

Gestão do Conhecimento durante o Processo de Desenvolvimento de Software

Eduardo da Cunha Kaminski¹, André Peres²

¹ Acadêmico do Curso de Sistemas de Informação da ULBRA Guaíba
edukaminski@gmail.com

² Professor Orientador do Curso de Sistemas de Informação da ULBRA Guaíba
peres@guaiba.ulbra.tche.br

Resumo: O artigo propõe estudo e análise de segmentar uma rede sem fio (Wireless) através de diversas redes virtuais (VLAN – Virtual Local Area Network). Desta forma será possível incrementar segurança através de grupos de usuários, onde os grupos de usuários estarão subdivididos em segmentos e terão a sua política de segurança pré-definida. Divisão lógica do segmento sem fio irá permitir que o grupo de usuários que acessam dados financeiros e/ou estratégicos não utilize o mesmo segmento lógico dos demais grupos, isto irá possibilitar aos administradores de rede controle através de grupos de usuários.

1 - INTRODUÇÃO

A tecnologia denominada rede sem fio - WLAN (*Wireless Local Network Access*), padronizada através do órgão IEEE (*Institute of Electrical and Electronics Engineers*) que estabelece a norma IEEE 802.11 para o desenvolvimento e operação das redes sem fio, está revolucionando o universo da computação. Muitos usuários e empresas estão se beneficiando da mobilidade e a flexibilidade de acessar recursos compartilhados tais como arquivos, impressoras, internet, etc. sem a necessidade de cabos. Entretanto a segurança e o gerenciamento necessitam estar paralelamente ligadas aos benefícios que esta tecnologia oferece.

Com a crescente propagação de redes sem fio nas instituições cria-se a necessidade de incrementar o nível de gerenciamento, um dos desafios é garantir a segurança. Preocupações que profissionais de TI deveriam ter ao implementar uma rede sem fio, nem sempre estão sendo considerada, é necessário analisar os riscos e considerar que as informações poderão estar ameaçadas. Dos principais pontos que deveriam ser considerados estão a confiabilidade e autenticidade da informação.

Para garantir a confidencialidade da informação alguns mecanismos podem ser considerados. O WEP (*Wired Equivalent Privacy*) criado em 1999, WPA (*Wi-Fi*

Protected Access) e o WAP2 podem ser utilizados para proteger o canal de comunicação.

Mecanismos que fornecem a autenticidade da informação são utilizados para identificar qual usuário ou equipamento está transmitindo ou acessando determinada informação. Mecanismos como OSA (*Open System Authentication*), SKA (*Shared Key Authentication*) e o protocolo 802.1x fornecem esta proteção.

Embora seja de extrema importância prover em uma rede sem fio a confiabilidade e a autenticidade da informação, é igualmente importante é sua segmentação destas redes. As redes sem fios podem ser vistas como um segmento não confiável, isto devido a não utilização em muitos casos de mecanismos de controle de acesso, desta forma qualquer usuário terá acesso sem controle algum. Segmentar uma rede é subdividi-la em grupos, estes grupos são denominadas sub-redes. A segmentação de redes locais (LAN) é denominada como VLAN (*Virtual Local Area Network*)

2 - REFERENCIAL TEÓRICO

REDES SEM FIO

A transmissão do sinal através de frequência de radio que se difunde pelo ar é controlada pelo padrão 802.11 que estabelece as normas para criação e para o uso de redes sem fio. Após aproximadamente sete anos de pesquisa o padrão 802.11 foi ratificado em 1997. Por utilizar frequência de radio a IEEE definiu o intervalo entre 2,4GHz e 2,485Ghz com velocidades de 1 Mbps e 2 Mbps.

O padrão 802.11b foi ratificado em 1999. Sua velocidade de transmissão pode chegar a 11 Mbps, também opera nas velocidades de 1 Mbps, 2 Mbps e 5,5 Mbps, cobre uma área de até 400 metros em um ambiente aberto e pode chegar até 50 metros em lugares fechados, quando maior a distancia menor a velocidade de transmissão.

A conclusão do desenvolvimento do padrão 802.11a ocorreu no final de 1999, o padrão 802.11b foi concluído alguns meses antes. O 802.11a opera nas seguintes velocidades: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps e 54 Mbps tendo uma alcance de até 50 metros. Utiliza a frequência de radio de 5 GHz, que tem algumas restrições quanto a sua operação em alguns países.

