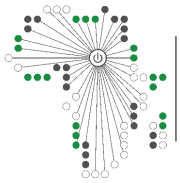

Universidade Virtual Africana

INFORMÁTICA APLICADA: CSI 4304

SEGURANÇA INFORMÁTICA AVANÇADA

Valdinacio Paulo

Prefácio

A Universidade Virtual Africana (AVU) orgulha-se de participar do aumento do acesso à educação nos países africanos através da produção de materiais de aprendizagem de qualidade. Também estamos orgulhosos de contribuir com o conhecimento global, pois nossos Recursos Educacionais Abertos são acessados principalmente de fora do continente africano.

Este módulo foi desenvolvido como parte de um diploma e programa de graduação em Ciências da Computação Aplicada, em colaboração com 18 instituições parceiras africanas de 16 países. Um total de 156 módulos foram desenvolvidos ou traduzidos para garantir disponibilidade em inglês, francês e português. Esses módulos também foram disponibilizados como recursos de educação aberta (OER) em oer.avu.org.

Em nome da Universidade Virtual Africana e nosso patrono, nossas instituições parceiras, o Banco Africano de Desenvolvimento, convido você a usar este módulo em sua instituição, para sua própria educação, compartilhá-lo o mais amplamente possível e participar ativamente da AVU Comunidades de prática de seu interesse. Estamos empenhados em estar na linha de frente do desenvolvimento e compartilhamento de recursos educacionais abertos.

A Universidade Virtual Africana (UVA) é uma Organização Pan-Africana Intergovernamental criada por carta com o mandato de aumentar significativamente o acesso a educação e treinamento superior de qualidade através do uso inovador de tecnologias de comunicação de informação. Uma Carta, que estabelece a UVA como Organização Intergovernamental, foi assinada até agora por dezenove (19) Governos Africanos - Quênia, Senegal, Mauritânia, Mali, Costa do Marfim, Tanzânia, Moçambique, República Democrática do Congo, Benin, Gana, República da Guiné, Burkina Faso, Níger, Sudão do Sul, Sudão, Gâmbia, Guiné-Bissau, Etiópia e Cabo Verde.

As seguintes instituições participaram do Programa de Informática Aplicada: (1) Université d'Abomey Calavi em Benin; (2) Université de Ougagadougou em Burkina Faso; (3) Université Lumière de Bujumbura no Burundi; (4) Universidade de Douala nos Camarões; (5) Universidade de Nouakchott na Mauritânia; (6) Université Gaston Berger no Senegal; (7) Universidade das Ciências, Técnicas e Tecnologias de Bamako no Mali (8) Instituto de Administração e Administração Pública do Gana; (9) Universidade de Ciência e Tecnologia Kwame Nkrumah em Gana; (10) Universidade Kenyatta no Quênia; (11) Universidade Egerton no Quênia; (12) Universidade de Addis Abeba na Etiópia (13) Universidade do Ruanda; (14) Universidade de Dar es Salaam na Tanzânia; (15) Universite Abdou Moumouni de Niamey no Níger; (16) Université Cheikh Anta Diop no Senegal; (17) Universidade Pedagógica em Moçambique; E (18) A Universidade da Gâmbia na Gâmbia.

Bakary Diallo

O Reitor

Universidade Virtual Africana

Créditos de Produção

Autor

Valdinacio Paulo

Par revisor(a)

Ambrosio Vumo

UVA - Coordenação Académica

Dr. Marilena Cabral

Coordenador Geral Programa de Informática Aplicada

Prof Tim Mwololo Waema

Coordenador do módulo

Robert Oboko

Designers Instrucionais

Elizabeth Mbasu

Benta Ochola

Diana Tuel

Equipa Multimédia

Sidney McGregor

Barry Savala

Edwin Kiprono

Kelvin Muriithi

Victor Oluoch Otieno

Michal Abigael Koyier

Mercy Tabi Ojwang

Josiah Mutsogu

Kefa Murimi

Gerisson Mulongo

Direitos de Autor

Apoiado por

Projeto Multinacional II da UVA financiado pelo Banco Africano de Desenvolvimento.

Índice

Descrição Geral do Curso

Bem-vindo(a) módulo de Segurança Informática Avançada (Criptografia e Segurança de Redes)

Bem-vindo ao Módulo de Segurança Informática Avançado. Este módulo fornece um estudo de alto nível sobre questões de segurança de computadores em redes de computadores e métodos avançados de criptografia de dados. Ele se concentra em aspectos avançados de segurança do computador, tais como: Criptografia, práticas de segurança, a segurança do sistema, a segurança para autenticação na web e técnicas de gerenciamento de senhas. Finalizando este módulo, você deverá ser capazes de criar arquiteturas de rede seguras adaptadas ao nível do investimento e de segurança exigidas. Assumir a responsabilidade pela instalação, configuração e manutenção de segurança de rede.

O módulo pretende dar aptidões de gestão de infra-estruturas informáticas, onde o papel da segurança informática é crítica para garantir a integridade dos dados e normal operacionalidade dos vários sistemas: redes informáticas, servidores e computadores pessoais da organização.

Hoje, notamos que a informação é considerada a chave dos negócios de uma organização/empresa, devido à sua utilidade e importância, entretanto, a problemática da Segurança da Informação da empresa é uma acção prioritária para os gestores, pois reconhecem o valor que ela têm e por esta razão as organizações devem certificar-se de que a gerem de forma eficaz. Por esta razão, o estudo deste módulo é importante porque você aprenderá os métodos e ferramentas em segurança de computadores para puder assegurar a confidencialidade da informação nas organizações e eles também aprender a proteger suas próprias informações e sistemas em ambiente de rede.

Pré-requisitos

- Introdução à Segurança Informática;
- Comunicação de Informação e Redes de Computadores;

Materiais

Os materiais necessários para completar este curso incluem:

- Servidor ou Computador pessoal com acesso;
- Telefones Inteligentes (Smart Phones);
- Acesso a Internet;
- Ferrametas de Software
- Vídeos On-line do Youtube;
- Infraestrutura de rede;

- Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", Fourth Edition, Prentice Hall PTR, 2006.
- Malik, S., "Network Security Principles and Practices". Cisco Press. 2002.
- Mark Rhodes-Ousley, et al. "Network Security: The Complete Reference," 2003.
- Kaufman, C., et al., "Network Security: Private Communication in a Public World". 2ed., Prentice Hall, 2002.
- Gert DeLaet, Gert Schauwers, "Network Security Fundamentals", Cisco Press Fundamentals Series, 2004.
- Oliveira, Victor. Segurança da Informação – Técnicas e Soluções, 1ed, Lisboa, 2001.

Objetivos do Curso

Após concluir este curso, o(a) aluno(a) deve ser capaz de:

- Identificar e discutir os conceitos de segurança da informação e as principais arquiteturas utilizadas para proteger redes e serviços;
- Aplicar os princípios e as funcionalidades de técnicas de criptografia, autenticação e gerenciamento de controle de acesso;
- Criar arquiteturas de rede seguras adaptadas ao nível do investimento e de segurança exigidas;
- Projectar e desenvolver sistemas de autenticação e de segurança;
- Conceber e desenvolver algoritmos de criptografia e des-criptografia para sistemas de segurança;
- Adotar éticas, profissionalismo e responsabilidades legais de engenheiros de segurança de rede;
- Estudar o impacto social da segurança de rede no dia-a-dia, por exemplo, em transações on-line, e-commerce e-gestão, etc..
- Identificar as principais formas de ameaças e de que maneira são feitos os ataques típicos;
- Analisar as vulnerabilidades dos sistemas em rede;
- Planear uma estratégia de segurança para uma rede de computadores.

Unidades

Unidade 0: Diagnóstico

O propósito desta unidade é verificar a compreensão dos conhecimentos que possui relacionados com Segurança de Computadores, os principais objectivos de segurança de computador, desafios de segurança do computador e o modelos de segurança de computador que podem ser adoptados pelas organizações. Conceitos abordados no Módulo anterior, Introdução à Segurança Informática.

Unidade 1: Conceitos gerais de segurança de computador

Nesta unidade você ira aprender os conceitos gerais sobre segurança informática. Definiremos o conceito de segurança informática, os principais objetivos que levam o estudo da segurança. Mais a diante abordaremos as causas do estudo da segurança e aspectos a ter em conta para implementação da segurança informática em rede de computador.

Unidade 2: Algoritmos de Criptografia

Nesta unidade iremos abordar as técnicas de segurança existentes. Falaremos do conceito Função Hashing que é muito envolvidos quando se fala de criptografia, este método de criptografia mais usado em assinaturas digitais. Abordaremos também métodos de autenticação de mensagens dos algoritmos de criptografia.

Unidade 3: Segurança de rede e ferramentas de segurança

Nesta unidade iremos abordar o conceito de segurança em redes de computadores. Veremos também que segurança de rede começa com a existência de politica de segurança da organização, desta politica deve ser definida pelos superiores da organização em coordenação com equipe técnica. Abordaremos os protocolos de segurança da informação na rede de computares.

Unidade 4: Segurança na Web

É nesta unidade, onde abordaremos os serviços e as principais formas ameaças da Web e os mecanismos de prevenção de estas ameaças. Iremos abordar o Protocolo SSL e TLS, que oferecem uma camada de segurança para duas aplicações comunicantes (cliente e servidor). Na final, abordaremos o conceito Virtual Private Network (VPN), no qual discutiremos a segurança em uma rede VPN, o seu mecanismo de funcionamentos por Tunelamentos, onde abordamos as principais ferramentas de segurança nas VPN's, como a Criptografia, Certificados digitais, RADIUS e o protocolo IPSec.

Avaliação

Em cada unidade encontram-se incluídos instrumentos de avaliação formativa a fim de verificar o progresso do(a)s aluno(a)s.

No final de cada módulo são apresentados instrumentos de avaliação sumativa, tais como testes e trabalhos finais, que compreendem os conhecimentos e as competências estudadas no módulo.

A implementação dos instrumentos de avaliação sumativa fica ao critério da instituição que oferece o curso. A estratégia de avaliação sugerida é a seguinte:

1	Avaliação final da Unidade 1	10%
2	Avaliação final da Unidade 2	10%
3	Avaliação final da Unidade 2	10%
4	Avaliação final da Unidade 4	10%
5	Teste final do Módulo	25%
6	Laboratório	35%

Leituras e outros Recursos

As leituras e outros recursos deste curso são:

Unidade 0

Leituras e outros recursos obrigatórios:

- Oliveira, Victor. Segurança da Informação – Técnicas e Soluções, 1ed, Lisboa, 2001.
- Kaufman, C., et al., "Network Security: Private Communication in a Public World". 2ed., Prentice Hall, 2002.
- Malik, S., "Network Security Principles and Practices". Cisco Press. 2002.
- Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", Fourth Edition, Prentice Hall PTR, 2006.

Unidade 1

- WADLOW, Thomas. Segurança de Redes. Editora Campus. Rio de Janeiro, 2000.
- REZENDE, Denis Alcides e ABREU, Aline França. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. Editora Atlas. São Paulo, 2000.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Axcel Books. Rio de Janeiro, 2000.
- KRAUSE, Micki e TIPTON, Harold F. Handbook of Information Security Management. Auerbach Publications, 1999.
- Information Systems Management Issues for the 1990s, Fred Niederman, James C. Brancheau and James C. Wetherbe, MIS Quarterly, Vol. 15, No. 4 (Dec., 1991), pp. 475-500

Unidade 2

- GARFINKEL, Simson. PGP: Pretty Good Privacy. O'Reilly & Associates. 1995.
- KHANNA, Raman. Distributed Computing Implementation and Management Strategies. Prentice Hall, 1993.
- Gradient Technologies White Paper – Encryption Security in the Enterprise. URL:
- White paper on the impact of the Public Key technology and Digital Signatures on CAD. URL: .

Unidade 3

- SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. Redes de computadores das LANs, MANs e WANs às Redes ATM. 2.ed. Rio de Janeiro:, 2015.
- KUROSE, James; ROSS, Keith. Rede de computadores e a internet: Umaabordagem top-down. 3.ed. São Paulo: Pearson Addison Wesley, 2006.
- McCumber, John. Assessing and Managing Security Risk in IT Systems: A Structured Methodology. 1.ed. Auerbach, 2005.
- Andrew S. Tanenbaum, Redes de Computadores Campus, 4ª edição, 2003.
- James F. Kurose, Keith W. Ross, Redes de Computadores e a Internet: uma abordagem Top-Down, 3ª edição, 2006.
- Luiz Fernando Soares, Guido Lemos, Sérgio Colcher, Redes de Computadores, das LANs, MANs e WANs às Redes ATM, 2ª edição, 1995.
- Osborne, McGraw-Hill, Networks Security, The complete reference, 2004.

Unidade 4

- A.D. Rubin, D. Geer, and M.J. Ranum, Web Security Sourcebook, John Wiley & Sons, New York, 1997.
- A.D. Rubin, D. Geer, A Survey of Web Security, Computer, September 1998, pp 34-41.
- B. Laurie and P. Laurie, Apache: The Definite Guide, 2nd Edition, O'Reilly, 1999.
- http://www.gta.ufrj.br/grad/04_1/vpn/Script/RDIIntroducao.html
- Scott, Charlie; Wolfe, Paul; Erwin, Mike.Virtual Private Networks, Second Edition. O'Reilly, 1999
- Brian Browne, "Best Practices For VPNImplementation," Business Communication Review, March2001.
- Hanks, S., Editor, "Generic RoutingEncapsulation over IPv4", RFC 1702, October 1994.

