Uma análise dos mecanismos de segurança de redes locais sem fio e uma proposta de melhoria

Gilson Marques Silva, João Nunes Souza

Faculdade de Computação – Universidade Federal de Uberlândia (UFU)
38.400-902 – Uberlândia – MG – Brasil

gilsonm@ctbctelecom.net.br, nunes@ufu.br

Abstract. *This paper presents the security mechanisms implemented in the wireless local area networks, identify the vulnerabilities associated with them, and propose a set of improvements which possibility rising the security level of the wireless local area networks.*

Resumo. *Este artigo apresenta os mecanismos de segurança implementados em redes locais sem fio, identifica as falhas associadas aos mesmos, e propõe melhorias que possibilitam a elevação do nível de segurança de redes locais sem fio.*

1. Introdução

As redes locais sem fio têm se tornado, cada vez mais, uma opção para ambientes corporativos; e com isso, os requisitos de segurança são cada vez mais importantes, haja vista que acessos indevidos à rede e a leitura ou alteração de dados em trânsito na mesma representam uma grande ameaça a estes ambientes.

O padrão IEEE 802.11 [IEEE Std 802.11-1999], responsável pela padronização das redes locais sem fio, agrega alguns mecanismos de segurança, como por exemplo o protocolo WEP (*Wired Equivalent Privacy*). Além disso, o padrão IEEE 802.1X [IEEE Std 802.1X-2001] também agrega mecanismos de segurança, não somente às redes locais sem fio, mas a todo o conjunto IEEE 802. No entanto, estes mecanismos e também os mecanismos agregados pelos fabricantes não são considerados eficazes face aos requisitos atuais de segurança.

A seção 2 apresenta uma visão geral do padrão IEEE 802.11. Os mecanismos de segurança do padrão 802.11, aqueles inseridos pelos fabricantes e também os mecanismos de segurança do padrão 802.1X, são apresentados nas seções 3,4 e 5 respectivamente. Cada uma destas seções apresenta também as fragilidades identificadas nestes mecanismos. As fragilidades de administração são apresentadas na seção 6. E finalmente a seção 7 apresenta uma proposta para elevar o nível de segurança de redes locais sem fio, observando todas as fragilidades identificadas nas seções anteriores. Logo esta proposta eleva o nível de segurança de redes locais sem fio.

2. Uma visão geral do padrão 802.11

O padrão IEEE 802.11 é um padrão para as redes locais sem fio em todos seus aspectos incluindo mecanismos de controle de acesso, confidencialidade e integridade, os quais serão detalhados e analisados neste artigo.

O padrão define três fases pelas quais qualquer cliente deve passar com sucesso, antes de obter acesso a rede sem fio. A figura 1 descreve estas 3 fases. Ela apresenta um esquema da conexão à rede local sem fio, incluindo a fase de sondagem, autenticação e associação. Cada seta para a direita representa a transmissão dos dados nela nomeados do cliente para o ponto de acesso, e cada seta para a esquerda representa uma transmissão dos dados nela nomeados do ponto de acesso para o cliente. Neste caso o padrão IEEE 802.11 é utilizado com o algoritmo SKA (*Shared Key Authentication*) e dois mecanismos adicionais: o SSID (*Service Set Identifier*) e a filtragem de endereços MAC. Estes mecanismos são detalhados nas seções 3 e 4.

