamento: exibir, nas informações do cliente às quais o atendente tem acesso, somente os últimos quatro dígitos do número do cartão de crédito do cliente e não o número inteiro. Dessa forma evita-se: que um atendente mal-intencionado faça uso incorreto do número do cartão; que outro funcionário ou pessoa que esteja passando pela estação de trabalho do atendente em particular veja o número inteiro do cartão de crédito na tela; e, por fim, evita-se que o número de cartão de um cliente seja acidentalmente revelado a um cliente diferente, que erroneamente tenha sido apresentado como o proprietário do cartão.

Salienta-se, ainda com base no exemplo do parágrafo anterior, a importância do fator humano na equação de segurança da informação. Não basta apenas que o sistema corporativo em si seja seguro e livre de falhas; é necessário que o projeto e funcionamento do sistema leve em consideração a ação dos usuários que interagem com o mesmo.

Uma outra maneira de fornecer confidencialidade para informações sensível é protegendo o acesso ao meio no qual a informação se encontra. Por exemplo, se um banco de dados possui todos os mecanismos de autenticação e autorização de acesso em perfeito funcionamento, obtém-se, dessa

forma, a confidencialidade dos dados, mesmo que as informações em si sejam armazenadas em claro (isto é, de forma legível; sem criptografia) dentro do branco de dados. Obviamente, esse procedimento não é recomendado para informações sensíveis como números de cartão de crédito. No caso de dados com tal grau de sensibilidade, é altamente recomendável que seja utilizada a criptografia além do uso do controle de acesso ao meio (SCHNEIER, 2000); garante-se, assim, a confidencialidade com duas camadas de proteção.

Da mesma forma que para ser armazenada em um banco de dados, a informação pode ser protegida com o controle de acesso ao meio, o mesmo também é válido para a sua transmissão em um meio de rede de comunicação. E, assim como ocorre no exemplo de armazenamento em banco de dados, recomenda-se que a transmissão de informações altamente sensíveis deve ter uma camada adicional de criptografia aplicada, além do uso do canal de comunicações seguro.

A.2.1.2 *Integrity*

A integridade é a propriedade de averiguar se um determinado conjunto de informações foi alterado ou não (PRADHAN, 1996). Por exemplo, garantir a integridade de um arquivo de texto no sistema de arquivos de um computador significa ter a capacidade de determinar, com certeza, se o arquivo foi alterado ou não. Em um sistema corporativo, a integridade reflete-se em garantir que nenhuma informação do sistema, seja ele em parte ou como um todo, foi alterada; caso ocorra alguma alteração, o sistema deve ser capaz de detectar a alteração automaticamente.

Salienta-se que a alteração das informações pode ser tanto acidental como intencional. Uma alteração acidental de dados caracteriza-se, por exemplo, quando o meio em que essa informação é armazenado sofre alguma falha, como um arquivo corrompido no disco rígido devido a falhas físicas ou magnéticas do disco; neste mesmo exemplo, a falha pode ocorrer, ainda, devido a um *bug* no sistema de arquivos do SO da máquina em o aplicativo está sendo executado, resultando na corrupção do arquivo que estava sendo gravado. Outro exemplo, também bastante comum, é o caso de transmissão de dados via rede; como trata-se de um meio muito sensível a alterações do ambiente, a ocorrência de erros na transmissão é freqüente e devem ser tratados. Enfim, verifica-se, com esses poucos exemplos, que são muitas as formas que a integridade das informações pode ser comprometida de forma acidental.

Adicionalmente, a integridade pode ser comprometida de forma intencional, isto é, alguém deliberadamente alterou os dados para algum propósito; seja ele tirar vantagem pessoal, sabotagem ou como tentativa de prejudicar outrem. Justamente para evitar esses casos é que a garantia de

integridade de informações é ainda mais importante, uma vez que as implicações dessas alterações nos dados são muito mais severas.

Existem diversas técnicas para garantir a integridade de dados. A tecnologia mais recente a ser empregada é com o uso de assinaturas digitais. Essa técnica em particular é bastante complexa e será tratada em seção específica do presente trabalho. Por hora, basta ressaltar que uma assinatura digital é capaz de detectar se ocorreu alguma alteração na informação que engloba de maneira bastante segura e garantida.