Operando em velocidade de até 54 Mbps o padrão 802.11g foi ratificado em 2003. Utiliza frequência de rádio de 2,4 GHz compatível com o padrão 802.11b, ou seja, um equipamento com padrão 802.11b pode trocar informações com outro equipamento com padrão 802.11g, limitando apenas a velocidade máxima de 11 Mbps do padrão 802.11b.

TOPOLOGIA DAS REDES SEM FIO (IBSS, BSS E ESS)

As redes IBSS (*Independent Basic Service Set*) são definidas através das conexões ponto-a-ponto, ou seja, equipamentos trocam informações diretamente entre-si sem a necessidade de um dispositivo que centralise o acesso. Por ser uma conexão ponto-a-ponto esta tecnologia também se refere a topologia AD-HOC

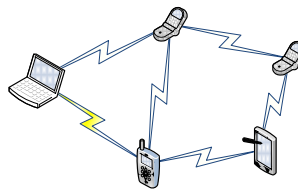


Figura 1: Topologia AD-HOC

Uma rede BSS é definida pela utilização de ponto de acesso para intercomunicação dos dispositivos móveis. O ponto de acesso tem a função criar uma rede sem fio, para identificação de uma rede um SSID (*Service Set Identifier*) é atribuído ao ponto de acesso. Desta forma os dispositivos móveis irão criar um canal chamado BSS. Apenas após a criação do canal BSS um computador pode trocar informações através desta rede.

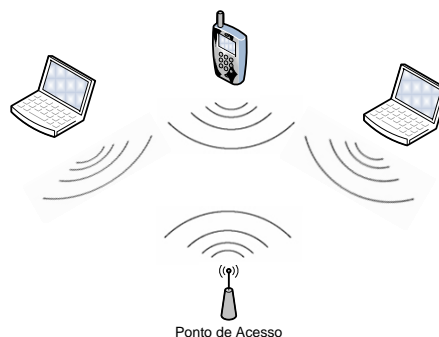


Figura 2: Basic Service Set

Redes BSS fornecem suporte para pequenas localidades como escritórios, pequenas empresas e casas. Estas redes não tem capacidade de fornecer uma cobertura para grandes área, para isto o 802.11 permite que haja ligação entre

diversos BBS através da core (espinha dorçal) destas grandes redes assim criando uma rede ESS.

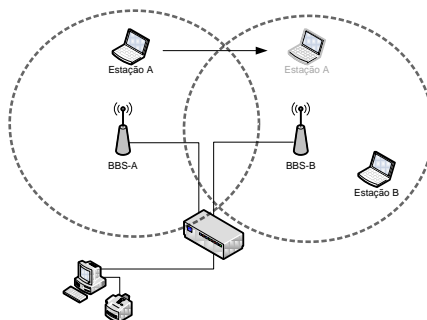


Figura 4 – A união duas BSS cria uma ESS

A figura 4 ilustra esta topologia a ligação de duas redes BBS, a rede A criando o BBS-A e do rede B criando o BBS-B. Esta ligação ocorre através de cabo ligados à um hub ou switch, criando uma ligação física e lógica entre as redes A e B. Desta forma os usuários podem compartilhar dados independente da rede em que estejam conectados, como por exemplo a estação B compartilhando arquivos e um computador ligado a rede ethernet compartilhando uma impressora.

CONFIDENCIALIDADE DA INFORMAÇÃO (WEP, WPA E WPA2)

O primeiro protocolo de segurança para rede sem fio, o WEP (*Wired Equivalent Privacy*) é parte do padrão IEEE 802.11 e foi introduzido para agregar confiabilidade na informação trocada durante a comunicação entre os dispositivos sem fio e é suportado por todos os equipamentos 802.1a/b/g.

O WEP usa uma chave compartilhada entre os dispositivos de rede, ponto de acesso e clientes. A chave compartilhada é estática podendo ter 40 bits, 64 bits ou 128 bits, desta forma a chave é utilizada para codificar e para decifrar os dados. Somente terá acesso ao meio de comunicação sem fio aquele dispositivo que conter a chave compartilhada.

