Os novos padrões de segurança em redes wireless

Afonso Comba de Araujo Neto, Bruno Castro da Silva

[1]Instituto de Informática – Universidade Federal do Rio Grande do Sul

afonso@cpd.ufrgs.br, bcs@inf.ufrgs.br

Resumo. *As tecnologias sem fio são cada vez mais importantes para empresas e usuários domésticos, na medida em que facilitam a interconexão de dispositivos móveis e reduzem custos de infra-estrutura. Entretanto, a rápida difusão de dispositivos* wireless *não foi acompanhada por um semelhante avanço nos métodos de segurança envolvidos. Este artigo apresentará uma revisão acerca das precariedades de segurança que motivam nosso trabalho, assim como um* survey *entre os novos padrões de segurança em redes wireless sendo propostos pelas organizações responsáveis.*

1. Introdução

As redes *wireless* foram criadas a fim de resolver alguns problemas inerentes às redes tradicionais. Sem a necessidade de cabeamento físico, os dispositivos que necessitam de acesso à rede não mais ficam restritos a uma localização específica, o que é extremamente bom para *notebooks* e outros dispositivos móveis. Dada uma área de cobertura, computadores podem acessar a rede a partir de praticamente qualquer ponto geográfico, sem que ao usuário seja imposto nenhum esforço adicional.

Ao mesmo tempo em que o paradigma *wireless* oferece vantagens, traz consigo uma série de problemas, como o da falta de privacidade e de segurança. Da mesma maneira com que usuários legítimos têm acesso a rede, usuários ilegítimos também podem ter. Mais do que isso, sem a restrição física do acesso (ex: necessidade de acesso físico a um *hub*), um usuário malicioso pode ter acesso muito fácil a todos os dados que trafegam na rede. Para piorar ainda mais a situação, é bastante difícil, ou inviável, detectar indivíduos que estejam monitorando o tráfego de uma rede *wireless* [Borisov et al., 2001].

Essas características das redes *wireless* tornam claras a necessidade de mecanismos eficientes de criptografia e autenticação. Com isso em mente, o IEEE incluiu no padrão 802.11 para redes *wireless* um mecanismo de segurança chamado WEP, ou *Wired Equivalent Privacy*. O objetivo deste mecanismo era garantir em uma rede sem fio a segurança implícita obtida pela restrição de acesso ao barramento em uma rede cabeada.

Entretanto, o WEP se mostrou extremamente deficiente em vários aspectos. Diversos trabalhos da comunidade científica demonstram as falhas do WEP e as razões pelas quais ele não é confiável. Inicialmente, o IEEE respondeu aos problemas de segurança com uma proposta de tecnologia que ficou conhecida como WPA, *WiFi Protected Access*[1]. O WPA foi pensado como um passo transitório para uma solução definitiva, na medida em que poderia ser implantado sem que fosse necessário substituir todo o *hardware* já desenvolvido para suportar o WEP.

Nas seções seguintes serão apresentadas as deficiências do protocolo WEP e as soluções propostas pelo padrão 802.11i. Além disso, será feita uma crítica acerca de cada

[1]O WPA utiliza conceitos já em discussão no GT IEEE-802.11i, grupo de trabalho responsável pela definição de um padrão de segurança em redes *wireless*.

solução, e as várias sugestões serão comparadas a fim de prover um bom panorama do estado da arte da segurança em redes *wireless*.

2. WEP: uma tecnologia falha

As redes *wireless* tradicionais são constituídas por dois elementos principais: o ponto de acesso, AP (*Access Point*), e as estações de trabalho. Os APs funcionam como *gateways* em uma rede *wireless*, fornecendo o primeiro ponto de contato para as estações de trabalho e são o ponto de conexão com outras redes. Para uma estação de trabalho ter acesso à rede ela precisa fazer a chamada *associação* com um ponto de acesso. O padrão 802.11 original, implementado na maior parte dos dispositivos *wireless* comercializados hoje em dia, especifica duas formas de associação: a **associação via sistema aberto** e **associação via autenticação por chave compartilhada**.