Unidade 0. Diagnóstico

Introdução à Unidade

O propósito desta unidade é verificar que conhecimentos possui relacionados com Segurança de Computadores, os principais objectivos de segurança do computador, desafios de segurança do computador e o modelos de segurança de computador que podem ser adoptados pelas organizações.

Ainda nesta unidade espera-se que você traga conhecimentos sobre ataques, ameaças e vulnerabilidades, mecanismos de prevenção no computador e que saiba ainda sobre os softwares maliciosos.

Objetivos da Unidade

Após a conclusão do estudo desta unidade, deverá ser capaz de:

- Identificar e discutir sobre os conceitos de segurança do computador;
- Descrever os mecanismos de autenticação e controle de acesso;
- Identificar as principais ameaças, vulnerabilidades e riscos para os sistema de informação;
- Apontar o melhor método e as ferramentas de segurança informática mais apropriadas;

Termos-chave

Firewall: Uma firewall é um software ou hardware que verifica as informações recebidas a partir da Internet ou de uma rede e bloqueia ou permite a respectiva passagem para o computador.

Segurança: Mecanismo de proteção das informações para garantir a confidencialidade, integridade e disponibilidade dessa informação.

Protocolos: Mecanismos de comunicação da rede desenvolvidos para garantir a segurança da transmissão de dados de um ponto para outros.

Avaliação da Unidade

De modo a verificar a consolidação dos seus conhecimentos, resolva as questões que lhe são apresentadas a seguir. Se tiver alguma duvida sobre estes conteúdos, leia o Módulo de Introdução à Segurança de Computadores.

Avaliação

1. Explique com detalhes os tipos de sistema de detecção de intrusão.
2. Mencione resumidamente três categorias de políticas de controle de acesso.
3. Quais são os requisitos necessários para o controle de acesso?
4. Liste pelo menos 4 meios de autenticação de usuário.
5. O que é uma firewall?
6. Como é que funciona uma firewall?

Leituras e Outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de "Leituras e Outros Recursos do curso".

- Pfleeger, Charles P., Pfleeger, Shari L., "Security in Computing", Fourth Edition, Prentice Hall PTR, 2006.
- Malik, S., "Network Security Principles and Practices". Cisco Press. 2002.
- Mark Rhodes-Ousley, et al. "Network Security: The Complete Reference," 2003.
- Kaufman, C., et al., "Network Security: Private Communication in a Public World". 2ed., Prentice Hall, 2002.
- Gert DeLaet, Gert Schauwers, "Network Security Fundamentals", Cisco Press Fundamentals Series, 2004.
- Oliveira, Victor. Segurança da Informação – Técnicas e Soluções, 1ed, Lisboa, 2001.

Unidade 1. Conceitos gerais de segurança de computador

Introdução à Unidade

Com a utilização da Internet, o conceito da partilha e acesso de informação mudou drasticamente, cada vez mais empresas abrem o seu sistema de informação aos seus parceiros ou aos seus fornecedores, podendo assim despertar a outros a curiosidade de saber a informação desta empresa. Por este motivo, as empresas devem estar preparadas para se defender destas invasão à informação privada, conseguinte elas devem conhecer os recursos da empresa a proteger e dominar o controlo de acesso e os direitos dos utilizadores da informação.

Entretanto, para poder proteger um sistema informático, é necessário identificar as potenciais ameaças e por conseguinte conhecer e prever a maneira de proceder para se defender do inimigo. Por esta razão nesta unidade iremos primeiro fazer a revisão dos conceitos de segurança informática já estudados no módulo anterior de introdução à segurança de computador e, de seguida, iremos abordar os princípios de segurança de computadores e questões de gestão de segurança de computadores.

Objetivos da unidade

Após a conclusão desta unidade, você deve ser capaz de:

- Definir conceitos e identificar princípios de segurança de computadores;
- Reconhecer o modelo de segurança do computador
- Identificar os aspectos de gestão da segurança de computadores;

Termos-chave

Segurança: Conjunto de medidas tomadas para proteção da informação.

Informação: A informação é um conjunto organizado de dados, que constitui uma mensagem sobre um determinado fenómeno ou evento.

Actividades de Aprendizagem

Actividade 1: Conceitos gerais de segurança da informação

Introdução

O termo segurança não é novo para nós e desde crianças já ouvimos este termo na rádio, televisão etc, aplicado em outras áreas nomeadamente: militar, alimentar, pública, rodoviária entre outros. Como vemos, este termo abrange variadíssimas áreas, mas no nosso âmbito de informática ela se dedica exclusivamente à proteção da informação.

Atualmente o conceito de Segurança da Informática está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foram reservadas para tratar de padrões de Segurança da Informação. A ISO/IEC 27002:2005 continua sendo considerada, formalmente, como 17799:2005 para fins históricos.

Entretanto, nesta lição, será discutido o conceito de segurança do computador para proteção da informação nela contida.

Detalhes da actividade

A segurança informática, geralmente, consiste em garantir que os recursos materiais ou software de uma individualidade ou organização são utilizados unicamente no âmbito previsto, sem que estes sejam acessíveis por pessoas não autorizadas.

Em informática, a segurança informática pode ser definida como a capacidade de oferecer proteção a um sistema de informação, a fim de preservar a integridade, disponibilidade e confidencialidade das informações do sistema (inclui hardware, software, firmware, informação / dados e telecomunicações).

A segurança informática visa geralmente responder à três (3) objectivos principais, nomeadamente:

- **Confidencialidade**, consistindo em assegurar que só as pessoas autorizadas têm acesso aos recursos trocados;
- **Integridade**, ou seja, garantir que os dados são efectivamente os que crê ser;
- **Disponibilidade**, permitindo manter o bom funcionamento do sistema de informação;

Estes três (3) objectivos de segurança formar a sigla do inglês designada CIA (Confidentiality, Integrity, and Availability). Hoje existem muitas críticas sobre CIA, porque não fornece um quadro completo de requisitos de segurança.

Em algumas bibliografias definem como sendo cinco (5) requisitos, adicionando mais dois "extras":

A autenticação, consiste em garantir a identidade de um utilizador, ou seja, garantir a cada um dos correspondentes que o seu parceiro é efectivamente aquele que crê ser. Um controlo de acesso pode permitir (por exemplo, por meio de uma senha que deverá ser codificada) o acesso a recursos unicamente às pessoas autorizadas.

Responsabilidade, acções de uma entidade pode ser rastreada única par essa entidade. Isto suporta isolamento de falhas, recuperação e detecção de intrusão e prevenção.

As causas da necessidade de segurança

A segurança de um sistema informático deve ser abordada num contexto global e nomeadamente ter em conta os aspectos seguintes:

- A sensibilização dos utilizadores para os problemas de segurança;
- A segurança lógica, ou seja, a segurança a nível dos dados, nomeadamente os dados da empresa, as aplicações/sistemas utilizados;
- A segurança das telecomunicações: tecnologias rede, servidores da empresa, redes e acesso, etc.;
- A segurança física, ou seja, a segurança a nível das infra-estruturas materiais: salas protegidas, lugares abertos ao público, espaços comuns da empresa, postos de trabalho do pessoal, etc.

Implementação de uma política de segurança

A segurança dos sistemas informáticos limita-se, geralmente, a garantir os direitos de acesso aos dados e recursos, implementando mecanismos de autenticação e de controlo que permitem garantir que os utilizadores dos recursos sejam da rede ou não possuam unicamente os direitos que lhes foram concedidos. A utilização de uma política de segurança pode, no entanto provocar um embaraço aos utilizadores, por esta razão deve ser estudada de maneira a não impedir os utilizadores de fazer o uso que lhes é possível, e fazer de modo a que possam utilizar o sistema de informação com total confiança.

Por esta razão é necessário definir inicialmente uma política de segurança, cuja implementação esteja de acordo com as quatro (4) etapas que são apresentadas a seguir:

- Identificar as necessidades em termos de segurança, os riscos informáticos que pesam sobre a empresa e as suas eventuais consequências;
- Elaborar regras e procedimentos a implementar nos diferentes serviços da organização para os riscos identificados;
- Supervisionar e detectar as vulnerabilidades do sistema de informação e manter-se informado das falhas sobre as aplicações e materiais utilizados;
- Definir as acções a empreender e as pessoas a contactar em caso de detecção de uma ameaça;

A política de segurança é, no entanto o conjunto das orientações seguidas por uma organização (em sentido lato) em termos de segurança e deve merecer uma abordagem a nível da Direcção da Organização. Neste sentido, não cabe só aos responsáveis informáticos definir os direitos de acesso dos utilizadores mas sim aos responsáveis hierárquicos da organização. O papel dos responsáveis informático é garantir que os recursos informáticos e os direitos de acesso a estes recursos estão em coerência com a política de segurança definida pela organização.

Neste sentido, os responsáveis informáticos tem a responsabilidade de organizar acções de formação e de sensibilização junto dos utilizadores, mas deve ir, além disso, cobrir os seguintes aspectos:

- Um dispositivo de segurança físico e lógico, adaptado às necessidades da empresa e aos usos dos utilizadores;
- Um procedimento de gestão das actualizações;
- Uma estratégia de backup (copia de segurança) correctamente planificada;
- Um plano de restauração após incidente;
- Sistemas documentados e actualizados;

Conclusão

Nesta lição você estudou os conceitos gerais sobre segurança informática. Definimos o conceito de segurança informática, os principais objetivos que levam o estudo da segurança. Mais a diante abordamos as causas do estudo da segurança e aspectos a ter em conta para implementação da segurança informática em rede de computador.

Avaliação

1. Quais os principais objectivos da segurança informática?
2. Quais os niveis de planeamento de segurança da organização?
3. Mencione (3) aspectos para implementação de politica de segurança.

Actividade 2: Gestão de segurança em Sistemas de informação

Introdução

Hoje o mundo dos negócios ocorre cada vez mais na Internet, entretanto é fundamental que cada organização vele pela segurança da informação e privacidade de seus negócios. As ameaças de segurança, vulnerabilidade e risco de privacidade estão a desafiar todas as organizações hoje, riscos estes que devem ser identificados, compreendidos e vencidos.

Muitas vezes as organizações não sabem quais os riscos que enfrentam e nem como gerir esses riscos uma vez identificados. Entretanto segundo o ITIL (Information Technology Infraestructure Library), é importante, as boas práticas de segurança e privacidade fornecerem oportunidades de crescimento da organização através de uma gestão de adequada da segurança do sistema de informação da organização.

Por esta razão, nesta lição iremos abordar a gestão de segurança discutindo as formas de planificação, politicas e praticas legais de implementação de segurança de sistemas de informação.

Detalhes da atividade

Actualmente, a segurança é assunto prioritário para organizações que se preocupam com confidencialidade da sua informação. Entretanto melhores práticas devem ser incorporadas por estas organizações modernas para assegurar o monitoramento contínuo dos dados e a integridade das informações coorporativas.

Por esta razão, para a boa gestão da segurança de informação de uma organização, começa pela planificação das acções a executar.

Planeamento de Segurança

Planeamento é o fator crítico e ao mesmo tempo de sucesso, para a iniciativa de gerir a segurança da informação. Este plano é que irá indicar o caminho e os passos (actividades) que irão apontar e suprir as necessidades de segurança da organização. O plano deve ser construído tendo em conta todos os níveis da organização, nomeadamente: Física, Lógica e Administrativa.

Segundo Wadlow, não é possível comprar um dispositivo ou software que torne a sua empresa segura, assim como não é possível comprar ou criar um software capaz de tornar seu computador seguro a 100%.

A segurança é um processo e segue um ciclo após a sua implementação, o que quer dizer que um (a) especialista em segurança deve:

- Analisar o problema levando em consideração tudo que sabe sobre a segurança;
- Sintetizar uma solução para o problema a partir de sua análise;
- Avaliar a solução e avaliar em que aspectos não correspondeu às suas expectativas.

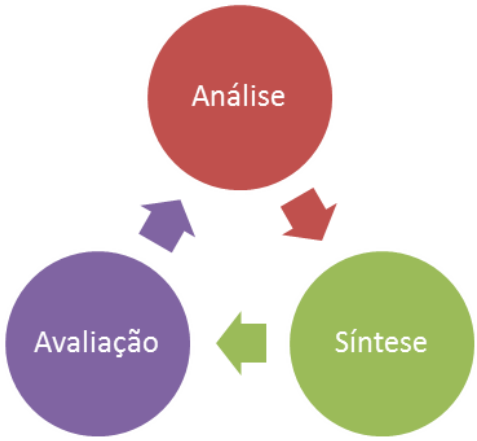

Fig. 1.1: Processo continuo de planificação de segurança.

Existem varias técnicas e normas para Gestão e Planeamento de Segurança, nomeadamente Information Security Management Maturity Model (ISM3), Information Security Forum's Standard of Good Practice"(SOGP), Control Objectives for Information and Related Technology (Cobit), Information Technology Infraestructure Library (ITIL) e Plano-Do-Check-Act (PDCA) entre outros, dos quais abordaremos o último.