O desenvolvimento do WEP considerou apenas as medidas necessárias para proteger uma rede sem fio considerando as necessidades de uma rede local onde os dispositivos de rede estão interligados por cabos. Assim com a evolução e disseminação da tecnologia sem fio, o protocolo WEP acabou apresentando falhas e se tornando vulnerável a ataques.

WEP é vulnerável por causa do tamanho limitado das chaves e por serem estáticas. A natureza estática das chaves compartilhadas torna sério o problema da troca das chaves das estações. Como consequência, muitos administradores de redes utilizam a mesma chave por semanas, meses e até anos. Criando oportunidades para que um invasor utilize ferramentas para descobrir a chave WEP em uso em uma rede e assim poder ter acesso à rede. Mesmo com as falhas e vulnerabilidades, conter segurança mesmo que limitada é melhor do que não ter.

Diante dos problemas apresentados pelo WEP, em 2003 foi disponibilizada outra solução o WPA (*Wi-Fi Protected Access*) que inclui mecanismos de protocolo de integridade de chave temporal chamado de TKIP (*Temporal Key Integrity Protocol*), as mesmas podem ser alteradas rapidamente com o passar do tempo, reduzindo a possibilidade de uma sessão ser quebrada.

Em junho de 2004, o IEEE ratificou o padrão 802.11i também conhecido como WPA2, que suporta o padrão de criptografia avançada AES (*Advanced Encryption Standard*) e características de gerenciamento de chaves com diversos tamanhos 128, 192 e 256 bits.

O WPA, assim como o WPA2, provê um esquema de criptografia significativamente mais forte e pode usar diversos métodos como uma chave privada compartilhada, chaves únicas designadas para cada usuário ou mesmo certificados SSL para autenticar tanto o cliente como o ponto de acesso. As credenciais de autenticação são verificadas com o uso do protocolo 802.1X, que será citado no item 3.2.4 deste trabalho. O WPA também pode ser usado no modo PSK (*Pre-Shared Key*). Nesse modo, há a presença de uma chave pré-determinada e a troca da chave é realizada pelo próprio ponto de acesso.

Entretanto o WPA requer pontos de acesso com hardware relativamente recente e o firmware atualizado em todos os dispositivos sem fio.

AUTENTICIDADE DA INFORMAÇÃO (OSA E SKA)

O padrão IEEE 802.11 define dois métodos que os dispositivos sem fio se autenticam antes da comunicação iniciar. Estes dois métodos são: Autenticação de Sistema Aberto (OSA – *Open System Authentication*) e Autenticação de Chave Compartilhada (SKA – *Shared-Key Authentication*).

O método OSA não necessita que o dispositivo sem fio envie ao ponto de acesso uma chave para ter acesso à rede sem fio. Quando o dispositivo solicitar acesso à rede é enviado um pedido de autenticação para o ponto de acesso mais próximo. O pedido de autenticação contém o tipo de autenticação que pretende utilizar (zero no caso de OSA). O ponto de acesso responde a solicitação de autenticação não requerendo nenhum tipo de desafio para conceder o acesso, assim, o dispositivo se conecta a rede.

Neste caso as redes sem fio usando OSA transmitem tudo em texto claro onde nenhuma criptografia é necessária. Neste tipo de autenticação, os dispositivos sem fio só precisam identificar o SSID da rede para ter acesso autorizado. É possível limitar em alguns produtos o acesso através do endereço MAC do dispositivo de acesso. Isso é considerado OSA.

Assim, um intruso pode capturar o tráfego, captura as medidas necessárias para autenticação, e percorrer os mesmos passos até ser autenticado e associado a um ponto de acesso.

SKA é autenticação de chave compartilhada (SKA) significa que alguma forma de autenticação ocorre antes de comunicações de rede sem fim iniciar, ou seja, o dispositivo sem fio deve ser configurado com a chave de criptografia necessário para que o ponto de acesso reconheça a autenticação e conceda acesso.

É importante notar que o ponto de acesso pode impor o uso de autenticação. Se um dispositivo de acesso envia um pedido de autenticação informando que o método que será utilizado é o OSA, o ponto de acesso pode negar o acesso à rede, isso se o ponto de acesso estiver configurado para aplicar o método SKA.