A associação via sistema aberto na verdade poderia ser chamada de associação sem autenticação. A estação de trabalho simplesmente requisita o acesso à rede e o ponto de acesso o concede, sem quaisquer restrições. É fácil perceber que este esquema implica uma rede completamente vulnerável: além de qualquer pessoa ter acesso aos recursos da rede e aos dados que trafegam na mesma, ainda é possível inserir pontos de acesso falsos, capazes de estender a rede de uma forma não originalmente prevista.

O protocolo WEP é empregado quando se utiliza o método de associação via autenticação por chave compartilhada. Toda a segurança do WEP está centrada em um único elemento: o compartilhamento de uma chave secreta entre todos dispositivos. Esta chave precisa ser configurada manualmente em todos os dispositivos que tiverem autorização para utilizar a rede. A partir dessa chave, a estação de trabalho se associa ao ponto de acesso através de um protocolo do tipo desafio-resposta. A partir daí, todos os pacotes passam a ser criptografados. A seguir será apresentado um resumo a respeito do funcionamento desse método de criptografia.

2.1. Criptografia no WEP

A chave secreta do WEP possui 40 ou 104 bits, dependendo da configuração dos dispositivos da rede. Como ela é configurada manualmente em cada dispositivo, sua transmissão pela rede não precisa ocorrer em nenhuma situação.

Além de permitir a associação dos dispositivos ao ponto de acesso, essa chave compartilhada é utilizada para cifrar todos os pacotes que trafegam na rede. A cifragem propriamente dita é feita através o algoritmo RC4[2]. A cifragem dos pacotes se dá através dos seguintes passos:

1. é feito um cálculo de integridade do pacote através do algoritmo de CRC32. O resultado desse cálculo, chamado de ICV (*integrity check value*) é concatenado ao fim do pacote;
2. é gerado um vetor de inicialização de 24 bits, chamado de IV (*Initialization Vector*). Este IV, em princípio, deveria ser diferente para cada pacote gerado, mas na prática se repete em períodos de tempo que dependem do tráfego da rede e da forma como o algoritmo o determina;
3. o IV é concatenado com a chave secreta, gerando uma chave de cifragem de 64 ou 128 bits, dependendo do tamanho da chave secreta;

[2]RC4 é um cifrador de *stream* projetado por Ron Rivest. É um cifrador de chave variável com operação voltada a byte e baseado em permutação aleatória. Análises mostram que o período do encriptador é maior que 10^{100}.

4. o pacote é cifrado utilizando-se o algoritmo RC4 com a chave do passo anterior. O algoritmo gera, com base nessa chave, uma seqüência de *bytes* pseudo-aleatórios (também chamado de *stream* pseudo-aleatório), que são misturados com os *bytes* do pacote através da operação ou-exclusivo (XOR);
5. o pacote cifrado é enviado juntamente com o valor IV, sendo que este último transita em claro.

Ao receber um pacote cifrado, o receptor concatena a chave secreta com o IV que recebeu, de modo a reconstruir a seqüência pseudo-aleatória utilizada na cifragem do pacote utilizando novamente o RC4. O passo seguinte da decifragem consiste em aplicar novamente a seqüência de operações XOR a fim de reconstruir o conteúdo original do pacote. O receptor deve também recalcular o CRC32 do pacote, a fim de detectar alterações no conteúdo do mesmo.

2.2. Os problemas do WEP

Foi necessário pouco tempo após a publicação do padrão para que surgissem muitos dispositivos que já o implementassem. As deficiências do WEP foram descobertas na mesma velocidade. A seguir relaciona-se as principais fraquezas deste padrão:

O tamanho em bits do IV é muito pequeno Para redes com muito tráfego, o valor máximo delimitado pelos 24 bits do vetor de inicialização pode ser atingido em menos de um dia. Isso causa a reutilização dos vetores de inicialização, o que é um problema de segurança, pois pacotes com o mesmo vetor de inicialização utilizam o mesmo *stream* pseudo-aleatório para sua cifragem. Se for feito um ou-exclusivo entre dois pacotes com o mesmo IV, obtem-se o ou-exclusivo entre o valor em claro dos pacotes. Se o conteúdo de um deles for conhecido, o que não é incomum, pode-se descobrir o valor do outro. Da mesma forma, é possível obter o *stream* que foi utilizado para cifragem, o que então permitirá a decifragem de todos os pacotes subseqüentes com o mesmo IV;