A.2.1.3 *Availability*

Disponibilidade significa ter a informação disponível quando ela for requisitada. Para tanto, é necessário ter diversos mecanismos de proteção em funcionamento em torno do sistema corporativo.

A.2.2 AAA

Autenticação, Autorização e Auditoria são os três pilares remanescentes que formam a base dos principais conceitos de segurança da informação. Cada um deles será explicado a seguir, inclusive com exemplos de sua utilização.

A.2.2.1 Autenticação

Autenticação é a capacidade de identificar quem é o usuário, ou seja, averiguar se trata-se do usuário A ou B. Esse processo de identificação pode ser realizado de diversas formas. De um modo geral, pode-se analisar as seguintes propriedades de um usuário para realizar a sua autenticação: o que o usuário **sabe**, o que ele **tem** e o que ele **é**. Ao analisar-se exemplos de métodos de autenticação, verifica-se que são essencialmente essas propriedades do usuário que estão sendo verificadas. Assim, pode-se averiguar que, por exemplo, com o emprego de usuário e senha, está-se analisando o que o usuário sabe; já com o uso de um cartão magnético, verifica-se o que o usuário tem; com a análise da impressão digital ou da retina ocular, a autenticação certifica o que o usuário é, ou seja, verifica alguma de suas propriedades fisiológicas. A seguir, será analisada cada uma

dessas três propriedades e seus respectivos exemplos em detalhes, verificando as vantagens e desvantagens de cada um desses métodos de autenticação.

A primeira e mais comum forma de autenticação é através do uso de um nome de usuário e senha, ou seja, o *login* no sistema é feito por meio da verificação de algo que o usuário sabe. Esse método é o mais fácil, rápido e econômico de ser implementado, pois pode ser realizado inteiramente por software, não necessitando de qualquer tipo de hardware adicional além do computador em si. A desvantagem do método de usuário e senha é que esta última pode ser compartilhada entre os diversos usuários; a divulgação ou empréstimo da senha não constitui uma boa prática de segurança da informação, uma vez que um usuário estaria assumindo a identidade de outro ou, pior ainda, uma pessoa que nem é usuária autorizada do sistema pode ter acesso com o conhecimento do *login* e senha de um usuário autêntico.

Outra forma de realizar a autenticação de usuários é verificar o que ele tem. Exemplos de implementação desse método são o uso de cartões magnéticos ou crachás de funcionário com *chip*; ambos itens podem ser passados facilmente de uma pessoa para outra. Assim, da mesma forma que na análise do que o usuário sabe, o método de autenticação através do que o usuário possui também apresenta a desvantagem que uma pessoa poder emprestar o item que ela tem para outra.

Finalmente, pode-se realizar a autenticação verificando o que o usuário é. Exemplos desse método são a análise de impressão digital ou da retina. Na impressão digital verifica-se as rugosidades da pele de algum dedo ou da mão inteira. Já na análise da retina, são identificados e mapeados os vasos sangüíneos presentes no fundo do olho. Todo ser humano possui impressões digitais diferentes uns dos outros. Esse fenômeno também ocorre com os vasos sangüíneos da retina ocular, isto é, duas pessoas distintas apresentam diferenças nas suas retinas. Dessa forma, é possível autenticar usuários através da conferência desses mapeamentos, verificando se as suas características fisiológicas conferem com as constantes no banco de dados do sistema.

Esse método de autenticação, no entanto, apresenta a desvantagem de necessitar de hardware especial para ser implementado. São necessários leitores de impressão digital ou de retina ocular em todos os pontos em que se desejar implantar o acesso autenticado. A grande vantagem desse método é que o usuário não consegue emprestar a sua impressão digital ou retina para outro; obviamente, todo sistema ou hardware é suscetível a falhas e pode ser burlado, mas é muito mais difícil forjar uma impressão digital ou uma imagem de retina ocular do que simplesmente revelar uma senha ou emprestar um cartão de acesso, como nos métodos analisados anteriormente.