Quando um dispositivo solicita acesso à rede, ele deve enviar uma solicitação de autenticação para o ponto de acesso, que contém o tipo de autenticação que deseja utilizar (um no caso de SKA). Ao receber este pedido, o ponto de acesso envia uma resposta de autenticação para o dispositivo. Esta resposta contém um desafio texto. Quando a dispositivo recebe o desafio, ele criptografa o aleatoriamente usando WEP e gerar uma resposta ao desafio. Ao receber a resposta, o ponto de acesso desifra a resposta usando as chaves pré-compartilhadas. O ponto de acesso compara a mensagem decifrada com o desafio que enviou para o dispositivo. Se estas são as mesmas, o ponto de acesso conclui que o dispositivo que pretendam aderir à rede é uma do dispositivo que não conhece

a chave secreta e, portanto, o ponto de acesso autentica o dispositivo para se conectar a rede.

PADRÃO 802.1X

A fim de oferecer um mecanismo de autenticação mais eficiente o padrão 802.1x foi definido. A autenticação por 802.1x, utilizada em rede com fio (802.3) e redes sem fio (802.11), impede que usuários e computadores não autenticados e não autorizados se conectem a rede. Este padrão fornece controle de acesso a redes de computadores baseado em portas (baseada em "porta" significa que a rede terá um único ponto de autenticação).

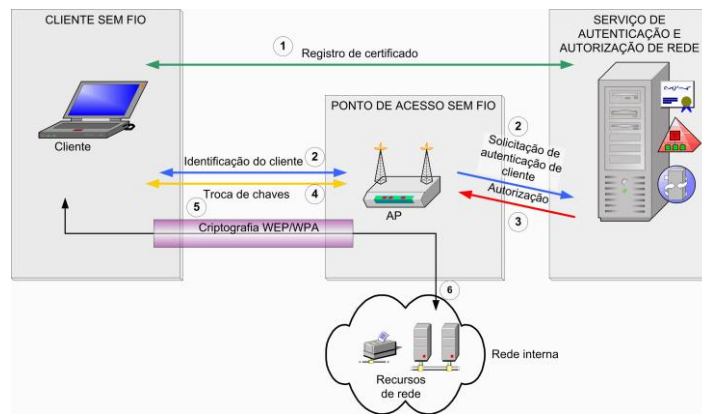


Figura 5: Processo de acesso à rede 802.1x

Os números da figura ilustram o processo de acesso à rede, descrito com mais detalhes nas etapas a seguir:

- 1) Antes de iniciar a comunicação na rede sem fio, o dispositivo móvel deve ter as suas credenciais de autenticação, para isso será necessário realizar uma pré-configuração e criação dos dados do usuário para acesso ao meio sem fio.
- 2) Quando o dispositivo movel estiver no perimetro do ponto de acesso, ele tenta estabelecer uma conexão. O cliente detecta o SSID da rede sem fio e usa-o para determinar as configurações corretas e o tipo de credencial que será utilizado.
- 3) O servidor RADIUS valida às credenciais do cliente comparando com a sua base de dados. Se o cliente for autenticado com êxito, o servidor RADIUS coleta as informações necessárias para decidir sobre a autorização ou não do cliente para acessar a rede sem fio. Ele usa informações de sua base de dados e restrições

definidas nas políticas de acesso para conceder ou negar o acesso ao cliente. Em seguida, o servidor RADIUS retransmite ao ponto de acesso a decisão.

- 4) Se o acesso for concedido ao cliente, o servidor RADIUS transmite a chave mestra do cliente ao ponto de acesso. O cliente e o ponto de acesso passam então a compartilhar as mesmas informações de chave comum, que podem ser usadas para criptografar e descriptografar o tráfego da rede sem fio entre eles.
- 5) O ponto de acesso estabelece a conexão sem fio do cliente à rede interna, permitindo que o cliente tenha acesso irrestrito aos sistemas na rede interna. Dessa forma, o tráfego entre o cliente e o ponto de acesso agora é criptografado.
- 6) Se o cliente requer um endereço IP, agora ele pode solicitar uma concessão DHCP (*Dynamic Host Configuration Protocol*) de um servidor na rede. Uma vez atribuído o endereço IP, o cliente pode iniciar a troca de informações normalmente com os sistemas no restante da rede.