O padrão não define como o IV deve ser modificado O problema anterior é acentuado por não haver regras para a geração do IV. É uma prática comum entre os dispositivos a reinicialização do IV em zero, sempre que estes dispositivos forem ligados. Com isso, o número de IVs utilizados diminui drasticamente;

O CRC32 não é adequado para detectar alterações propositais nos pacotes O algoritmo CRC32 é um ótimo mecanismo para detecção de erros aleatórios. Entretanto, ele utiliza um cálculo linear sobre os dados, de modo que é relativamente simples implementar um método que permita modificar o pacote de maneira que o destinatário não seja capaz de detectar tal alteração através da simples conferência do *checksum*;

Por ser parte da chave, o conhecimento do IV fornece pistas da chave secreta Para alguns valores IV é possível obter parte da chave secreta através de um algoritmo probabilístico. Para o ataque, basta o conhecimento do *stream* RC4 utilizado. A descoberta da chave envolve apenas a tarefa de se obter na rede alguns pacotes com os valores IV adequados e cujo conteúdo do pacote (ou pelo menos parte dele) seja conhecido. Note que o fato de todos os dispositivos utilizarem a mesma chave secreta faz com que todos os pacotes que trafegam na rede possam ser utilizados no ataque. Em uma rede com bastante tráfego, é possível obter a chave secreta em apenas algumas horas [Fluhrer et al., 2001];

O padrão não define formas automatizadas da atualização da chave secreta A maioria dos problemas citados seriam menos críticos se houvesse uma política de troca das chaves secretas. Entretanto, o fato da troca ser manual não permite que isso seja feito regularmente, sendo que em redes com muitos dispositivos isso seja uma tarefa praticamente inviável. Além disso, se algum dos dispositivos for comprometido, ou se algum dos usuários da rede acidentalmente perder a chave, então toda a rede ficará comprometida.

É importante salientar que, por mais problemas que o WEP possa ter, o seu uso é recomendável quando a única alternativa é o abandono completo da criptografia. Entretanto, em ambientes corporativos, e mesmo para usuários domésticos que se importam com a privacidade, o WEP simplesmente não é suficiente. Outro problema para os ambientes corporativos é a falta de mecanismos de autenticação em nível de usuário. O acesso a um dispositivo que contenha a chave compartilhada, ou a simples configuração da chave em qualquer dispositivo não confiável, são suficientes para garantir acesso completo a todos recursos da rede.

3. O padrão IEEE 802.11i

Com o objetivo de resolver as deficiências do padrão WEP, a IEEE designou ao chamado *Task Group i* a missão de criar um novo padrão de segurança para redes *wireless*. O padrão ainda não foi completamente estabelecido, mas as suas principais características já foram definidas [Robinson, 2004].

O padrão 802.11i define duas grandes classes de solução: a primeira, que atualmente foi certificada pela *WiFi Alliance*, é comercialmente conhecida como WPA; a segunda solução provavelmente será chamada de WPA2 [Burns, 2004].

3.1. WPA: uma solução imediatista

Um dos objetivos da primeira solução proposta pelo padrão 802.11i foi tentar resolver os problemas de segurança do WEP da melhor maneira possível, mas de forma a não implicar a troca de *hardware* nos dispositivos que já suportam WEP. De fato, isso foi um dos pré-requisitos impostos ao grupo, pois era necessário entregar aos usuários da tecnologia WEP uma solução que exigisse, no máximo, uma atualização de *software* ou *firmware*.