Utilizaremos o método Plano-Do-Check-Act (PDCA), criado na década 20 por Walter A. Shewhart , por ser hoje o principal método da Administração para melhoria de qualidade. Ele é composto por quatro passos e se baseia no controle de processos, mas pode ser adaptado para ser utilizando num ciclo de verificação do processo de segurança do sistema de informação.

Os quatro passo são identificados pela sigla **PDCA** que são o acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Fazer, Verificar/Controlar, Actuar).

Planificar: Consiste em definir o que se quer, planejar o que será feito, estabelecer metas e definir os métodos que permitirão atingir as metas propostas. No caso de segurança de um Sistema de Informação, esta actividade pode corresponder à avaliação de riscos de segurança da informação e à selecção de controles adequados.

Fazer: É uma fase que envolve a implementação e operação dos controles, implementar e executar o planeado conforme as metas e métodos definidos. No caso de segurança de um Sistema de Informação, esta actividade pode corresponder a métodos definidos na planificação.

Controlar: Consiste em verificar a eficiência e eficácia dos resultados obtidos, verificar continuamente os trabalhos para ver se estão sendo executados conforme planeados. No caso de segurança de um Sistema de Informação, esta actividade pode corresponder à análise dos relatórios gerados e avaliação de eficácia dos métodos tomados.

Actuar: Nesta fase realizam-se mudanças, quando for necessário, para levar aos objetivos definidos, tomar acções corretivas ou de melhoria, caso tenha sido constatada, na fase anterior, a necessidade de corrigir ou melhorar algum processo. No caso de segurança de um Sistema de Informação, esta actividade pode corresponder aos ajustes necessários ou à continuidade dos métodos que produziram resultados positivos.

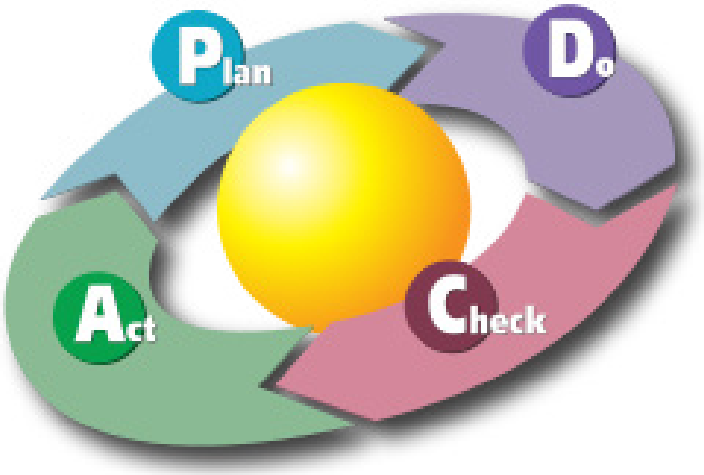

Fig. 1.2: Ciclo PDCA.

Durante o estudo de planeamento da segurança importa estudar, por exemplo, os seguintes aspectos:

- Controle de acesso ao recurso da rede;
- Proteção contra vírus;
- Segurança para equipamentos Portáteis;
- Certificação digital de chave pública;
- Detecção e controle de invasões;
- Firewall;
- VPN – Virtual Private Network;
- Controle de acesso remoto seguro;
- Segurança de correio eletrônico;
- Segurança para aplicativos Desktop;
- Monitoramento e gerenciamento da segurança;
- Segurança para servidores;
- Etc.

Politicas de Segurança

No domínio da língua portuguesa, política é definida como "orientação ou conjunto de diretrizes que regem a actuação de uma pessoa ou entidade". Uma política é considerada uma "declaração ou plano formal, breve e de alto nível que envolve as crenças gerais, metas, objectivos e procedimentos aceites por uma organização para uma área de um assunto específico." Fonte??

Na área de computação, a Política de segurança tem como objectivo principal possibilitar a gestão da segurança na organização, estabelecendo regras e padrões para proteção da informação. Resumindo, política de segurança determina o que é permitido e o que é proibido com relação à informação e recursos da organização.

A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma organização. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais lidam. Na política de segurança também são definidas as penalidades para aqueles que não cumprirem as regras.

É importante ressaltar que cada País tem legislação sobre o que deve ser seguido para que tenha um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia em termos de segurança da informação. Também este princípio é o mesmo nas organizações, cada organização define suas politicas e padrões de modo a garantir o sucesso do seu negócio.

Procedimentos de Segurança

A segurança na infraestrutura tecnológica deve ser tratada com prioridade dentro das organizações. Para que seja abordado de forma eficaz é necessário que as organizações adotem um conjunto de normas que possibilitem a redução de vulnerabilidades, riscos e ameaças à infraestrutura de tecnológica da organização. Estes procedimentos vão desde senhas clonadas passando por incêndios e roubo de informações confidenciais, diante desse cenário uma política de segurança adequada é o diferencial para a continuidade da rede.

Acompanhe, a seguir, algumas das acções que representam procedimentos de segurança para a infraestrutura tecnológica da organização.

Segurança física

A segurança física está diretamente relacionada aos aspectos associados ao acesso físico a recursos de informação, além disso, está também relacionada com as técnicas de preservação e recuperação das informações e seus meios de suporte e armazenamento. Wadlow (2000) enfatiza que, "A segurança física é uma parte importante da segurança global da rede, mas é um dos aspectos mais mal compreendidos da segurança de rede".

Para garantir a segurança do sistema de informar alguns aspectos devem ser considerados como os itens a seguir:

- Assegurar que existem portas, trancas, blindagem, guardas na sala de equipamentos;
- Proteção para Links de comunicação, equipamentos de rede e computadores;
- Monitoramento e controle de entrada e saída em sala de equipamentos e sempre que possível manter o equipamento em local trancado;
- Monitoramento de câmeras de vídeos na sala de equipamentos;
- Sistemas de alarmes para salas de equipamentos;
- Não permitir a entrada de pessoas não autorizadas;
- Cabos de redes em locais seguros;
- Sistemas de fornecimento de energia ininterrupto.

Segurança lógica

A Segurança Lógica é um aspecto abrangente e complexo, requerendo, consequentemente, um estudo muito mais apurado e detalhado. Contudo, podemos definir o controle lógico como sendo barreiras que impedem ou limitam o acesso à informação, geralmente eletrônico, e que, de outro modo, ficaria exposta ao acesso não autorizado por elementos mal intencionados. A segurança é directamente relacionada com a confidencialidade, integridade e disponibilidade (CIA) da infraestrutura tecnológica da organização.

Existem variados mecanismos de segurança lógica, nomeadamente:

- Programas de detectores de intrusões (Antivírus, Firewall, filtros anti-spam, etc.);
- Mecanismos de criptografia;
- Mecanismos de controle de acesso por palavras-chave;
- Mecanismos de certificação e utilização de protocolos seguros;
- Desabilitar boot via drive A: ou CDROM no computador principal;
- Mecanismos de restrições de acesso remoto por VPN (virtual private network);
- Desabilitar ou apagar contas de utilizadores não usadas;
- Definir uma política de backup;
- Manter o parque de máquinas com sistemas operacionais atualizados;
- Manter os utilizadores treinados.

Aspectos éticos e legais sobre segurança

A ética profissional é definida como sendo um conjunto de normas de conduta que deverão ser postas em prática no exercício de qualquer profissão.

A Ética na Segurança da Informação também está relacionada com conceitos Privacidade, Integridade, disponibilidade e confidencialidade são os quatro atributos que definem uma segurança da informação, entretanto, o código de ética dos profissionais da área de computação contemplam alguns aspectos básicos de obrigações éticas ligados a este conceitos.

As obrigações básicas são:

- Usuários de sistemas computacionais (hardware e software) devem garantir os aspectos de segurança, privacidade e interesses econômicos da organização;
- Cada usuário deverá aceder/alterar/apagar a informação cujo acesso é permitido;
- Nunca destruir maliciosamente ou modificar programas, arquivos ou dados de outra pessoa;
- Nunca violar a privacidade de um indivíduo, grupo ou organização;
- Nunca invadir um sistema por lucro ou na desportiva;
- Nunca criar ou disseminar vírus de computador;
- Nunca usar tecnologia para facilitar a discriminação ou assédio.

Conclusão

Nesta actividade você..analisou/aprendeu a identificar/analisou etc.....(veja oa seus objectivos para poder saber que tipo de actividade que deve colocar) os mecanismos para a gestão de segurança. Afirmamos que o planeamento é o fator crítico e ao mesmo tempo de sucesso, para a iniciativa de gerir a segurança da informação. Este plano é que irá apontar o caminho e os passos (actividades) que irão apontar e suprir as necessidades de segurança da organização.

A seguir abordamos o método Plano-Do-Check-Act (PDCA) que permite o controle de processos, mas pode ser adaptado para ser utilizando num ciclo de verificação de processos de segurança de sistemas de informação. Também discutimos os procedimentos físicos e lógicos para segurança da informação. No final foram abordados alguns aspectos éticos sobre a segurança.

Avaliação

1. Qual a importância de planeamento de segurança na organização?
2. Quais os itens do Processo continuo de planificação de segurança? Caracterize cada um deles.
3. O que significa a sigla PDCA?
4. O que entende de Politica de Seguraça.

Resumo da Unidade

Chegamos ao fim da unidade. Nesta unidade você estudou os conceitos gerais sobre segurança informática. Definimos o conceito de segurança informática, os principais objetivos que levam o estudo da segurança.

Você estudou também os mecanismos para a gestão de segurança. Verificamos que o planeamento é o fator crítico e ao mesmo tempo de sucesso, para a iniciativa de gerir a segurança da informação. Este plano é que irá indicar o caminho e os passos (actividades) que irão apontar e suprir as necessidades de segurança da organização.

Mais adiante abordamos as método Plano-Do-Check-Act (PDCA) que permite o controle processos, mas pode ser adaptado para ser utilizando num ciclo de verificação de processo de segurança de sistema de informação.

Avaliação da Unidade

Para verificar se compreendeu os assuntos discutidos nesta unidade, responda as a seguintes questões:

Instruções

1. Em caso de duvidas leia novamente os conteúdos correspondentes ou consulte a Internet.No contexto da segurança da informação as proteções são medidas que visam livrar os activos de situações que possam trazer prejuízos. Assumindo neste contexto que a segurança pode ser: (1) Físicas, (2) Lógicas, (3) Administrativas.

   Faça a devida correspondência dos procedimentos a baixa:
   (a) Procedimento (b) Fechadura (c) Firewall (d) Cadeado (e) Normas

2. Analise as opções, qual dos controles abaixo é um controle Lógico para segurança lógico?

   a. Firewall;

   b. Treinamento dos colaboradores;

   c. Compra softwares de gestão da informação;

   d. Procedimentos de resposta a incidentes de segurança;

3. Suponha que o seu computador foi infectado por um vírus de computador, apresente um plano de e Planeamento de Segurança utilizado o Método Plano-Do-Check-Act (PDCA).Indique as acções levadas a cabo em cada fase do método.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

- Information Systems Management Issues for the 1990s, Fred Niederman, James C. Brancheau and James C. Wetherbe, MIS Quarterly, Vol. 15, No. 4 (Dec., 1991), pp. 475-500
- WADLOW, Thomas. Segurança de Redes. Editora Campus. Rio de Janeiro, 2000.
- REZENDE, Denis Alcides e ABREU, Aline França. Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais. Editora Atlas. São Paulo, 2000.
- DIAS, Cláudia. Segurança e Auditoria da Tecnologia da Informação. Axcel Books. Rio de Janeiro, 2000.
- KRAUSE, Micki e TIPTON, Harold F. Handbook of Information Security Management. Auerbach Publications, 1999.
- KATZAM JR, Harry. Segurança de em Computação. Editora LTC. Rio de Janeiro, 1977.
- http://pt.encydia.com/es/C%C3%ADrculo_de_Deming
- http://10.13.146.103:20111/sublinha/309792/
- www.oficinadanet.com.br/artigo/1307/seguranca_da_informacao_conceitos_e_mecanismos

Unidade 2. Algoritmos de Criptografia

Introdução à Unidade

A criptografia é tão antiga quanto a própria escrita, visto que já estava presente no sistema de escrita hieroglífica dos egípcios. Os romanos também utilizavam códigos secretos para comunicar seus planos de batalha. Com as guerras mundiais e a invenção do computador, a criptografia cresceu incorporando complexos algorítmos matemáticos. A criptologia faz parte então da história humana porque sempre houve fórmulas secretas e informações confidenciais que não deveriam cair no domínio público ou na mão de inimigos.

Entretanto, podemos afirmar que a criptografia tem como principal objectivo prover uma comunicação segura, garantindo serviços básicos de autenticação, privacidade e integridade dos dados.

A Criptografa abrange desde a concepção até a implementação de sistemas de computação relacionados a diversos aspectos de segurança. A presente Unidade visa apresentar, de forma geral dos temas relacionados com ferramentas e algoritmos utilizados na criptografia de dados.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Identificar e aplicar as principais técnicas de criptografia;
- Identificar princípios e as funcionalidades de criptografia, autenticação e gerenciamento de controle de acesso;
- Aplicar as técnicas de criptografia, autenticação e gerenciamento de controle de acesso;
- Indicar os principais os algoritmos de criptografia.

Termos-chave

Chave: Em ciências de computação, chave são elementos fundamentais que interagem com os algoritmos para a cifragem/decifragem das mensagens.

Texto codificado (cifrado): Texto ilegível, gerado pela codificação de um texto claro/legível para o utilizador.