(VLAN) REDES LOCAIS VIRTUAIS

Redes locais virtuais conhecidas pela sigla VLAN (*Virtual Local Access Network*) é a segmentação de redes locais. A segmentação de uma rede é subdividir uma rede local em dois ou mais grupos, estes grupos estarão utilizando o mesmo meio físico para transmissão dos dados, entretanto logicamente estarão separadas.

Em uma rede de computador quando uma máquina inicia a transmissão todas as outras não devem gerar ruído na rede. Mesmo que apenas dois computadores estejam trocando informações, todos os outros não devem emitir qualquer sinal na rede, caso haja, será considerada uma colisão e a transmissão será iniciada novamente.

VLAN podem agregar segurança quando um grupo de computadores e/ou usuários necessita ter um nível maior de segurança, desta forma estes usuários podem ter mecanismos de segurança para cada VLAN.

Uma rede sem fio pode ser segmentada assim como as redes com fio, utilizando a tecnologia VLAN. Entretanto a segmentação em uma rede sem fio é definida pelo nome que identifica a rede (SSID), assim cada SSID irá identificar uma sub-rede da VLAN. Esta funcionalidade é restrita ao modelo do ponto de acesso, não está disponível em todos os modelos.

3 - CONCLUSÃO

A proposta é fazer uma pesquisa e análise das tecnologias citadas acima, criando redes virtuais para distintos grupos de usuários, aumentando a segurança e gerenciamento no acesso às informações e na confiabilidade da informação obtida e enviada.

Os estudos das tecnologias irão dar o andamento do trabalho de acordo com sua possível integração, caso haja necessidade de desenvolvimento de algum conector que auxilia no processo de integração este será avaliado para uma possível criação na sua segunda etapa. Toda a delimitação do tema e desenvolvimento está sendo exposta na primeira etapa deste trabalho, e a sua seqüência será a sua possível o experimentos a fim de validar a segurança e gerenciamento acima proposto.

4 - PRÓXIMOS PASSOS

As próximas etapas para conclusão do trabalho:

- Finalizar a pesquisa sobre aplicação do padrão 802.1x;
- Definir quais softwares e equipamentos irão ser utilizados no experimento;
- Definir o cenário de testes:
 - Definição das redes virtuais;
 - Definição dos grupos de acesso;
 - Definição das políticas de segurança;
 - Esboço e cronograma do experimento;

5 - BIBLIOGRAFIA

Geier, Jim; Wireless-Nets, Ltd. **Implementing 802.1X Security Solutions for Wired and Wireless Networks Networks**. Publicado por Wiley Publishing, Inc. Indianapolis, Indiana, publicado simultaneamente no Canada, 2008

Harold F. Tipton; **Krause**, Micki. **Information Security Management Handbook**, Sixth Edition, Purchase Hardcopy, Auerbach Publications 2007

Hideki Imai; Mohammad Ghulam Rahman; Kazukuni Kobar., Wireless Communications Security. Artech House 2006

David D. Coleman; David A. CWNA: Certified Wireless Network Administrator Study Guide (Exam PW0-100). Westcott. Sybex. 2006

Harris, Shon. CISSP: All-in-One Exam Guide, Fourth Edition, McGraw-Hill/Osborne. 2008

Harris, Shon. CISSP Certification Passport. McGraw-Hill/Osborne. 2002

Chandra, Praphul. Wireless Networking: Know It All. Newnes. 2008

Joseph Davies. Deploying Secure 802.11 Wireless Networks with Microsoft Windows, Microsoft Press. 2004.

Moraz Eduardo. Treinamento Profissional Anti-Hacker. São Paulo: Digerati books. 2006

Stewart, James Michael. Tittel, Ed. Chapple, Mike. CISSP: Certified Information Systems Security Professional Study Guide, Fourth Edition. Sybex. 2008

Davies, Joseph. Northrup, Tony. Windows Server 2008 Networking and Network Access Protection (NAP). Microsoft Press. 2008

McGraw-Hill. CWNA Certified Wireless Network Administrator Official Study Guide: Exam PW0-100, Third Edition. Osborne. Planet3 Wireless. 2005