A principal característica do WPA é a utilização do protocolo chamado TKIP (*Temporal Key Integrity Protocol*), o qual foi desenvolvido especialmente a fim de resolver os principais problemas do WEP. O TKIP é implementado como uma camada de software que funciona sobre o WEP, de forma a resolver os seus problemas, mas sem tornar o sistema incompatível com o padrão original. Ele acrescenta quatro características novas ao protocolo WEP:

- É adicionado um novo código de integridade dos pacotes, denominado *Michael*, que utiliza uma chave de autenticação e facilita a detecção de alterações propositais no pacotes;
- Passam a existir regras no seqüenciamento dos vetores de inicialização, a fim de dificultar ataques de repetição e o reuso de IVs. O tamanho do IV é aumentado para 48 bits;
- É utilizada uma função *hash* para o cálculo da chave, a fim de remover a correlação entre vetores de inicialização e a seqüência pseudo-aleatória gerada pelo RC4. Além disso, esta função passa a incluir o endereço MAC do dispositivo como parte da chave, fazendo com que cada dispositivo acabe utilizando uma chave diferente;
- A chave secreta passa a ser substituída a cada 10 mil pacotes enviados.

Note que o TKIP ainda utiliza o algoritmo de *stream* RC4. Entretanto, ele resolve os problemas do WEP implementando uma política de uso de chaves adequadas e a sua substituição periódica. Dessa forma, a segurança é obtida utilizando o mesmo *hardware* do WEP. Além disso, ataques de força bruta são dificultados na medida em que a chave efetiva passa de 104 bits para 128 bits, no WPA, devido ao uso da função *hash*.

Para a geração da seqüência de chaves que serão utilizadas para cifragem dos dados, o protocolo TKIP utiliza uma chave mestre como base. No WPA (e também no WPA2), existem duas formas de se obter essa chave mestre. A primeira é uma autenticação em nível de usuário e a segunda é a partir de uma chave cadastrada diretamente nos dispositivos.

O esquema de autenticação em nível de usuário do WPA presume a utilização de um servidor de autenticação, o qual provê sua funcionalidade através do uso de um protocolo chamado EAP (*Extensible Authentication Protocol*) [Haining, 2002]. A arquitetura de autenticação do WPA é baseada no padrão 802.1X, responsável pela definição de um *framework* para autenticação e gerência dinâmica de chaves tanto em redes cabeadas quanto em redes wireless.

Nesse esquema, ao tentar se associar a um ponto de acesso, o cliente estabelece uma sessão EAP com o servidor de autenticação. O padrão não define o método específico de autenticação a ser utilizado, podendo ser implementado desde autenticação por desafio-resposta até autenticação via certificados digitais. Isso, na prática, depende do servidor de autenticação em questão.

Após uma autenticação bem sucedida, é gerada uma chave de sessão entre o servidor de autenticação, o ponto de acesso e o dispositivo cliente. Essa chave é válida somente durante essa sessão, e é então utilizada pelo TKIP para geração das chaves temporárias.

Para o seu uso em ambientes domésticos, onde seria inviável ou desnecessário a utilização de um servidor de autenticação, o WPA funciona em um modo denominado PSK (*Pre Shared Key*). Esse modo é exatamente o mesmo empregado no WEP, ou seja, uma chave é cadastrada manualmente em cada um dos dispositivos autorizados a fazer parte da rede. A diferença para o WEP é que, no WPA, o algoritmo TKIP gera chaves temporárias a partir desta chave secreta, de modo que a chave secreta propriamente dita nunca é utilizada diretamente para cifragem do tráfego entre os dispositivos.

4. WPA2: a solução definitiva

Uma solução mais completa para o problema de segurança em redes *wireless* é o WPA2, também chamado de RSN (*Robust Security Network*). A IEEE e a WiFi Alliance pretendem unificar o WPA2 e o 802.11i de modo a reduzir o número de padrões concorrentes, e também facilitar a adoção de soluções integradas por parte de fabricantes de *hardware*.