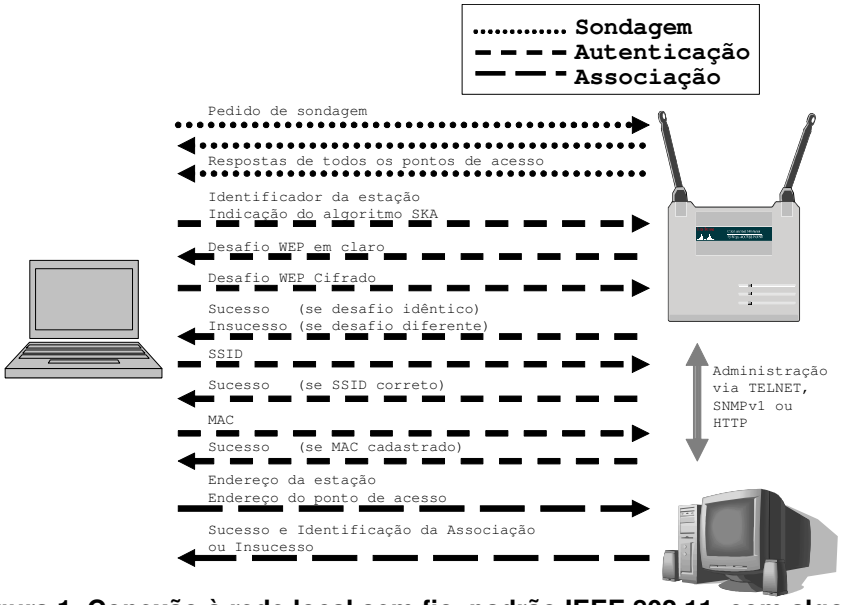

Figura 1. Conexão à rede local sem fio, padrão IEEE 802.11, com algoritmo SKA, e dois mecanismos adicionais: SSID e filtragem MAC

As fases de conexão são:

Fase de Sondagem – O cliente envia requisições de acesso em todos os canais e todos os pontos de acesso que estiverem na área de cobertura responderão com informações que poderão ser utilizadas na fase de associação. Esta fase é indicada na figura 1 pelas três primeiras linhas.

Fase de Autenticação – Existem dois tipos de autenticação definidos no padrão; *Open Systems Authentication* (OSA) e *Shared Key Authentication* (SKA). A configuração do ponto de acesso e a indicação do cliente, definirão qual esquema será utilizado. Estes dois protocolos serão detalhados na seção 3. Esta fase é indicada na figura 1 pelas linhas de ordem quatro a onze.

Fase de Associação – O cliente, agora autenticado e de posse das informações recebidas na fase de sondagem, envia uma requisição de associação para o ponto de acesso escolhido. O ponto de acesso retornará uma resposta contendo o identificador da associação que poderá ser utilizado para pedidos de reassociação ou desassociação. Esta fase é indicada na figura 1 pelas duas últimas linhas.

O padrão IEEE 802.11 utiliza o protocolo WEP para garantir a confidencialidade e integridade dos dados no ar. No entanto o WEP, baseado no protocolo *stream cipher* RC4, é considerado vulnerável, pois apresenta falhas no algoritmo de KSA (*Key*

Scheduling Algorithm), que trata a questão de reuso de *key-stream*. Estudos sobre as fraquezas do protocolo WEP são apresentados em [Arbaugh e Shankar 2001] e [Roshan 2002].

3. Mecanismos de segurança do IEEE 802.11 e as fragilidades identificadas

O padrão IEEE 802.11 considera o controle de acesso à rede, a confidencialidade e integridade dos dados. Ele propõe um modelo de acesso baseado nas três fases apresentadas na seção 2. Como os mecanismos de segurança estão implementados na fase de autenticação, este artigo analisa esta fase em detalhes. O padrão permite dois tipos de autenticação:

OSA (*Open System Authentication*), onde toda negociação é feita em texto plano, e nenhuma condição é imposta, ou seja, todos clientes que solicitam a autenticação serão autenticados. Basicamente é uma autenticação nula.

SKA (*Shared Key Authentication*), no qual o protocolo WEP é utilizado. Neste tipo de autenticação o ponto de acesso envia um desafio em texto plano para o cliente. O cliente deve cifrar o desafio com o protocolo WEP, utilizando uma chave de sessão pré compartilhada, e depois deve enviá-la novamente ao ponto de acesso, que verificará se a resposta ao seu desafio está correta. Estes passos estão ilustrados nas quatro primeiras linhas da fase de autenticação da figura 1.

O padrão IEEE 802.11 utiliza o atributo SSID como um identificador para a rede. Entretanto ele é transmitido, periodicamente, por *broadcast*, em texto plano, o que permite que qualquer cliente o capture, através da escuta em modo simples na rede sem fio e o use quando necessário. Assim sendo o SSID não é considerado um mecanismo eficaz de segurança quando implementado desta forma.