Codificar (cifrar): Acto de transformar um texto claro em um texto codificado.

Decodificar (decifrar): Acto de transformar um texto codificado em um texto claro.

Função: Uma função é relação entre dois ou mais conjuntos, estabelecida por uma lei de formação. Os elementos de um grupo devem ser relacionados com os elementos do outro grupo, atravéz dessa lei.

Criptografia: A criptografia pode ser entendida como um conjunto de métodos e técnicas para cifrar ou codificar informações legíveis por meio de um algorítmo, convertendo um texto original m um texto ilegível, sendo possível mediante o processo inverso recuperar as informações originais.

Algorítmo: Algorítmo é um conjunto finito d e regras que provê uma sequência de operações lógicas e matemáticas para resolver um tipo de problema específico.

Actividades de Aprendizagem

Actividade 1: Ferramentas de criptografia

Introdução

A criptografia considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código, é um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso das tecnologias de informação e comunicação.

A primeira vista, parece ser difícil implementar uma técnica de criptografia, porem actualmente existem muitas ferramentas para garantirem os mecanismos de criptografia e alguns já estão instalados no sistema operativo do computador.

Entretanto, nesta secção iremos abordar o conceito criptografia, a sua importância e principais técnicas de criptografia (simétrica e assimétrica).

Detalhes da actividade

A criptografia, é considerada como a ciência e a arte de escrever mensagens em forma cifrada ou em código. É um dos principais mecanismos de segurança que você pode usar para se proteger dos riscos associados ao uso de recursos tecnológicos de comunicação.

Pode-se criptografar informações basicamente por meio de códigos ou de cifras. Os códigos protegem as informações trocando partes destas por códigos predefinidos. Todas as pessoas autorizadas a ter acesso a uma determinada informação devem conhecer os códigos utilizados.

Figura 3. – Esquema geral para cifragem de um texto.

Com o uso da criptografia você pode:

- Proteger os dados sigilosos armazenados em seu computador;
- Criar uma área (partição) específica no computador, na qual todas as informações que forem lá gravadas serão automaticamente criptografadas;
- Proteger seus backups contra acesso indevido;
- Proteger as comunicações realizadas pela Internet, como os e-mails enviados/recebidos e as transações bancárias e comerciais realizadas.

De acordo com o tipo de chave usada, os métodos criptográficos podem ser subdivididos em duas grandes categorias: criptografia de chave simétrica e criptografia de chaves assimétricas.

Criptografia simétrica

A Criptografia simétrica também chamada de criptografia de chave secreta ou privada, utiliza uma mesma chave tanto para codificar como para decodificar informações, isto é, a senha é usada tanto pelo remetente para codificar a mensagem, como pelo destinatário para decodificá-la. Este modelo é considerado o mais antigo de criptografia.

A principal vantagem é a simplicidade, esta técnica apresenta facilidade de uso e rapidez para executar os processos criptográficos.

O principal problema que reside na utilização deste sistema de criptografia é que quando a chave de ciframento é a mesma que a utilizada para deciframento, esta última pode facilmente ser obtida a partir do conhecimento da primeira, ambas precisam ser compartilhadas previamente entre origem e destino, antes de se estabelecer o canal criptográfico desejado, e durante o processo de compartilhamento a senha pode ser interceptada, por isso é fundamental utilizar um canal seguro durante o compartilhamento.

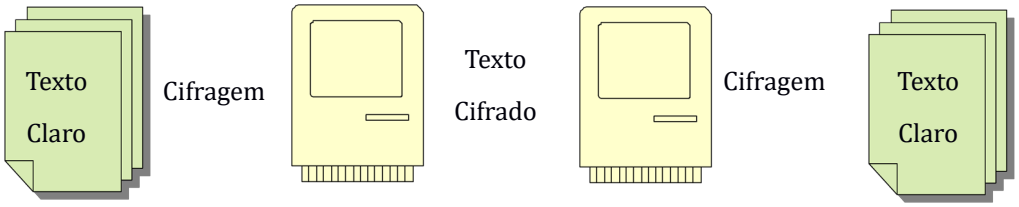

Figura 4. – Esquema de criptografia simétrica.

Exemplos de métodos criptográficos que usam chave simétrica são: AES, Blowfish, Twofish , CAST .RC4, 3DES e IDEA.

Criptografia assimétrica

A criptografia assimétrica também conhecida como criptografia de chave pública, utiliza duas chaves distintas: uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu dono. Quando uma informação é codificada com uma das chaves, somente a outra chave do par pode decodificá-la. É com a chave privada que o destinatário poderá descodificar uma mensagem que foi criptografada.

A grande vantagem deste sistema é permitir a qualquer um enviar uma mensagem secreta, utilizando a chave pública.

Como desvantagem, assume-se a confidencialidade da mensagem apenas quando a chave privada estiver segura. Caso contrário, quem possuir acesso à chave privada terá acesso às mensagens.

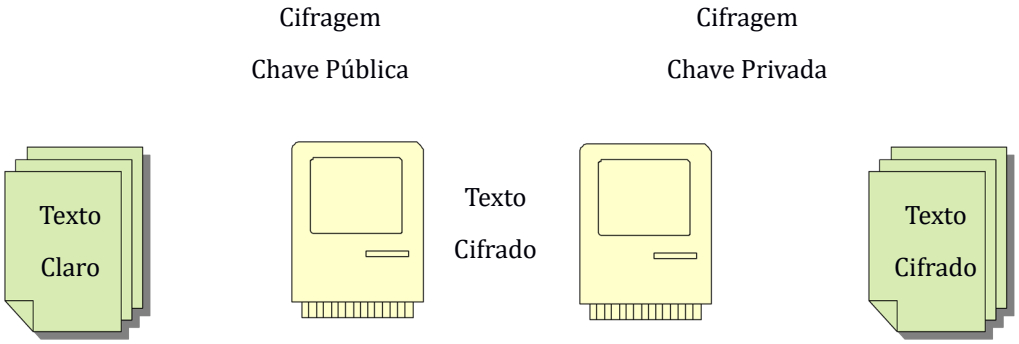

Figura 5. – Esquema de criptografia assimétrica.

Exemplos de métodos criptográficos que usam chaves assimétricas são: RSA, DSA, ElGamal ,ECC e Diffie-Hellman.

Conclusão

A criptografia só pode ser efetivada se os princípios básicos de confidencialidade, autenticação, integridade da informação forem seguidos e oferecidos. É por isso que a criptografia é um recurso tão importante na transmissão de informações pela rede e, mesmo assim, não é capaz de garantir 100% de segurança.

Uma pergunta que você deve estar a colocar-se, então qual o modelo de criptografia que devemos utilizar, simétrico ou assimétrico? A resposta é simples, devemos utilizar os dois, um modelo denominado híbrido.

Em síntese, os mecanismos de criptografia abordados nesta actividade, se bem empregados propiciam a proteção desejada à informação, aumentando a segurança dos dados e minimizando o impacto dos ataques submetidos às informações que trafegam através das redes de computadores.

Avaliação

1. Pesquise na Internet, os marcos/acontecimentos históricos da relacionados com a utilização de criptografia, e preencha a tabela a seguir:

Ano	Acontecimento

2. Pesquise na Internet, os principais algoritmos simétrico e assimétrico de criptografia, e preencha a tabela a seguir.

Algoritmo	Descrição

3. Diferencie a criptografia Simétrica da Assimétrica.

Actividade 2 - Função hash e de autenticação de mensagens

Introdução

Com o crescente uso das redes de computadores, por organizações, para conduzir seus negócios e a massificação do uso da Internet, surgiu a necessidade de se utilizar melhores mecanismos de segurança das transações e de informações confidenciais.

Devido a esta preocupação, a proteção da informação tem se tornado um dos interesses primários dos responsáveis da administradores de sistemas. A maneira mais comum de impedir estes ataques é a criptografia da informação.

A criptografia oferece técnicas para codificar e decodificar dados, de tal maneira que possam ser armazenados, transmitidos e recuperados sem sua alteração ou exposição.

Entretanto, nesta actividade iremos abordar algumas das funções implementadas em algorítmos de criptografia bem como as formas de validação para o acesso a informação confidencial e no fim abordaremos as assinaturas digitais.

Função Hash

As técnicas criptografia simétrica ou assimétrica infelizmente não pode ser empregues na prática, de forma isolada, é necessário o emprego de um mecanismo fundamental para o adequado emprego da assinatura digital. Este mecanismo é a função hashing.

Esta função tem a função principal de controlar a integridade assegurando que a mensagem recebida é a enviada pela outra parte e que não foi manipulada.

Uma função de hashing é uma função de criptografia que gera uma saída de tamanho fixo (geralmente 128 a 256 bits) independentemente do tamanho da entrada. O resultado desta saída se denomina de hash da mensagem.

O hash é uma mensagem gerada de tal forma que não é possível realizar o processamento inverso para se obter a informação original e que qualquer alteração na informação original produzirá um hash.

Os principais algorítmos de funções hashing são:

MD2 (Message Digest Algorithm RDA-MD2) & MD4

Desenhada para computadores com processador de 8 bits, e hoje quase não se utiliza. Conhecem-se muitos ataques a versões parciais de MD2. O MD4 demostrou ser mais lento e possibilita existência de colisões.

MD5 (Message Digest Algorithm RDA-MD5)

É uma versão melhorada de MD4. De momento é considerado seguro. O algoritmo foi projetado para ser rápido, simples e seguro. Seus detalhes são públicos e livres, e têm sido analisados pela comunidade de criptografia. Foi descoberta uma fraqueza, mas até agora ela não afetou a segurança global do algoritmo.

SHA-1 (Secure Hash Algorithm)

É muito similar, no seu modo de operação, ao MD5. Este algoritmo é ligeiramente mais lento do que MD5, mas a maior longitude do hash da mensagem, o faz mais seguro frente à procura de colisões.

SHA-2 (Secure Hash Algorithm)

Este é muito similar ao SHA-1, no seu modo de operação. Este algoritmo é ligeiramente mais rápido que o SHA-1, mas a maior longitude deste algoritmo é a utilização de duas funções hash similares, de diferentes tamanhos de bloco diferentes uma com 256 bits e outra com 512 bits.

Autenticação de Mensagens

Algumas vezes, não temos a necessidade de criptografar documentos. O que precisamos é simplesmente, provar que as informações desse documento não foram modificadas. Para esses casos particulares, serviços de autenticação e integridade de dados são requeridos e podem ser realizados por dois mecanismos: Código de Autenticação de Mensagem (Message Authentication Code - MAC) e Assinaturas Digitais. A meta de um MAC ou de uma assinatura digital é tornar possível enviar informação de uma parte para outra, estando o receptor apto a demonstrar que essa informação de facto veio do remetente que alega tê-la enviado e ainda que essa mesma não foi adulterada na transmissão.

Muitas pessoas confundem MACs e assinaturas digitais com checksums. Um checksum típico é um mecanismo que tem como função encontrar erros que são resultados de ruídos ou outras fontes não intencionais. Por outro lado, uma assinatura digital ou MAC é um checksum criptográfico que é ordenado para detectar ataques iniciados por fontes intencionais ou acidentais.

Códigos de Autenticação de Mensagem são mecanismos usados com sistemas de criptografia simétrica, com a finalidade de proteger a informação. Quando executado sobre uma informação, este gera um valor (pequeno pedaço de dados) que serve como código para o documento.

Obviamente que o atacante também pode modificar o MAC da mesma forma que pode modificar os dados. Porém, sem o conhecimento da chave utilizada para criar o MAC, não é possível para este modificar a informação enviada.

Assinaturas digitais

Uma assinatura digital é um tipo específico de MAC (Código de Autenticação de Mensagem) que resulta de sistemas de criptografia assimétrica. Para assinar uma mensagem, uma função Message Digest (MD) é usada para processar o documento, produzindo um pequeno pedaço de dados, chamado de hash. Uma MD é uma função matemática que refina toda a informação de um arquivo em um único pedaço de dados de tamanho fixo. Uma vez computorizada uma message digest, criptografa-se o hash gerado com uma chave privada. O resultado de todo este procedimento é chamado de assinatura digital da informação. A assinatura digital é uma garantia que o documento é uma cópia verdadeira e correta do original.

Todo o processo de geração e verificação de assinatura digital pode ser visto na figura 6, utilizando o algoritmo de criptografia assimétrica RSA.

Para ser possível que um documento ou uma assinatura adulterada não seja detectada, o atacante deve ter acesso a chave privada de quem assinou esse documento.

O que faz assinaturas digitais diferentes de MACs é que enquanto estes últimos requerem chaves privadas para verificação, assinaturas digitais são possíveis de serem verificadas usando chaves públicas.

A assinatura digital também é valiosa, pois pode-se assinar informações em um sistema de computador e depois provar sua autenticidade sem se preocupar com a segurança do sistema que as armazena.