Outro conceito freqüentemente associado à autenticação é o de não-repúdio. Esse conceito nada mais é do que garantir que uma ação possa ser inequivocamente associada a um usuário. Em outras palavras, um usuário não pode negar que tomou uma determinada ação. Por exemplo, ao

fazer um acesso autenticado através de senha, cartão ou impressão digital, o usuário não tem como repudiar que abriu determinada porta ou fez login no sistema, pois somente ele conhece a sua senha, possui o seu cartão ou tem a digital necessária. Da mesma forma, o conceito de não-repúdio também está relacionado à assinatura digital; nesse caso, quando um usuário envia uma mensagem assinada digitalmente, o mesmo não pode negar que enviou a mensagem, pois somente ele possui aquela assinatura.

A.2.2.2 Autorização

Uma vez autenticado o usuário, isto é, estabelecido que o usuário é realmente quem ele alega ser, o passo seguinte é determinar o que ele pode fazer. Autorização é, portanto, uma lista de ações ou comandos que o usuário pode executar no sistema. Por exemplo, a maioria dos sistemas operacionais divide os seus usuários em, no mínimo, dois grupos: um grupo de administradores e outro de usuários comuns. O primeiro é mais restrito e os seus usuários podem realizar mais ações, como gerenciar o sistema, criar novas contas, instalar novos programas, entre outras tarefas; já o segundo grupo, que constitui a grande maioria dos usuários no exemplo de sistema operacional, possui acesso mais limitado, podendo apenas executar as tarefas mais comuns. Com esse exemplo, ilustra-se a utilidade do conceito de autorização: segregar os usuários do sistema conforme a sua função.

Da mesma forma que no exemplo dos sistemas operacionais, as aplicações, de um modo geral, também precisam separar os seus usuários conforme as suas respectivas funções dentro do sistema. Assim, os sistemas corporativos também possuem grupos de usuários administradores do aplicativo e os demais grupos, conforme as suas funções corporativas. Essas funções específicas também são chamadas de políticas do sistema. O processo que determina quem pode fazer o que é a autorização. Assim, o controle de autorização de um sistema corporativo de autorizar ou rejeitar um comando conforme as políticas do sistema.

Sistemas corporativos bem implementados e flexíveis permitem configurar as políticas de autorização do sistema em tempo real, ou seja, durante o uso do sistema em execução. Mas também existem sistemas em que as políticas são pré-configuradas e não podem ser modificadas. Tal solução não constitui uma boa prática de segurança da informação, uma vez que, detectada uma falha de segurança do sistema em função de uma política mal elaborada, a mesma não terá como ser alterado por meio de configuração; será necessário re-programar o sistema o que, por sua vez, decorrerá em custos adicionais com programação, teste e instalação, além do fato de a falha de

segurança permanecer aberta até que o sistema seja corrigido.

A.2.2.3 Auditoria

O último conceito da tríade AAA é o de *Auditing* ou, traduzindo para o português, teria-se "ato de fazer auditoria" ou, simplesmente, Auditoria. Este terceiro conceito do AAA também é chamado por alguns autores de *Accounting* ou Rastreabilidade, em português. Conforme o nome do termo traduzido sugere, esse conceito traduz-se na capacidade do sistema corporativo rastrear as ações dos usuários, o consumo de recursos, e as ações de gerenciamento do sistema. Tal rastreamento pode ser implementado em arquivos de log (registro) ou em banco de dados. São essas informações que permitem a realização de auditorias sobre o sistema.

A diferença na nomenclatura, geralmente, é devida ao contexto em que o conceito é aplicado. No contexto empresarial de um modo geral, o termo *accounting* é o mais empregado, pois traduz a idéia de cobrança; já no contexto de segurança da informação, o termo *auditing* parece mais apropriado, pois associa-se bem à segurança.

O uso de arquivos de *log* é mais simples e rápido de implementar. Na maioria das vezes, os arquivos de *log* não passam de arquivos texto ao qual são acrescentadas linhas com informação das ações realizadas pelos usuários. A desvantagem dessa solução é que, conforme o arquivo de *log* cresce em tamanho, o acesso a suas informações torna-se mais lenta e insegura, pois arquivos texto não possuem nenhuma proteção contra corrupção.