Como na fase de sondagem os pontos de acesso respondem a qualquer solicitação de informação, a tarefa de mapear a rede fica simples e direta, pois qualquer cliente pode obter informações a partir da solicitação direta aos pontos de acesso. Além disso, como o SSID é enviado em texto plano e por *broadcast*, sua leitura também torna-se direta.

São apresentadas a seguir algumas conclusões sobre a efetividade destes mecanismos de segurança, identificadas neste artigo.

No algoritmo OSA não existe qualquer tipo de controle de acesso. Logo considerar as fragilidades deste esquema não faz sentido. Neste cenário a rede é considerada como pública, pois oferece acesso a qualquer cliente que esteja em sua área de cobertura.

No entanto, quando o algoritmo SKA é utilizado, existe uma validação por desafio/resposta utilizando o protocolo WEP. Neste caso o desafio é enviado em texto plano e pode ser capturado por qualquer cliente que esteja coletando os pacotes na rede de forma promíscua. A resposta ao desafio, embora cifrada, também pode ser capturada, logo, têm-se acesso ao *key-stream*, ou seja, o primeiro passo para a leitura de dados confidenciais e para a quebra da chave WEP, conforme descrito em [Roshan 2002].

4. Mecanismos de segurança agregados pelos fabricantes e as fragilidades identificadas

Os principais fabricantes de equipamentos para redes locais sem fio, face as necessidades de segurança do mercado estão antecipando aos padrões e agregando novos mecanismos de segurança aos seus equipamentos. Entretanto nem sempre tais mecanismos são eficazes.

O primeiro mecanismo é denominado "rede fechada" onde não se transmite o SSID por *broadcast.* O SSID é utilizado como uma senha simples, necessária no processo de autenticação. Neste caso, o cliente é solicitado a informar o SSID correto como uma das etapas do processo de autenticação.

Quando um cliente legítimo percorre o processo de autenticação, de acordo com a figura 1, ele envia o SSID em texto plano, o que possibilita sua captura e posterior utilização. Desta maneira o SSID não agrega segurança ao sistema.

Outro mecanismo inserido é a filtragem de endereços MAC. Como mais uma etapa no processo de autenticação, o endereço MAC do cliente é verificado contra uma base de endereços MAC autorizados. Esta base pode ser armazenada em cada ponto de acesso ou de forma centralizada, em um servidor RADIUS (*Remote Authentication Dial-In User Service*).

A filtragem MAC não é a solução para os problemas de acesso indevido às redes locais sem fio. Como os endereços MAC podem ser falsificados e alterados com facilidade um invasor pode capturar um endereço MAC cadastrado através da captura de pacotes na rede. Em seguida ele poderá alterar o endereço MAC de seu cartão para o endereço MAC capturado.

5. Mecanismos de segurança do IEEE 802.1X e as fragilidades identificadas

O padrão IEEE 802.1X prevê o controle de acesso por porta para toda a família IEEE 802, e também pode ser utilizado para as redes locais sem fio. Porém existe uma grande diferença entre as redes locais sem fios e as demais redes cabeadas, como *ethernet* ou *token ring.* Nas redes cabeadas a ligação entre o cliente e sua porta de acesso é definida por um cabo fisicamente conectado às duas partes, e no caso das redes locais sem fio, esta ligação é o ar. Desta forma, o padrão falha justamente em não se preocupar com os aspectos de segurança nesta parte da conexão, sendo possível a captura, adulteração e repetição de pacotes de validação. Em [Mishra e Arbaugh 2002] é feita uma análise dos aspectos de segurança do 802.1X exibindo algumas possibilidades de ataques contra o padrão.

O padrão IEEE 802.1X considera um autenticador no processo de autenticação. O ponto de acesso pode tornar-se um repassador de pacotes de autenticação já que toda a base é armazenada no autenticador. O autenticador pode ser definido no próprio ponto de acesso, porém as atuais soluções de mercado não têm optado pela implementação desta funcionalidade nos equipamentos. Pelo contrário, têm deixado esta tarefa a cargo de servidores especializados, como por exemplo, servidores RADIUS.

A validação de usuário e senha através do protocolo RADIUS pode ser utilizada sem mecanismos de cifragem. Neste caso, as credenciais do usuário trafegam entre o

cliente e o ponto de acesso em texto plano, e entre o ponto de acesso e o autenticador, cifrado apenas pela chave do próprio RADIUS. No entanto as credenciais podem ser protegidas desde o cliente até o ponto de acesso, com o auxílio de outros protocolos, por exemplo o MD5 (*Message Digest 5*).