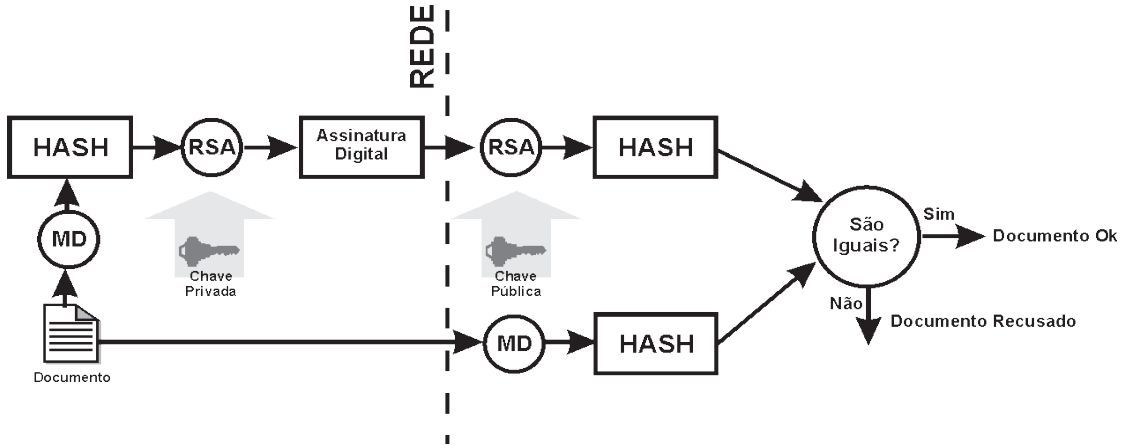

Fig. 6: Geração e verificação de assinatura digital.

Conclusão

Nesta actividade abordamos uma das funções mais utilizada na técnica de segurança com criptografia de dados. Também definimos a função hashing como sendo função de criptografia que gera uma saída de dados de tamanho fixo independentemente do tamanho da entrada. Abordados os principais algoritmos de hashing sendo os mais utilizados na actualidade o MD5 e SHA-2.

Abordamos também a certificação digital, na qual em sua essência assumimos que é um tipo de tecnologia de identificação que permite que transações eletrônicas sejam realizadas considerando sua integridade, autenticidade e confidencialidade, de forma a evitar que adulterações, captura de informações privadas ou outros tipos de acções indevidas ocorram.

Avaliação

1. Defina a função Hash.
2. Quais os algoritmos de criptografia na função Hash?
3. O que entende por assinaturas digitais.

Resumo da Unidade

Por isso é que técnicas de segurança existentes são aperfeiçoadas a cada dia e outras são criadas. Na criptografia o conceito Função Hashing é muito envolvido, sendo este método de criptografia mais usado em assinaturas digitais.

Abordamos também métodos de autenticação de mensagens dos algoritmos de criptografia, que numa análise rápida e assumindo que todos algorítmos operando em conjunto com a função hash, nos leva a concluir que

Em resumo, os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: a cifragem, a assinatura e o hashing. Estes mecanismos são componentes dos protocolos criptográficos, embutidos na arquitetura de segurança.

Para quem deseja trabalhar com computação, criptografia é uma área interessante. Obviamente, é necessário ter muita afinidade com cálculos, afinal, como pode ser notado, matemática é a base para os conceitos que envolvem a criptografia.

Avaliação da Unidade

Instruções

1. Em caso de duvidas leia novamente a texto das actividades correspondentes ou faça consulta na Internet.
2. Diferencie os algoritmos de criptografia Hash MD5 e SHA-2?
3. Descreva, usando as suas pr'prias palavras, o que é MAC (Message Authentication Code).
4. Na criptografia de chave assimétrica, as mensagens são codificadas com uma chave (escolha a opção correcta):

   A) privada e decodificada com a chave pública correspondente.

   (B) pública e decodificada com a chave privada correspondente.

   (C) pública e decodificada com a mesma chave pública.

   (D) privada e decodificada com as chaves pública e privada correspondentes.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

- GARFINKEL, Simson. PGP: Pretty Good Privacy. O'Reilly & Associates. 1995.
- KHANNA, Raman. Distributed Computing Implementation and Management Strategies. Prentice Hall, 1993.
- Gradient Technologies White Paper – Encryption Security in the Enterprise. URL: http://www.gradient.com/Products/NetCrusader/WhitePaper/wp_pbkey.htm
- White paper on the impact of the Public Key technology and Digital Signatures on CAD. URL. http://datakey.com/resources/whitepapers

Unidade 3. Segurança de rede e ferramentas de segurança

Introdução à Unidade

Cada dia mais e mais pessoas acessam redes de computadores. Sem dúvida a rede mais conhecido é a Internet. Com ela você pode colocar informações em sua máquina e disponibilizar para todo o mundo.

Os problemas relacionados com a segurança de redes e as maneiras de solucionar são o objectivo desta unidade. Inicialmente será abordada a segurança em redes de computadores, as técnicas disponíveis para melhor a confiabilidade (em termos de segurança) e as formas de emprego, seja por criptografia ou através de Firewalls. Serão apresentado alguns exemplos de técnicas de criptografia e seu emprego no estabelecimento de conexões confiáveis.

Por de trás de mecanismos e ferramentas de segurança estão os padrões e protocolos que permitem comunicação entre os intervenientes diante regras bem definidas. Estes protocolos de segurança garantem o sigilo da informação e das identidades dos intervenientes da comunicação, tanto em comunicação física como em lógica (sem fio).Em suma, nesta unidade abordaremos a segurança de redes de computador, as boas praticas, principais protocolos e aplicativos utilizados nesta área.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Identificar os protocolos e padrões de segurança na Internet;
- Distinguir as formas de segurança em redes sem fio;
- Identificar as principais aplicações de autenticação na Internet;
- Aplicar as boas práticas de segurança;
- Descrever as formas seguras de transações eletrônicas;
- Identificar as formas de autenticação remotas (RADIUS servisse).

Termos-chave

Vulnerabilidade: Falha ou fraqueza que, se explorada, pode resultar em comprometimento intencional ou não intencional do sistema.

IP (Internet Protocol): Protocolo de camada de rede que contém informações de endereços e algumas informações de controle que permitem que os pacotes/ dados sejam direcionados e entregues do host de origem para o host de destino. O IP é o principal protocolo de camada de rede no conjunto de protocolos da internet.

Autenticação: é a capacidade de garantir que alguém, ou algum equipamento o acesse, dentro de um contexto definido.

Acesso Remoto: Acesso a redes de computador a partir de um local remoto. As conexões de acesso remoto podem ser originadas de dentro da rede da empresa ou a partir de um local remoto fora da rede da empresa.

Protocolos: Protocolo é o conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas na comunicação.

Actividades de Aprendizagem

Actividade 1: Protocolos e padrões de segurança na Internet;

Introdução

Dizemos que uma casa está segura, quando as vulnerabilidades dela foram minimizadas. Mas, segundo a ISO (International Standardization Organization - Organização Internacional para Padronização), no contexto da computação, vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações.

Inicialmente os dispositivos se conectavam à rede de Internet por meio de conexão discada (modem e de uma linha telefônica), hoje, a conexão deixou se ser exclusiva a estes diapositivos computacionais da rede corporativa, passou também a ser acedida por dispositivos móveis, TVs e até eletrodoméstico. A possibilidade de acesso à rede alargou-se e ao mesmo tempo as vulnerabilidades também se alargaram, por esta razão é importante que estudemos as formas de proteger a informação tanto da organização como pessoal.

Detalhes da actividade

O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém. A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objectivos de uma organização, formalizados nos termos de uma política de segurança. (SOARES; LEMOS e COLCHER,1995, p.448):

A segurança de rede começa com a existência de politica de segurança da organização. Nesta política devem estar definidas as formas de acesso à informação da organização. Existem diferentes formas e níveis de segurança para proteger as informações enviadas na rede. A forma mais básica é a autenticação e a autorização do usuário ou dispositivo, onde ele se identifica para a rede e para o ponto remoto através de um nome de usuário e uma senha, que são verificados antes que o dispositivo possa entrar no sistema. Este processo de segurança pode ser reforçado com a criptografia dos dados para evitar que outras pessoas usem ou leiam os dados e com a utilização do firewall.

Protocolos de segurança

Vimos anteriormente que os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos: o ciframento, a assinatura digital e o hashing. Esses mecanismos são componentes de protocolos criptográficos, embutidos na arquitetura de segurança dos produtos destinados comunicação eletrônica, portanto, estes protocolos provêm os serviços associados à criptografia que viabilizam a comunicação na rede mundial.

A seguir, alguns exemplos de protocolos que empregam sistemas criptográficos:

- SSL (Secure Sockets Layer) e TLS (Transport Layer Security);
- PGP (Pretty Good Privacy);
- Kerberos;
- SSH;
- IPSec;
- S/MIME;
- SET e outros

Padrões de segurança

Atualmente para o estudo de Segurança da Informação, somos remetidos ao estudo de normas de padronização. Entretanto, a Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799. A série de normas ISO/IEC 27000 foi reservada para tratar de padrões de Segurança da Informação, incluindo a complementação ao trabalho original do padrão inglês.

Portanto para o estudo de atributos básicos de padrões de segurança, estes devem seguir as normais internacionais estabelecidas pela ISO (Organização Internacional para Padronização), das quais passamos a citar algumas normas segundo a norma ISO/IEC 27001.

Salientar que esta norma é universal para todos os tipos de organizações e foi elaborada para especificar os requisitos para o estabelecimento, implementação, operacionalização, monitorização, revisão, manutenção e melhoria de um SGSI, dentro do contexto dos riscos de negócio de uma organização.

A atribuição do certificado de garantia de segurança seguindo a norma ISO/IEC 27001 envolve alguns passos de auditoria, que consiste na revisão linear da documentação do sistema de informação, política de segurança da organização e plano de tratamento de risco.

A norma 27001 apresenta alguns requisitos que sugerem alguns procedimentos para uma boa Gestão de Segurança da Informação, que são indicadas a seguir:

- Definição do contexto;
- Identificação de riscos;
- Avaliação de riscos;
- Tratamento do risco;
- Comunicação do risco;
- Monitoramento e análise crítica de riscos.

Após o processo de análise e avaliação dos riscos, existem várias opções para o seu tratamento:

- Aplicar medidas de segurança: escolher as medidas mais apropriadas para reduzir o custo;
- Aceitar o risco: conhecer e conscientemente aceitar o risco, sabendo que este atenta à política de segurança da organização;
- Evitar o risco: não permitir acções que possam causar a ocorrência de riscos;
- Transferir o risco: transferir os riscos associados para outras partes, por exemplo, seguradoras ou fornecedores.

Neste sentido, observa-se que os padrões de segurança podem ser úteis para satisfazer os requisitos de segurança de um sistema de informação através da reutilização de práticas bem sucedidas para a segurança da informação, podendo ser associados a modelos de referência e utilizados para implementar um processo de gestão de riscos de segurança da informação.

Dentro da série 27000 ainda podemos referir que existem outras normas, nomeadamente: 27002 (Código de Práticas), 27003 (Guia de Implementação), 27004 (Métricas e Medição), 27005 (Directrizes de Gestão de Risco) e 27006 (Directrizes de Serviços de Recuperação de Desastres).

Conclusão

Chegamos da actividade da lição onde abordados o conceito de segurança em redes de computadores. Vimos também que segurança de rede começa com a existência de politica de segurança da organização, desta politica deve ser definida pelos superiores da organização em coordenação com equipe técnica. Abordamos os protocolos de segurança da informação na rede de computares, onde assumimos estes trabalham com as técnicas de encriptação já estudada nas lições anteriores.

No final, abordamos os padrões de segurança nas organizações e vimos que esta deve seguir as normas estabelecidas ela ISSO (Organização Internacional para Padronização), organismo que estabelece as normas e certifica os mecanismos de segurança adoptados pelas organizações.

Avaliação

1. O que é um protocolo de segurança?
2. Aponte pelo menos três (3) protocolos de segurança e descreva - os. (faça buscas na internet)
3. O que são normas de Padrões de Segurança?

Actividade 2: Segurança de rede sem fio

Introdução

A segurança de dados transmitidos é feita desde à muito tempo. Com as ligações físicas ainda se consegue acreditar que ela é efectiva, mas com as redes sem fio muitos ainda duvidam que os seus dados não estejam sendo acessíveis por pessoas não autorizadas. Ai criptografia sem duvidas desempenha um papel importantíssimo.

Hoje, as redes sem fio estão ganhando campo, sendo adoptadas largamente pelas organizações devido à mobilidade e economia de custos em materiais de comunicação físicos, apesar de existirem equipamentos ainda bastantes caros.

Nesta actividade, abordaremos a segurança nos dispositivos sem fios, os principais protocolos usados nesta comunicação.

Detalhes da actividade

Redes sem fio, tradução do inglês Wireless Network, é qualquer tipo de conexão entre dispositivos de comunicação para transmissão de informações sem o uso de fios ou cabos. Deste modo, qualquer comunicação que exista sem a existência de um fio ou um cabo caracteriza-se por uma conexão wireless. Podemos citar diversos meios de utilização do wireless, como a conexão existente entre a TV e o controle remoto, entre o celular e as torres das operadoras e até o rádio da polícia com as centrais de operação e outros exemplo.

O funcionamento de uma rede sem fio é bastante simples, é necessário apenas a utilização de um aparelho chamado Ponto de acesso (Acess Point), assim, ele transforma os dados da rede em ondas de rádio ou infravermelho e o transmite por meio de antenas.

Existem dois tipos de topologias de redes sem fio: as chamadas aplicações WLAN (Wireless Local Area Network) ou indoor e WWAN (Wireless Wide Area Network) ou outdoor.

Padrões de redes Wireless

Existem 4 padrões principais para as Redes sem fio: 802.11b, 802.11a e 802.11g.