O WPA2 irá fornecer mecanismos de pré-autenticação, através dos quais uma estação se autentica em um AP com o qual irá se comunicar no futuro de modo que, durante o *roaming*, ocorre uma diminuição significativa do tempo de perda de sinal. Além disso, será empregado o protocolo CCMP para cifragem, o qual é baseado no algoritmo de criptografia AES utilizado em modo de operação CCM (*Counter Mode with CBC-MAC*). O CCM, que é independente do algoritmo de criptografia utilizado, é um modo genérico de operação que fornece autenticação e cifragem ao mesmo tempo, utilizando uma chave de 128 bits [Schneier, 1996]. O uso do AES, ao invés do RC4, garante maior segurança devido exatamente à melhor qualidade deste algoritmo.

Assim como o WPA, o WPA2 será definido em duas instâncias: o *WPA2 enterprise*, o qual conterá todos os requisitos necessários para suportar a autenticação prevista pelo padrão 802.1X com o protocolo EAP, e o *WPA2 personal*, que implementará o modo PSK e será voltado para ambientes SOHO (*Small Office/Home Office*).

Espera-se que a migração para o WPA2 das redes que utilizam o WPA não envolva maiores dificuldades, já que ele prevê um modo de operação conhecido como "*mixed-*

mode". Neste modo, um dispositivo WPA2 é capaz de tratar simultaneamente dispositivos que utilizem tanto tecnologia WPA quanto WPA2.

Uma questão importante é o fato de que, mesmo que o *framework* utilizado pelo WPA2 seja basicamente o mesmo do WPA, a adoção deste novo padrão não será transparente. Isso é devido a necessidade de atualização de *hardware* que ele implica. O *hardware* que implementa o WEP e o WPA não é capaz de oferecer criptografia AES com desempenho adequado. Provavelmente a migração para o WPA2 irá ocorrer lentamente, junto com o desenvolvimento da tecnologia *wireless*, e só acontecerá de maneira brusca em redes que exijam mecanismos de cifragem muito superiores ao RC4.

5. Conclusões

As deficiências do WEP foram prontamente detectadas pela comunidade científica e pelos usuários de redes *wireless*. A primeira reação por parte dos administradores foi a de implementar técnicas que transferissem a responsabilidade pela privacidade e autenticação para os níveis superiores da rede. Essas medidas retiravam do padrão 802.11 a responsabilidade por prover segurança, e consistiam na aplicação de mecanismos como VPNs (Virtual Private Networks) e IPSec (padrão da IETF para comunicação IP segura) [Schneier, 1996]. A abordagem por parte das organizações responsáveis pela definição dos padrões seguiu mais ou menos a mesma linha: primeiramente foram pensados mecanismos provisórios que sanassem os principais problemas do WEP. O padrão WPA tenta solucionar os problemas de segurança através do aumento do número de bits das chaves/IVs e também através da inserção de novos mecanismos na gerência e manipulação das chaves. O WPA2, por sua vez, exigirá maiores modificações em termos de *hardware*, provavelmente tornando os novos sistemas incompatíveis com a infra-estrutura atual. Entretanto, o pressuposto de que a segurança *wireless* deve ser provida pelo próprio padrão 802.11, e não por mecanismos externos adicionados ao gosto de cada administrador, exige que o paradigma atualmente utilizado seja substituído. Embora seja difícil prever a evolução dos sistemas de segurança, pode-se esperar que a adoção completa dos novos padrões ocorra aproximadamente no mesmo ciclo de substituição natural do *hardware* de redes *wireless*, caso o preço dos novos equipamentos acompanhe a crescente necessidade de sua adoção.

Referências

Borisov, N., Goldberg, I., and Wagner, D. (2001). Intercepting mobile communications: The insecurity of 802.11. In *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, Roma, Itália.

Burns, J. (2004). On the way: 802.11i and wpa2. *Communications News*.

Fluhrer, S., Mantin, I., and Shamir, A. (2001). Weaknesses in the key scheduling algorithm of RC4. *Lecture Notes in Computer Science*, 2259:1–24.

Haining, T. P. (2002). Enhanced wired equivalent privacy for ieee 802.11 wireless lans. *IEEE Document 802.11-00/362*.

Robinson, F. (2004). Examining 802.11i and wpa: The new standards – up close. *NetworkComputing Document*.

Schneier, B. (1996). *Applied Cryptography*. John Wiley and Sons, Inc., New York, 2nd edition.