No primeiro caso, como as credenciais são transmitidas em texto plano, elas podem ser facilmente capturadas no ar e oportunamente utilizadas. No segundo caso, também é possível capturar as credenciais protegidas e mesmo sem poder interpretá-las, o invasor pode utilizá-las oportunamente, de modo a fornecer acesso ao sistema, caracterizando um ataque por repetição.

O padrão 802.1X pode ser utilizado para a distribuição automática de chaves de sessão, que serão utilizadas entre o cliente e o ponto de acesso. Esta funcionalidade elimina os riscos associados ao uso de chave pré compartilhada, e diminui os perigos advindos das fragilidades do protocolo WEP. Entretanto, neste caso, o mecanismo de troca de chave de sessão deve estar associado a processos de reautenticação, com geração e distribuição de novas chaves.

Neste contexto se o invasor consegue credenciais válidas para autenticação, ele poderá receber uma chave de sessão sem maiores dificuldades. E ainda se o processo não estiver protegido por outros algoritmos, como o MD5, a chave de sessão poderá ser capturada e utilizada.

6. Administração e gerência dos pontos de acesso e as fragilidades identificadas

O padrão IEEE 802.11 é omisso quanto à administração dos pontos de acesso. Neste caso cada fabricante determina um tipo de acesso e interface em seu equipamento para que este possa ser administrado e gerenciado.

A maioria dos equipamentos disponíveis no mercado são administrados via rede, podendo ser configurados para permitir sua administração pelas interfaces sem fio ou por aquelas conectadas a rede cabeada, quando existentes. Um grande problema é o fato de que, na maioria dos casos, protocolos sem funcionalidades de confidencialidade são utilizados. Exemplos incluem o TELNET, SNMPv1 (*Simple Network Management Protocol version 1*) e HTTP (*HyperText Transfer Protocol*). Nenhum destes protocolos provêm cifragem dos dados, logo propiciam a um invasor a captura do tráfego de administração, de onde pode-se extrair chaves definidas no equipamento, credenciais para administração e gerência dos equipamentos, além de outros detalhes da rede.

7. Proposta de melhoria do nível de segurança das redes locais sem fio

Esta seção apresenta uma proposta para melhorar os mecanismos de segurança das redes locais sem fio. Esta proposta pode ser considerada como uma extensão do padrão IEEE 802.11, já que é compatível com as premissas e protocolos atualmente utilizados. Logo, sua implementação pode ser adotada sem a necessidade de expansão do *hardware* dos atuais equipamentos e desenvolvimento ou agregação de novas funcionalidades, como por exemplo novos algoritmos criptográficos, funções *hash* e outras.

A figura 2 apresenta um esquema da conexão à rede local sem fio, incluindo a fase de sondagem, autenticação e associação. A figura representa a nova proposta e sua interpretação é análoga a da figura 1.