O padrão 802.11 foi desenvolvido pelo IEE (Institute of Electrical and Electronics Engineers) para redes sem fio. O padrão 802.11 pode ser comparado aos padrões de rede de local cabeada 802.3 e 802.5 para Ethernet e Token-Ring. Com estes padrões é possível trabalhar com vários equipamentos de diferentes fabricantes e com grande eficiência.

802.11a: Opera numa frequência de 5Ghz, o que oferece grande confiabilidade, por ser uma frequência menos utilizada. Fornece uma velocidade mais rápida que o padrão 802.11b (até 54 Mbps), porém com um alcance operacional menor.

802.11b: é o tipo de rede wireless mais popular, com frequência é de 2.4 Ghz e velocidade máxima de 11 Mbps e alcance máximo operacional de 100 metros em ambiente fechado e 180 metros em área aberta.

802.11g: é uma linha de produtos de fabricantes de rede sem fio que combina conceitos da 802.11a e 802.11b, conhecida como tecnologia "G", apresenta velocidade do 802.11a, mas é totalmente compatível com redes 802.11b existentes. É mais barato que a tecnologia 802.11a, mas ainda usa a frequência de 2.4 Ghz.

802.11n: o padrão 802.11n introduziu a possiblidade de utilização de canais que permitem a duplicação de taxas de transferência por canal. As taxas de transferências disponíveis vão de 65 Mbps a 300 Mbps. Método de transmissão: MIMO-OFDM e faixa de frequência: 2,4 GHz e/ou 5 GHz.

Protocolos de segurança de rede sem fio

Existem vários protocolos de segurança em redes sem fio, a seguir veremos alguns mais utilizados na segurança de redes sem fio:

WEP (Wired Equivalent Privacy): Foi o primeiro protocolo de criptografia lançado para redes sem fio (o mais antigo). O WEP é um sistema de criptografia adotado pelo padrão IEEE 802.11. Ele utiliza uma senha compartilhada para criptografar os dados e funciona de forma estática, por esta razão é considerado o mais frágil em termos de segurança.

WPA (Wi-Fi Protected Access): O WPA criptografa as informações e assegura que a chave de segurança de rede seja modificada. Existem dois tipos de autenticação WPA: WPA e WPA2. O WPA foi criado para funcionar com todos os adaptadores de rede sem fio. O WPA2 é mais seguro que o WPA, mas não funciona com alguns adaptadores de rede antigos. O WPA foi criado para ser usado com um servidor de autenticação 802.1X, que distribui chaves diferentes para cada usuário. Isso é conhecido como WPA-Enterprise ou WPA2-Enterprise. Ele também pode ser usado no modo de chave pré-compartilhada, isso é conhecido como WPA-Personal ou WPA2-Personal.

Autenticação 802.1X: A autenticação 802.1X pode ajudar a aumentar a segurança de redes sem fio 802.11 e redes Ethernet com fio. A 802.1X usa um servidor de autenticação para validar usuários e fornecer acesso de rede. Em redes sem fio, a 802.1X pode funcionar com chaves WPA, WPA2 ou WEP. Esse tipo de autenticação normalmente é usado na conexão com uma rede de local de trabalho.

Conclusão

A segurança é um ponto fraco das redes sem fio pois o sinal propaga-se pelo ar em todas as direções e pode ser captado a distâncias de centenas de metros por utilizadores com intenções de invasão de dados, o que torna as redes sem fio inerentemente vulneráveis à interceptação. A escolha de um equipamento mais moderno em redes sem fio pode ajudar na implementação de mecanismo de segurança mais sofisticado.

Avaliação

1. 1. O que são redes sem fio?
2. 2.Quais os principais padrões de redes sem fio?
3. 3.Quais o protocolos de segurança das redes sem fio?

Actividade 3: Aplicações de autenticação da Internet

Introdução

Quando um cliente na rede se liga ao Ambiente de Trabalho Remoto, há necessidade de verificar se está a ligar ao computador remoto ou ao servidor correcto. Esta medida de segurança ajuda a evitar que seja ligado a um computador ou servidor diferente do pretendido. Este processo é recorre a aplicações de autenticação.

A forma da verificação requerida para ligar é determinada pela sua política de segurança do sistema, que é definida pelo administrador de sistema. Nesta actividade iremos abordar alguns serviços utilizados para a autenticação remota.

Detalhes da atividade

A internet é um local inseguro. Alguns protocolos utilizados na internet não provêm segurança. Ferramentas para intersecção de senhas de usuários pelas redes são de uso comum por utilizadores mal intencionados. Assim, aplicações que enviam dados em modo texto pela rede, como FTP e Telnet, são extremamente vulneráveis. O Firewal é um dos mecanismos de segurança muito usado na actualidade, este é o responsável pelo controle dos dados transferidos de e para o seu computador através da internet, além de prevenir que informações pessoais ou confidenciais sejam transmitidas pelo seu computador para a internet e impedir a invasão da máquina por software malicioso.

É importante salientar que antes de selecionar e configurar um serviço de autenticação, saiba como esses serviços funcionam e como precisa ser configurado. Além da autenticação, cada um dos serviços suportados fornece a capacidade de configurar regras de autorização que definem como os privilégios de usuário serão atribuídos a um determinado usuário remoto. Certifique-se de que a função ou privilégio de usuário adequado seja atribuído.

Kerberos

O protocolo Kerberos foi desenvolvido para solucionar problemas deste tipo, provendo uma autenticação confiável sobre redes abertas e inseguras nas quais a comunicação entre computadores pode ser interceptada. Ele proporciona autenticação forte para aplicações cliente/servidor pelo uso de criptografia de chave secreta, de modo que um cliente prova sua identidade a um servidor (e vice-versa) através de tais redes.

(http://www.gta.ufrj.br/grad/10_1/1a-versao/kerberos/kerberos.html)

SSL & TLS

Secure Sockets Layer (SSL): SSL é um protocolo que permite a transmissão de informações através da internet de forma criptografada. O SSL garante que a informação seja enviada, sem alterações e exclusivamente para o servidor para o qual pretende enviar.

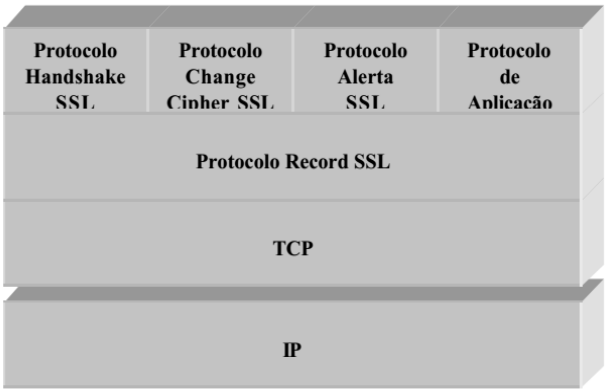

Fig. 7: Estado do protocolo SSL e suas camadas

Transport Layer Security (TLS): TLS foi criado como o sucessor do SSL, é protocolo de segurança por meio de criptografia, interoperabilidade, extensibilidade e eficiência. Isso quer dizer que este protocolo é capaz de estabelecer uma conexão segura entre duas entidades e de garantir que dois aplicativos consigam se comunicar ou trocar parâmetros independentemente da forma como foram construídos.

Para aprofundar mais sobre os protocolos de segurança SSL & TLS veja em: http://www.gta.ufrj.br/grad/11_1/tls/

Radius: Abreviação de Serviço de Autenticação e Dial-in Remoto do usuário (remote authentication and dial-In user service, no inglês). Sistema de autenticação e contabilidade. Verifica se informações como o nome do usuário e sua senha, que passam pelo servidor do RADIUS, estão corretas; em caso positivo, autoriza o acesso ao sistema. Este método de autenticação pode ser usado com um token, smart card, etc., para fornecer autenticação de dois fatores.

Transação Eletrônica Segura

Vimos como os protocolos seguros são usados para assegurar a privacidade e integridade das comunicações na rede e estes também são replicados para aplicações que funcionam na rede. Entretanto, transações são mais complicadas que simples relações entre cliente e servidor.

O principal objectivo dos protocolos de segura é garantir as transações de dados; em particular, compras com cartão de crédito. SSL e S-HTTP podem ser usados para assegurar a transação entre comprador e vendedor. Porém, há outras partes envolvidas na transação, como a prestadora do cartão de crédito e o banco do comprador.

Programas de verificação de Vulnerabilidades

Hoje os dados são o maior activo das organizações e estes circulares pela Internet. O utilizador mal intencionado também circula pela internet e está cada vez mais sofisticado. Muitas das vezes os administradores não conseguem identificar as vulnerabilidades dos seus sistema devido a falta de meios.

Entretanto, devido ao custo elevado de soluções proprietárias de software para a verificação de vulnerabilidades é a criação de relatórios de forma automática.

Nesta secção iremos abordar algum exemplo de softwares que podem ser utilizados para testar e vulnerabilidade de sistemas:

Nessus: é uma ferramenta para verificação de vulnerabilidades, em alguns casos durante sua utilização equipamentos podem ficar inoperantes ou lentos devido ao grande número de testes (através de portas) que este aplicativo realiza.

Segundo o wikipedia do Nessus (https://pt.wikipedia.org/wiki/Nessus), ele é um programa de verificação de falhas/vulnerabilidades de segurança (portas, vulnerabilidades, exploits). Ele é composto por um cliente e servidor, sendo que o scan propriamente dito é feito pelo servidor (servidor Nessus). O Nessus ajuda a identificar e resolver alguns problemas de vulnerabilidades. A parte Servidor executa os testes enquanto a parte cliente permite a configuração e emissão de relatórios. O Nessus é distribuído sob os termos da Licença Pública Geral GNU.

Skipfish: Uma ferramenta para teste de segurança em sites totalmente automatizada e é muito leve e muito rápida (podendo executar 2.000 pedidos por segundo). Assim como as demais ferramentas de segurança, possui diversos tipos de testes de segurança, incluindo Blind SQL Injection. (O programa funciona em Windows, Linux e Mac OS X).

Websecurify: é uma ferramenta open source muito fácil de usar que identifica automaticamente as vulnerabilidades de aplicações web. Ela pode criar relatórios simples (que podem ser exportados em vários formatos). A ferramenta tem suporte a vários idiomas e é extensível, apresentando suporte a plugins. (O programa funciona em Windows, Linux e Mac OS X).

Wireshark: (anteriormente conhecido como Ethereal) é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do Wireshark são parecidas com o tcpdump mas com uma interface GUI, com mais informação e com a possibilidade da utilização de filtros.

É então possível controlar o tráfego de uma rede e saber tudo o que entra e sai do computador, em diferentes protocolos, ou da rede à qual o computador está ligado (https://pt.wikipedia.org/wiki/Wireshark).

Para mais programas de verificação de vulnerabilidades de segurança acesse:

- http://sectools.org/tag/sniffers/
- http://webresourcesdepot.com/10-free-web-application-security-testing-tools/
- http://insecure.org/tools/tools-pt.html

Conclusão

Nesta lição abordamos alguns serviços utilizados para a autenticação remota. Muitos dos serviços estão implementados em alguns softwares que podemos encontrar no mercado. Estes softwares implementam os protocolos de segurança para autenticação remota, Kerberos, SSL & TLS, Radius entre outros. Em ambiente Unix, muitos administradores de rede configuram os acessos remotos através do Nessus, por este ser simples e indicam as vulnerabilidades detectadas e os passos que devem ser seguidos para eliminá-las.

Avaliação

1. Qual mecanismo mais utilizado para aumentar a segurança de redes de computadores li(gados à internet.

    a) Criptografia

    b) Firewall

    c) Autenticação

    d) Controle de acesso

2. Pesquise mais sobre Serviço de Autenticação e Dial-in Remoto do usuário (RADIUS)

Resumo da Unidade

Chegamos ao fim da unidade onde abordados o conceito de segurança em redes de computadores. Vimos também que segurança de rede começa com a existência de uma política de segurança da organização, esta política deve ser definida pelos superiores da organização em coordenação com a equipa técnica. Abordamos os protocolos de segurança da informação na rede de computares, onde assumimos que estes trabalham com as técnicas de encriptação já estudada nas lições anteriores.

Abordamos os padrões de segurança nas organizações e vimos que estes deve seguir as normas estabelecidas pela ISSO (Organização Internacional para Padronização), organismo que estabelece as normas e certifica os mecanismos de segurança adoptados pelas organizações.

A segurança foi o ponto de destaque nesta unidade, onde abordamos a sua importância nas redes sem fio e vimos que a escolha de um equipamento mais moderno em redes sem fio pode ajudar na implementação de mecanismo de segurança mais sofisticado.

Na ultima lição abordamos alguns serviços utilizados para a autenticação remota e afirmamos que muitos dos serviços estão implementados em alguns softwares que podemos encontrar no mercado. Estes softwares implementam os protocolos de segurança para autenticação remota, como a caso de Kerberos, SSL & TLS, Radius entre outros.

Avaliação da Unidade

Para verificar se compreendeu os assuntos discutidos nesta unidade, responda às seguintes questões:

Instruções

Em caso de dúvidas leia novamente os conteúdos correspondentes ou consulte a Internet.