A outra opção de implementação citada é a rastreabilidade através de banco de dados. Essa solução é mais custosa de ser implementada em termos de recursos e tempo, pois é mais complexa e demando todo o suporte em hardware e software de um banco de dados. A vantagem é que um banco de dados é muito mais robusto que um simples arquivo texto em termos de capacidade de armazenamento e proteção contra corrupção de dados. Adicionalmente, o banco de dados possui a vantagem de ter o acesso controlado pelo SGBD (Sistema Gerenciador de Banco de Dados), que possui seus métodos próprios de autenticação, autorização e rastreabilidade; ou seja, mais uma camada de segurança para reforçar o sistema corporativo como um todo.

Adicionalmente, uma característica desejável ao rastreamento é que ele seja feito em tempo real, ou seja, que as informações de rastreamento sejam armazenadas à medida que as ações forem executadas. Da mesma forma, o acesso a essas informações também deve ser disponibilizado em tempo real, isto é, não deve ser necessário aguardar um fechamento ou *commit* do sistema para se ter acesso aos *logs*. Essa característica é particularmente interessante em sistemas corporativos que

realizarão alguma forma de cobrança dos recursos consumidos por seus usuários.

As informações a serem armazenadas em um *log* são: a identidade do usuário, o comando executado pelo mesmo, a hora e data em que a ação foi iniciada e, conforme for o caso, quando a execução do comando terminou. Essas informações são de vital importância no caso da ocorrência de uma falha na segurança do sistema. É com base nas informações contidas nos arquivos de *log* que será feita a investigação, ou auditoria, sobre o ataque. O registro do sistema permite rastrear as comandos que causaram a falha de segurança, rastrear as ações do invasor e determinar, assim, como corrigir o problema para que a falha não se repita.

APÊNDICE B

Questionário de Avaliação de Conhecimentos em Segurança da Informação

1. A Segurança da Informação nos sistemas corporativos do Exército Brasileiro é responsabilidade exclusiva dos programadores de *software*.

a. Certo

b. Errado

2. Existem seis pilares de segurança da informação que são abreviados como CIA + A³. As siglas iniciais significam Confidencialidade, Integridade e Disponibilidade (*Availability*). O que significam as três siglas restantes?

a. Autenticação, Autorização e Acessibilidade

b. Autenticação, Autorização e Auditoria

c. Autenticação, Acessibilidade e Auditoria

d. Autorização, Acessibilidade e Arquivamento

3. Qual item a seguir não faz parte da classificação segundo o grau de sigilo do Governo Federal?

a. Ultra-secreto

b. Secreto

c. Restrito

d. Reservado

4. A criptografia cobre todos os propósitos a seguir, exceto:

a. Previne a recepção não autorizada dos dados (Confidencialidade)

b. Garante que a informação não foi alterada durante o trânsito (Integridade)

c. Assegura que a mensagem foi escrita pelo remetente (Autenticação)

d. Garante que os dados estão disponíveis sempre que necessário (Disponibilidade)

5. Qual área da Segurança da Informação preocupa-se com a evidência do histórico ou rastro de um acesso, seja ele bem-sucedido ou não?

a. Autorização

b. Auditoria

c. Autenticação

d. Disponibilidade (*Availability*)

6. Como é chamado o ataque a um sítio *web*, composto por uma base de dados, no qual o atacante executa comandos não autorizados tirando proveito de código inseguro do sistema conectado à Internet, esquivando-se do *firewall*?

a. Buffer Overflow

b. Cross-site Scripting (XSS)

c. Denial of Service (DoS)

d. SQL Injection

7. A revisão do código-fonte não é um passo obrigatório do ciclo de vida de desenvolvimento de software, pois a sua necessidade irá depender dos dados que a aplicação for processar, armazenar e transmitir.

a. Certo

b. Errado

c. Depende

8. Qual a afirmação correta sobre a diferença entre funções *hashing* e criptográficas?

a. Não é possível recuperar os dados originais de uma função *hash*

b. Toda função criptográfica é sempre mais rápida do que uma função *hash*

c. A criptografia é resistente a ataques de força bruta

d. *Hashing*, ao contrário da criptografia, possibilita a obtenção dos dados originais de volta.

Gabarito: 1.b, 2.b, 3.c, 4.d, 5.b, 6.d, 7.b, 8.a

APÊNDICE C
Certificações

C CERTIFICAÇÕES

Atualmente, existem diversas certificações de segurança para o profissional da área de Tecnologia da Informação, seja ele um desenvolvedor de *software* ou um consultor de segurança. Com o objetivo de estimular o leitor deste texto a estudar e qualificar-se, este capítulo descreve a mais renomada dessas certificações, a *Certified Information Systems Security Professional* (CISSP). Nas seções a seguir, é dada uma visão geral da referida certificação; também são fornecidos detalhes dos processos de exame e recomendação para a obtenção da aprovação. Adicionalmente, este capítulo em particular facilita o estudo inicial do profissional que não possui proficiência na língua inglesa, uma vez que o sítio da certificação é disponibilizado apenas em inglês.

No texto a seguir, a primeira seção descreve brevemente a organização ISC². Em seguida, é abordada a certificação CISSP propriamente dita. Nessa seção, é descrito o processo do exame de qualificação, o a certificação, o processo de recomendação, as características das possíveis auditorias e, por fim, algumas palavras sobre a manutenção da certificação.

C.1 ISC²

A *International Information Systems Security Certification Consortium*, também conhecida pela sigla ISC², é um consórcio sem fins lucrativos. Na realidade, trata-se de um consórcio de profissionais da área de segurança da informação que, em sua maioria, trabalham como consultores de segurança de empresas e órgãos governamentais. Mas também compõe esse consórcio, desenvolvedores de *software* e outros profissionais de sub-áreas afins de TI. Maiores informações sobre a ISC2 podem ser obtidas no site da organização em www.isc2.org.

C.2 CISSP

Uma das certificações mais bem conceituadas internacionalmente para o profissional de Segurança da Informação é a CISSP (HARRIS, 2005); sigla em inglês de *Certified Information*

Systems Security Professional que, traduzido para o português, significa Profissional Certificado em Sistemas de Segurança da Informação. Trata-se de uma certificação concedida somente aos mais bem qualificados profissionais do ramo. Ao contrário de outras certificações de TI, nas quais somente a realização de uma prova é necessária para a obtenção do certificado, na CISSP é necessário ter cinco anos de experiência profissional comprovada na área de segurança da informação, em dois ou mais dos seguintes domínios:

- Controle de Acesso;
- Segurança de Aplicação;
- Continuidade de Negócio e Planejamento de Recuperação de Desastre;
- Criptografia;
- Segurança da Informação e Gerenciamento de Risco;
- Legal, Regulamentos, Conformidade (*Compliance*) e Investigações;
- Segurança de Operações
- Segurança Física (de Ambiente);
- Segurança na Arquitetura e Design;
- Segurança de Redes e Telecomunicações.

A obtenção de tal certificação efetivamente comprova a experiência e capacitação do profissional em segurança da informação. Mesmo antes da obtenção da certificação propriamente dita, o estudo, preparo e acompanhamento para a obtenção da certificação já aumenta significativamente o preparo do profissional e a qualidade do seu trabalho. Por isso, será indicado a seguir, os passos necessários para a obtenção da certificação CISSP.

É necessário completar com êxito quatro processos para que o candidato torne-se um profissional certificado com a CISSP:

- Exame;
- Certificação;
- Recomendação;
- Auditoria.

C.2.1 Exame

Para sequer poder realizar a prova de examinação da CISSP, o candidato deve comprovar previamente a sua experiência de, no mínimo, cinco anos na área de segurança da informação, conforme os domínios listados anteriormente. Alternativamente, caso o candidato possua curso superior na área de Ciência da Computação, basta comprovar quatro anos de experiência profissional, nos mesmos moldes explicados previamente.

Adicionalmente, também é necessário atestar pela veracidade das informações prestadas, legalmente comprometendo-se com o código de ética da ISC². Finalmente, é necessário responder perguntas sobre histórico criminal e antecedentes relacionados.

C.2.2 Certificação

Para receber o seu certificado, o candidato deve ser aprovado na prova de exame CISSP; submeter um formulário de endosso; e, caso seja amostrado para uma auditoria, deverá ser aprovado na comprovação de sua experiência profissional.

C.2.3 Recomendação

Esta é a peculiaridade mais interessante e importante da certificação CISSP. Uma vez aprovado na prova de exame, é necessário que a inscrição do candidato seja recomendada por um profissional já certificado pela a CISSP. Esta é uma etapa indispensável para que o candidato possa ser agraciado com a certificação. O profissional que faz a recomendação atesta a veracidade da experiência alegada pelo candidato; e, adicionalmente, também atesta que o candidato tem boa reputação no meio profissional de segurança da informação.

Salienta-se que este é um dos principais diferenciais da certificação CISSP, pois quem faz a recomendação, indica apenas profissionais que conhece. Assim, para preservar a boa reputação e qualidade da certificação, apenas bons profissionais são recomendados. Dessa forma, ao contrário de outras certificações da indústria de Tecnologia da Informação, não é qualquer um que pode ser candidato a receber a certificação; ou seja, os próprios profissionais já certificados fazem um controle de qualidade da certificação.

C.2.4 Auditoria

Antes da obtenção da certificação, alguns candidatos aprovados serão selecionados randomicamente para sofrer uma auditoria.

C.2.5 Manutenção da Certificação

Esta é mais uma peculiaridade importantíssima da certificação CISSP. Para que o profissional certificado com a CISSP mantenha-se digno do título, é necessário, a cada três anos, obter uma recertificação. Afinal, a comprovação de que o profissional certificado mantém o seu nível de qualidade é tão importante quanto selecionar e examinar apenas bons candidatos para a concessão do certificado.

Os requerimentos para manter-se as credenciais em um bom patamar são continuamente atualizados. Mas, de uma modo geral, a recertificação é obtida através da atualização profissional do agraciado com cursos que gerem créditos educacionais reconhecidos pela ISC². A cada ano do ciclo de três anos da recertificação é necessária a obtenção de um mínimo de créditos educacionais e, ao final do ciclo, um total ainda maior de créditos é exigido. Em outras palavras, não basta fazer o mínimo, é necessário atualizar-se continuamente para manter a certificação CISSP.

Finalmente, apenas a título de informação, é necessário pagar uma taxa anual em dólares à *International Information Systems Security Certification Consortium*.

APÊNDICE D

Cronograma de Atividades

MÊS/	DATA	TRABALHO DE CONCLUSÃO DE CURSO (30 Mar/14 Ago)	
Abril	24 (SI 7)	Linha de acompanhamento 1 e entrega do primeiro relatório de acompanhamento à SCD	
Maio	SI 8	Pesquisa bibliográfica e fundamentação teórica	
	SI 9		
	SI 10		
	SI 11		
Junho	SI 12		
	SI 13	Análise inicial do sistema do estudo de caso	
	SI 14		
	19 (SI 15)	Linha de acompanhamento 2 e entrega do segundo relatório de acompanhamento à SCD	
	SI 16	Elaboração dos procedimentos de Segurança da Informação	
Julho	SI 17		
	SI 18	Elaboração da validação das propostas	
	SI 19		
	SI 20	Análise detalhada da validação	
	SI 21	Revisão final do texto	
Agosto	3 (SI 22)	Linha de acompanhamento 3 e entrega do terceiro relatório de acompanhamento à SCD	
	14 (SI 23)	140900Ago09	Aluno entrega TCC ao orientador.
		141000Ago09	Orientador entrega TCC à SCD.
	17 a 21 (SI 24)	17 (SI 24)	SCD entrega TCC à CATC
	SI 25		
Setembro	4 (SI 26)	CATC entrega ficha de avaliação final do TCC à SCD	
	11 (SI 27)	9 (SI 27)	SCD entrega TCC insuficientes aos autores para que sejam refeitos.
	SI 28		
	25 (SI 29)	Alunos entregam TCC revisados ao orientador.	
Outubro	SI 30		
	5 a 9 (SI 31)	7 (SI 31)	CATC entrega notas finais dos TCC revisados à SCD.
		9 (SI 31)	SCD entrega parecer final dos TCC á STE.
	SI 32		
	SI 33		
	30 (SI 34)	Alunos entregam a versão encadernada em capa dura e a mídia à SCD	