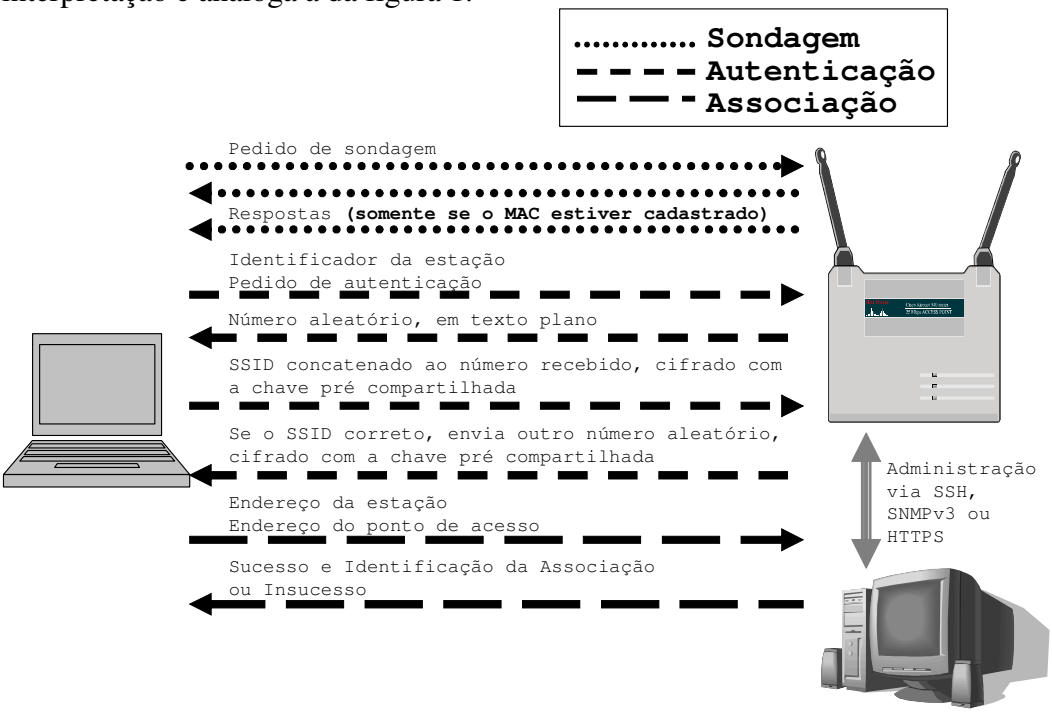

Figura 2. Conexão à rede local sem fio, de acordo com a presente proposta

As alterações propostas elevam o nível de segurança das redes locais sem fio, sob os seguintes aspectos:

7.1. Como dificultar o processo de mapeamento da rede

Esta seção apresenta um mecanismo para dificultar o mapeamento da rede, através da filtragem MAC e uso de um número aleatório.

O mapeamento da rede é dificultado devido a verificação do endereço MAC durante a fase de sondagem. Nesta sondagem o endereço MAC do cliente é verificado contra uma base de endereços MAC cadastrados. Caso o endereço MAC do cliente não esteja cadastrado, o ponto de acesso fica mudo e não transmite resposta alguma.

Mesmo considerando os fatos acima é possível não adotar a filtragem MAC. Em redes grandes e dinâmicas o custo de administração da base de endereços MAC deve ser observado.

O problema da captura e falsificação de um endereço MAC cadastrado continua existindo. No entanto esta medida evita que simples usuários usem o software de seus cartões sem fio para mapear a rede; mas não a torna segura diante de usuários mais experientes e determinados a mapeá-la. Logo este não é um mecaniso eficaz contra a falsificação ou clonagem de endereços MAC.

Esta proposta também previne a captura do SSID. Um número aleatório gerado pelo ponto de acesso é transmitido para o cliente antes que o SSID seja enviado ao ponto de acesso. O cliente, ao receber o número aleatório, concatena o SSID ao número recebido, depois cifra o conjunto utilizando o protocolo WEP com a chave pré

compartilhada e envia o mesmo ao ponto de acesso. O ponto de acesso decifra o conjunto, verifica o SSID e o número recebido. Este processo é ilustrado nas quatro primeiras linhas da fase de autenticação da figura 2.

Nesta solução o SSID não trafega em claro pela rede. E mesmo se capturado pelo invasor, o conjunto não poderá ser utilizado, pois o SSID está concatenado a um número aleatório gerado pelo ponto de acesso. Logo, com a contribuição do número aleatório, o invasor não terá êxito caso capture um conjunto *SSID+número aleatório*, com o intuito de repetí-lo oportunamente, como ocorre nos casos onde somente o SSID é utilizado. Assim inibe-se ataques por repetição nesta fase.

7.2. Como tornar o processo de autenticação mais eficaz e robusto

Esta seção apresenta um mecanismo para tornar o processo de autenticação mais eficaz, através do uso de chaves pré compartilhadas, chaves de sessão e números aleatórios.

Este mecanismo prevê o uso de uma chave pré compartilhada que é utilizada somente no processo de autenticação. Diferente do padrão 802.11 que utiliza a chave pré compartilhada no processo de autenticação e também para prover a confidencialidade dos dados no ar.