1. Estude a normas ISO/IEC 27005 (Directrizes de Gestão de Risco).
2. Baixe os softwares Nessus ou Skipfish consoante o seu sistema operativo e faça um teste de vulnerabilidades na sua maquina. Estude os resultados e possíveis soluções para minimizar as vulnerabilidades.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

- SOARES, Luiz Fernando Gomes; LEMOS, Guido; COLCHER, Sérgio. Redes de computadores das LANs, MANs e WANs às Redes ATM. 2.ed. Rio de Janeiro:, 2015.
- KUROSE, James; ROSS, Keith. Rede de computadores e a internet: Umaabordagem top-down. 3.ed. São Paulo: Pearson Addison Wesley, 2006.
- McCumber, John. Assessing and Managing Security Risk in IT Systems: A Structured Methodology. 1.ed. Auerbach, 2005.
- Andrew S. Tanenbaum, Redes de Computadores Campus, 4ª edição, 2003.
- James F. Kurose, Keith W. Ross, Redes de Computadores e a Internet: uma abordagem Top-Down, 3ª edição, 2006.
- Luiz Fernando Soares, Guido Lemos, Sérgio Colcher, Redes de Computadores, das LANs, MANs e WANs às Redes ATM, 2ª edição, 1995.
- Osborne, McGraw-Hill, Networks Security, The complete reference, 2004.
- http://cartilha.cert.br/redes/

Unidade 4: Segurança na Web

Introdução à Unidade

A Web foi projectada, inicialmente, sem muita ou quase nenhuma preocupação com segurança. O objetivo principal era disponibilizar informações de uma forma mais amigável que os recursos disponíveis na época. Com o rápido crescimento da Web e com a diversificação de sua utilização, a segurança se tornou um ponto de importância crucial, principalmente para quem tem a Web como uma das principais fontes de rendimento ou de comércio.

Nesta unidade iremos abordar alguns aspectos de segurança que devem ser levados em consideração em um servidor Web, a segurança da máquina, do cliente Web, dos dados em trânsito, assim como algumas recomendações para tornar o servidor Web mais seguro.

Objetivos da Unidade

Após a conclusão desta unidade, deverá ser capaz de:

- Identificar os principais protocolos de segurança da web;
- Listar as formas de segurança em web;
- Descrever as principais formas de ataque;
- Aplicar as boas praticas de segurança na web.

Termos-chave

Autenticação: Processo de verificação de identidade de um indivíduo, dispositivo ou processo. A autenticação normalmente ocorre por meio do uso de um ou mais fatores de autenticação.

Ameaça: Condição ou atividade que pode fazer com que as informações ou os recursos de processamento de informações sejam intencionalmente ou acidentalmente perdidos, modificados, expostos, inutilizados ou de outra forma afetados em detrimento da organização.

Protocolo: Método de comunicação aceite e usado dentro das redes. Especificação que descreve as regras e procedimentos que os computadores devem seguir para desempenhar as atividades em uma rede.

Porta: Pontos de conexão lógica (virtual) associados a um protocolo de comunicação particular a fim de facilitar a comunicação entre as redes.

Firewall: O Firewall é uma importante barreira de entrada entre a rede privada e a Internet. Ele deve ser utilizado para restringir as portas disponíveis na rede, os tipos de pacote que podem passar pela rede, os protocolos permitidos, etc.

Actividades de Aprendizagem

Actividade 1: Segurança em Web Services

Introdução

Construir Web Services seguros implica entender as ameaças em que os serviços estão expostos e ter definido qual o nível de segurança que deve ser alcançado. A maneira mais eficaz de se implementar segurança em aplicações web é estar em consonância com os princípios, padrões e práticas de segurança. Os impactos negativos de uma falha de segurança podem comprometer os dados confidenciais, ou ceder acesso, não autorizado, e até mesmo comprometer a reputação e confiabilidade da organização.

Nesta actividade iremos abordar alguns aspectos de segurança, principais ameaças e técnicas de segurança de tráfego na web.

Detalhes da actividade

A World Wide Web (WWW) é fundamentalmente uma aplicação cliente/servidor trabalhando sobre a internet e intranets TCP/IP. Dessa maneira, as ferramentas de segurança e as técnicas explicadas neste módulo são relevantes para a segurança na Web.

As Ameaças na Web

Atualmente, a Web enfrenta diferentes formas de ameaça que foram surgindo ao longo de sua evolução. A Internet funciona para a Web como seu mecanismo de transporte e, portanto, herda assuas vulnerabilidades de segurança. Devido à pressa na construção de novas funcionalidades em todo o ambiente, projectistas não consideraram o impacto em segurança que esta nova tecnologia causaria, deixaram de ver importantes pontos de possíveis ataques e vulnerabilidades. E quando a Web caminhou para o mundo comercial, as ameaças tornaram-se mais sérias e os pesquisadores começaram a procurar se defender de ataques seus dado.

A seguir apresentamos as principais formas de ameaças na web:

Integridade: Ataques contra a integridade consistem em alterações maliciosas de dados, programas, mensagens e até mesmo de informações da memória. Este tipo de ataque é devastador. Na maioria dos sistemas, este tipo de ataque permite, ao atacante, ler/modificar/remover qualquer arquivo, enviar mensagem, etc.

Confidencialidade: Este ataque tenta revelar informações confidenciais para terceiros. Um atacante pode tentar obter estas informações na máquina do usuário ou no servidor. Por exemplo, os "browsers" normalmente mantêm caches locais de visitas efetuadas pelos usuários a servidores Web, que podem revelar alguns "hábitos" deste usuário.

Negação de Serviço: Esta é uma das mais sérias ameaças na Web e a mais difícil de prevenir. Este tipo de ataque consiste em acções maliciosas que desviam acessos a um determinado serviço que se encontra disponível. Um exemplo típico deste tipo de ataque, são os acessos feitos a determinado servidor Web que é desviado para um outro servidor, normalmente um clone.

Autenticação: Neste caso, o atacante se faz passar por outro, obtendo a senha do usuário por algum método qualquer, como por exemplo, filtrando pacotes na rede e capturando senhas não criptografadas.

Segurança no Servidor web

Em um ambiente cliente/servidor as atenções normalmente estão direcionadas para o servidor, onde residem as informações e, portanto, se encontra o foco de ameaças. Segurança no servidor Web consiste, em geral, em um ponto crítico em relação para algumas organizações que tem a Web a sua principal fonte de renda.

Os assuntos de segurança tratados aqui são direcionados ao servidor Apache em ambiente Unix por ser o mais utilizado na Internet. Mas, a maioria das recomendações, tópicos, sugestões, etc. é válida para outros servidores Web.

Configurações Básicas: Um dos maiores problemas de segurança na web, assim como em serviços de rede, é a má configuração e esta pode levar a. um desastre. Se não se tem uma boa configuração torna-se difícil o emprego de uma política de segurança satisfatória.

Estrutura de Diretórios: Separação dos diretórios Raiz e de Documentos. A Raiz do servidor: tem informações de controle do servidor, como: arquivos de configurações, aplicações adicionais, etc. Raiz de Documentos (o Web space do servidor): contém o conteúdo "público" (informações disponibilizadas via conexões HTTP). Geralmente este é um sub-diretório do diretório raiz do servidor.

Server-Side Include (SSI): SSI é um código HTML que "injeta" a saída de um comando ou um arquivo dentro da página quando enviada pelo servidor para o browser. A formatação HTML é um conteúdo estático, SSI é um conteúdo dinâmico. Os SSI's são bastante úteis, mas podem também acabar com a portabilidade e podem abrir sérios furos na segurança.

Autenticação: Em geral, serviços Web são muito dependentes de servidores de nomes. Se um servidor de nome é atacado, servidores Web dependentes deste serviço podem ter sua autenticação comprometida.

CGI Scripts: É um mecanismo independente de plataforma, provido pelo servidores Web, que permite executar programas/scripts a partir de uma URL. Estes scripts são geralmente escritos em Perl, Shell, Tcl, Java, Python ou C (maioria escritos em linguagem interpretadas).

Conclusão

Chegamos ao fim desta actividade, onde abordadmos os serviços da as principais formas ameaças da Web e mecanismos de prevenir estas ameaças através de mecanismos de segurança na Web.

Avaliação

1. Defina por suas palavras o que são Serviços Web?
2. Indique as principais formas de ameaças da web.
3. Quais são os aspectos importantes a ter em conta na segurança do servidor web?

Actividade 2: Principais protocolos da web

Introdução

Nesta actividade iremos conhecer os principais protocolos TCP/IP (também conhecidos como protocolos para Internet) e as suas principais características. Este protocolo forma o grupo de protocolos de comunicação que implementam a pilha de protocolos sobre a qual a Internet carrega e a maioria das redes comerciais funcionam. São chamados de protocolos TCP/IP porque o protocolo TCP (Transfer Control Protocol) e o IP (Internet Protocol) foram os primeiros a ser definidos.

Detalhes da atividade

A comunicação na Internet é feita utilizando-se vários protocolos, dos quais passamos a citar:

HTTP (Hyper Text Transfer Protocol): É o protocolo utilizado para controlar a comunicação entre o servidor de Internet e o browser. Quando se abre uma página da Internet, vemos texto, imagens, links ou outros serviços associados à Internet ou a uma Intranet. O HTTP é o responsável por redireccionar os serviços quando seleccionamos alguma das opções da página web.

HTTPS (Hyper Text Transfer Protocol Over Secure Socket Layer): Versão do protocolo HTTP seguro, que fornece autenticação e comunicação criptografada na World Wide Web feita para comunicações que precisem ser seguras, como autenticação da Web.

SMTP (Simple Mail Transfer Protocol): Como o nome indica, este protocolo serve para efectuar a transferência de emails entre os servidores. O servidor de email utiliza o POP ou IMAP para enviar as mensagens de email aos utilizadores.

FTP (File Transfer Protocol): Este protocolo permite transferência de dados ou ficheiros entre computadores, mesmo com sistemas operativos diferentes como o Linux e o Windows. O FTP é também um comando que permite ligação de um cliente a um servidor FTP de forma a transferir dados via Internet ou Intranet.

SET (Secure Eletronic Transaction): o SET é um protocolo desenvolvido por um consórcio de empresas, formado pela Visa, MasterCard, Netscape, IBM, Microsoft, GTE, SAIC, Terisa Systems e Verisign, para garantir a transmissão segura de informações pessoais e financeiras em redes públicas. Essa segurança é garantida com o uso de esquemas de criptografia durante as actividades de autorização, autenticação e identificação da compra e venda eletrônica.

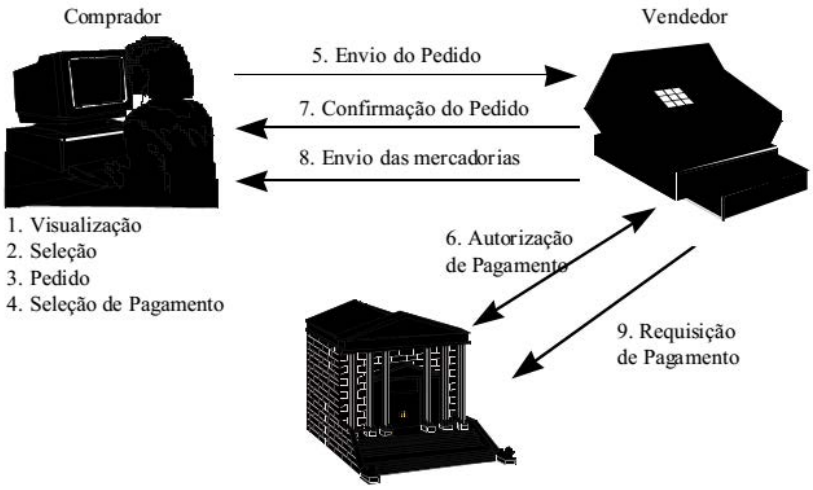

Fig. 8: Processo de compra utilizando o protocolo STL

IPSec: O Protocolo IPSec implementa uma forma de tunelamento na camada da rede (IP) e é parte das especificações da pilha de protocolos IPV6. Ele fornece autenticação em nível da rede, a verificação da integridade de dados e transmissão com criptografia e chaves fortes de 128 bits. Implementa um alto grau de segurança na transmissão das informações.

O protocolo IPSec dificulta de maneira permanente uma eventual tentativa de ataque vindo por parte do "hacker", tornando muito difícil fazer um grampo em linhas de comunicação e obter qualquer informação útil do tráfego da rede.

Transport Layer Security (TLS) & Secure Sockets Layer (SSL) : Protocolos já descritos na unidade anterior, mas não deixaremos de abordar devido à sua importância na segurança web. Estes protocolo permite que aplicativos cliente/servidor possam trocar informações em total segurança, protegendo a integridade e a veracidade do conteúdo que trafega na Internet. O protocolo SSL foi originalmente desenvolvido pela Netscape para ser utilizado, em seus browser's, na transmissão de dados sigilosos.

Conclusão

Nesta actividade vimos os principais protocolos utilizados na Web, suas principais características.

Vimos que o Protocolo SSL, doravante Protocolo TLS, oferece uma camada de segurança para duas aplicações comunicantes (cliente e servidor). O interessante deste protocolo e que não é restrito a um único tipo de aplicação, pelo contrario, ele é aberto para assim ser empregue com qualquer tipo de aplicação, onde o cliente e servidor desejem trocar dados. Para isto o TLS se vale da criptografia simétrica, criptografia assimétrica e do cálculo de um código de autenticação da mensagem (MAC).

Entretanto, podemos assumir que o protocolo SET tem se mostrado como um forte candidato a padrão de comunicação em comércio eletrônico apesar de haver ainda muitas ciríticas sobre as várias entidades envolvidas.

Avaliação

1. O que são protocolos de segurança web?
2. Qual o protocolo da é web é considerado o mais frágil em termos de segurança?
3. Qual o protocolo da web responsável pelo encaminhamento de ficheiros e documentos entre computadores na Web?
4. Indique as principais diferenças entre os protocolos HTTPS e IPSec.

Actividade 3: Rede Privada Virtual (VPN)

Introdução

Nos últimos tempos das redes de computadores no mundo das redes informáticas tem usado muito o termo privado ou publico. O conceito VPNs tem sido muito abordado e utilizado, razão pela qual passou a ser uma das tecnologias mais usadas nos dias de hoje.

Nesta lição iremos abordar o VPNs, sua tecnologia, protocolos utilizados; tipos de VPNs e seu desenvolvimento.

Detalhes da atividade

Rede Privada Virtual ou Virtual Private Network (VPN) é a implementação de uma rede de comunicação privada sobre uma rede pública, como a Internet. De forma geral, os dados são transmitidos pela rede pública utilizando protocolos padrão e a comunicação se dá através de túneis (com ou sem criptografia) entre pontos autorizados, fornecendo assim a confidencialidade e segurança necessárias.

Por definição, Virtual Private Network (VPN) é uma rede de comunicações privada construída sobre uma rede de comunicações pública. Esta implementação pode ser feita com ajudas de softwares., nomeadamente: SoftEther; OpenVPN; Cisco VPN; UltraVPN; CyberGhost; Hamachi; Loki VPN Client; WinGate VPN entre outros.

Como a Internet é uma rede pública, é preciso criar alguns mecanismos de segurança para que as informações trocadas entre os computadores de uma VPN não possam ser lidas por outras pessoas. A proteção mais utilizada é a criptografia, pois essa garante que os dados transmitidos por um dos computadores da rede sejam os mesmo que as demais máquinas irão receber. Depois de criptografados, os dados são então encapsulados e transmitidos pela Internet, utilizando o protocolo de tunelamento.

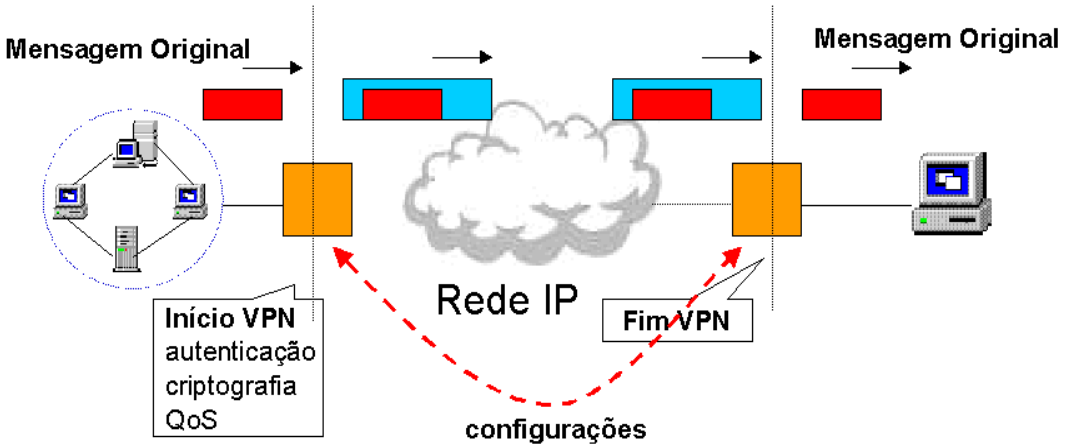

Fig. 8: Modelo de uma VPN

Fonte: http://www.gta.ufrj.br/seminarios/semin2002_1/Ivana

Tipos de VPN's

Exixtem baicamente 3 tipos de VPN's, a seguir apresentados:

VPN de acesso: Oferece um acesso remoto à rede intranet ou extranet em cima de uma infra-estrutura que compartilha as mesmas políticas da rede privada. Por intermédio da VPN o usuário ganha um meio de acesso seguro aos recursos corporativos onde quer que esteja e quando necessário.

VPN para Intranet: As ligações interligam e integram a rede da sede, os escritórios remotos e as filiais em cima de uma infra-estrutura compartilhada. Os negócios utilizam a mesma política da rede privativa assim como segurança, qualidade de serviço, gerenciamento e confiabilidade.

VPN para Extranet: Realiza perfis de interação por meio da rede Internet com uma infra-estrutura compartinhada que usa conexões dedicadas: cadeias entre clientes e fornecedores, empresas e sócios, comunidades de interesse comum.

Tunelamento

As redes virtuais privadas baseiam-se no protocolo de tunelamento. O uso do tunelamento nas VPNs incorpora um novo componente a esta técnica, antes de encapsular o pacote, ele é criptografado. Esse protocolo de tunelamento encapsula o pacote com um cabeçalho adicional que contém as informações de roteamento.

O chamado túnel é o caminho lógico percorrido pelo pacote ao longo da rede intermediária.

Contudo, o processo de tunelamento envolve encapsulamento, transmissão ao longo da rede intermediária e desencapsulamento do pacote. O transporte da informação é feitos cmo ajuda dos seguintes protocolos de comunicação:

- IPSec – Internet Protocol Security
- L2TP – Layer 2 Tunneling Protocol
- L2f - Layer 2 Forwarding
- PPTP – Point-to-Pont Tunneling Protocol

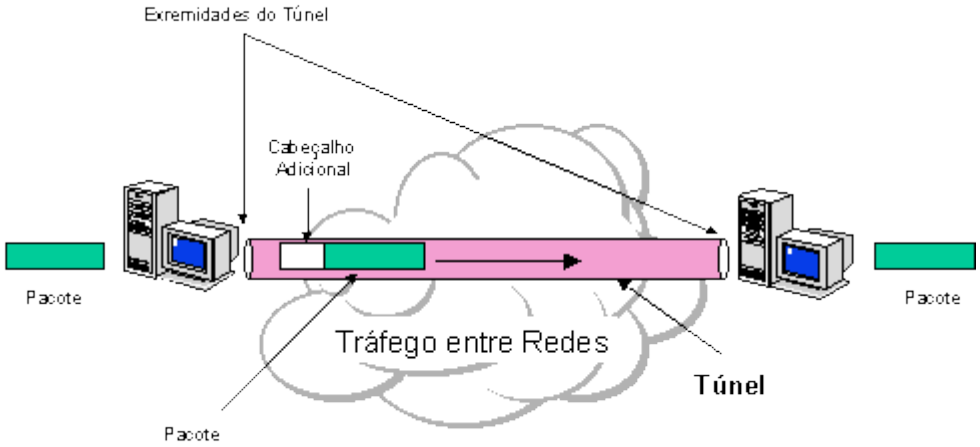

Fig. 9: Exemplo de transporte de um pacote por tunelamento

Os túneis podem ser criados de duas maneiras diferentes, voluntariamente ou compulsoriamente.

Tunelamento voluntário

O cliente emite uma solicitação VPN para configurar e criar um túnel voluntário. Neste caso, o computador do usuário funciona como uma das extremidades do túnel e, também, como cliente do túnel.

Tunelamento compulsório

Um servidor de acesso discado VPN configura e cria um túnel compulsório. Neste caso, o computador do cliente não funciona como extremidade do túnel. Outro dispositivo, o servidor de acesso remoto, localizado entre o computador do usuário e o servidor do túnel, funciona como uma das extremidades e atua como o cliente do túnel.

Conclusão

Nesta actividade abordamos o conceito Virtual Private Network (VPN), temo que passou a ser muito conhecidos na actualidade polos administradores de redes coorporativas. A segurança em uma rede VPN é um fator importantíssimo que deve ser tratado com muita atenção pois os dados estão passando em um meio público. Dentre as principais ferramentas de segurança que temos nas VPN's apontamos o Firewall, Criptografia, Certificados digitais, RADIUS e o protocolo IPSec.

Por fim vimos os Tunelamentos, mecanismo de funcionamento de Redes Virtuais Privadas (VPN).

Avaliação

1. O que é uma VPN?
2. Quais as principais tipos de VPN?
3. O que é tunelamento?
4. Quais são os principais tipos de VPNs através da Camada de Rede?

Resumo da Unidade

Chegamos ao fim desta unidade, onde abordadmos os serviços da as principais formas ameaças da Wed e mecanismos de prevenis estas ameaças através de mecanismos de segurança na Web.

Na segunda actividade, vimos o Protocolo SSL, doravante Protocolo TLS, oferece uma camada de segurança para duas aplicações comunicantes (cliente e servidor). O interessante deste protocolo e que não é restrito a um único tipo de aplicação, pelo contrário, ele é aberto para assim ser empregue com qualquer tipo de aplicação, onde o cliente e servidor desejem trocar dados. Para isto o TLS se vale da criptografia simétrica, criptografia assimétrica e do cálculo de um código de autenticação da mensagem (MAC).

Na ultima actividade da unidade abordamos o conceito Virtual Private Network (VPN), no qual discutimos a segurança em uma rede VPN, o seu mecanismo de funcionamentos por Tunelamentos, onde abordamos as principais ferramentas de segurança nas VPN's, como o Firewall, Criptografia, Certificados digitais, RADIUS e o protocolo IPSec.

Avaliação da Unidade

Agora verifique a sua aprendizagem resolvendo os seguintes exercícios:

Instruções

1. Em caso de duvidas sobre algumas das questões leia novamente as lições que abordam o conteúdo em duvida.
2. Defina o Conceito de Segurança no âmbito de IT?
3. Cite os dois modos de funcionamento do IPSec
4. Mencione alguns softwares de VPN .
5. Cite uma vantagem e uma desvantagem da utilização de uma VPN.

Respostas às questões colocadas nas actividades

Respostas a actividade 1

1. Um serviço Web é uma solução utilizada na integração de sistemas e na comunicação entre aplicações diferentes.
2. As principais formas de ameaças da web são: Integridade, Confidencialidade, Negação de Serviço e Autenticação.
3. Os espectos importantes a ter em conta na segurança do servidor web são: Configurações básicas mal feitas; Estrutura de Diretórios de Rais e publico; configuração do Server-Side Include; Autenticação dos nomes; CGI Scripts.

Respostas a actividade 2

1. Protocolos de segurança web são meanismos de comunicação abstrato ou concreto que realiza uma função de segurança e aplicação de métodos de criptografia.
2. O protocolo da web é considerado o mais frágil em segurança é HTPP.
3. O protocolo da web responsável pelo encaminhamento de ficheiros e documentos é FTP.

Respostas a actividade 3

1. Uma VPN (Rede Privada Virtual) é a implementação de uma rede de comunicação privada sobre uma rede pública, como a Internet.
2. Os principais tipos de VPN são: VPN de acesso, VPN para Intranet, VPN para Extranet.

3. O tunelamento é uma técnica que consiste no encapsulamento de um protocolo dentro de outro.
4. Os principais protocolos da VPN são: PPTP, L2TP e IPSec.

Respostas a Avaliação da Unidade

A segurança é o processo de proteger a informação do mau uso, tanto acidental quanto intencional por pessoas internas ou externas a organização, incluindo empregados, consultores e hackers.

O IPSec funciona de dos modos:

Modo de transporte e modo de tunelamento. No primeiro, apenas a mensagem é criptografada e ocabeçalho IP não é modificado.

Já no segundo, opacote IP é criptografado por inteiro, e assim énecessário encapsular um novo pacote IP paradistribuí-lo.

SoftEther; OpenVPN; Cisco VPN; UltraVPN

Uma vantagem é o baixo custo de uma VPN, já que ela funciona através de uma rede pública. Uma desvantagem é a falta de controle sobre a qualidade do serviço desta rede pública, já que é difícil garantir velocidade, alocação debanda, entre outros aspectos.

Leituras e outros Recursos

As leituras e outros recursos desta unidade encontram-se na lista de Leituras e Outros Recursos do curso.

- A.D. Rubin, D. Geer, and M.J. Ranum, Web Security Sourcebook, John Wiley & Sons, New York, 1997.
- A.D. Rubin, D. Geer, A Survey of Web Security, Computer, September 1998, pp 34-41.
- B. Laurie and P. Laurie, Apache: The Definite Guide, 2nd Edition, O'Reilly, 1999.
- http://www.gta.ufrj.br/grad/04_1/vpn/Script/RDIIntroducao.html
- Scott, Charlie; Wolfe, Paul; Erwin, Mike.Virtual Private Networks, Second Edition. O'Reilly, 1999
- Brian Browne, "Best Practices For VPNImplementation," Business Communication Review, March2001.
- Hanks, S., Editor, "Generic RoutingEncapsulation over IPv4", RFC 1702, October 1994.

Sede da Universidade Virtual africana

The African Virtual University
Headquarters

Cape Office Park

Ring Road Kilimani

PO Box 25405-00603

Nairobi, Kenya

Tel: +254 20 25283333

contact@avu.org

oer@avu.org

Escritório Regional da Universidade Virtual Africana em Dakar

Université Virtuelle Africaine

Bureau Régional de l'Afrique de l'Ouest

Sicap Liberté VI Extension

Villa No.8 VDN

B.P. 50609 Dakar, Sénégal

Tel: +221 338670324

bureauregional@avu.org