A chave pré compartilhada somente é utilizada para autenticar o cliente e distribuir uma chave de sessão. Logo uma quantidade bem menor de tráfego é cifrado com esta chave. Desta forma os ataques citados em [Roshan 2002] contra o protocolo WEP tornam-se inviáveis.

O primeiro número aleatório gerado pelo ponto de acesso é utilizado no processo de autenticação, evitando que partes do tráfego desta fase sejam coletadas e posteriormente utilizadas.

A autenticação pode ser dividida em duas partes. Primeiro ocorre a validação do valor do SSID, que agora pode ser considerado seguro. Segundo ocorre a validação por desafio/resposta. Onde o desafio é o SSID concatenado ao número aleatório gerado e a resposta é este conjunto cifrado com a chave pré compartilhada.

Desta forma passos adicionais são eliminados na fase de autenticação. E a filtragem MAC, definida na fase de sondagem, é considerada como uma pré autenticação.

7.3. Como reduzir os efeitos das fraquezas do protocolo WEP

Esta seção apresenta um mecanismo para reduzir os efeitos das fraquezas do protocolo WEP, através da distribuição e uso de chaves de sessão de forma periódica e dinâmica.

Um processo de distribuição dinâmica de chaves de sessão é adicionado ao final da fase de autenticação para garantir a confidencialidade dos dados trafegados na rede. O processo de quebra da chave WEP consome um determinado tempo que deve ser maior que o período de reautenticação. Este tempo depende da quantidade de tráfego sendo transmitido na rede, quanto mais tráfego, menor o tempo para a quebra. Uma nova chave de sessão é gerada e distribuída a cada reautenticação, que ocorre periodicamente. Neste caso os dados estão protegidos, pois mesmo se a chave WEP for quebrada, a chave revelada não mais estará em uso. O período para a reautenticação

deve ser definido de acordo com a carga da rede, quanto mais tráfego menor o tempo de reautenticação. Alguns parâmetros de carga são considerados em [Mahan 2001].

Este processo de geração e distribuição da chave de sessão é apresentado na última linha da fase de autenticação da figura 2; quando o ponto de acesso transmite um novo número aleatório, protegido pela chave pré compartilhada, que será utilizado como chave de sessão.

7.4. As melhores práticas para administração dos pontos de acesso

Esta seção apresenta as melhores práticas para tornar o processo de administração dos pontos de acesso mais seguro, através do uso de protocolos com recursos que garantem a confidencialidade dos dados. Estas práticas já são adotadas por alguns frabricantes.

Protocolos que oferecem a cifragem dos dados transmitidos deve ser adotados para as comunicações de administração e gerência. Exemplos destes protocolos são o SSH (*Secure Shell*), SNMPv3 (*Simple Network Management Protocol version 3*) e HTTPS (*HyperText Transfer Protocol Secure*).

Desta forma é garantido que o tráfego de administração e gerência dos pontos de acesso não seja utilizado para a obtenção de chaves, credenciais de acesso e nem mesmo sob o aspecto de comprometer a configuração dos pontos de acesso.

8. Trabalhos futuros e conclusão

Esta proposta de melhoria do nível de segurança de redes locais sem fio ainda não está totalmente definida. O autor dará continuidade ao trabalho, especificando em detalhes os números gerados e utilizados na fase de autenticação, detalhando a estrutura de cada um dos pacotes em cada uma das fases incluindo os pacotes do processo de reautenticação e emissão de novas chaves. Além disso o autor pretende agregar novas melhorias elevando ainda mais o nível de segurança destas redes.

Referências

IEEE Std 802.11-1999, “Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications”, Março.

IEEE Std 802.1X-2001, “Port-Based Network Access Control”, Junho.

Arbaugh, W., Wan, Y. e Shankar, N. (2001) “Your 802.11 Wireless Network has No Clothes”, http://www.cs.umd.edu/%7Ewaa/wireless.pdf, Março.

Mahan, R. (2001) “Security in Wireless Network”, http://www.sans.org/rr/wireless/wireless_net3.php, Novembro.

Mishra, A. e Arbaugh, W. (2002) “An Initial Security Analysis of the IEEE 802.1X Standard”, http://www.cs.umd.edu/~waa/1x.pdf, Fevereiro.

Roshan, P. (2002) “802.11 Wireless LAN Security White Paper”, http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml.