Segurança em Redes Sem Fio

Segurança da Informação

Charles Tim Batista Garrocho

Instituto Federal de São Paulo – IFSP
Campus Campos do Jordão

garrocho.ifspcjo.edu.br/SEGA6

charles.garrocho@ifsp.edu.br

Curso Superior de TADS

Wi-Fi

Foi uma marca licenciada originalmente pela (Wi-Fi Alliance) para descrever a tecnologia de redes sem fio embarcadas (WLAN) baseadas no padrão IEEE (Institute of Electrical and Eletronics Engineers) 802.11.

O Wi-Fi opera em faixas de frequências que não necessitam de licença para instalação e/ou operação. Este fato as torna atrativas. Para se ter acesso à internet através de rede Wi-Fi deve-se estar no raio de ação de um ponto de acesso.

Os principais padrões das redes sem fio são:

Padrão	**Velocidade**	**Alcance**
a	54 Mbit/s	5000 m
b	11 Mbit/s	140 m
g	54 Mbit/s	140 m
n	150 Mbit/s	250 m

Mecanismos de Criptografia (WEP)

WEP (Wired Equivalent Privacy): é foi criado em 1999 e é compatível com praticamente todos os dispositivos WiFi disponíveis no mercado. Justamente por ser tão popular, é também o mais sujeito a falhas de segurança e o que possui mais buracos conhecidos.

O padrão WEP se torna mais inseguro à medida que o **poder de processamento** dos computadores aumenta. Por ser um sistema de segurança de 128 bits (fator que define os caracteres possíveis, ou seja, o número máximo de combinações de senha), é possível descobrir a palavra-passe de uma rede WiFi desse tipo em poucos minutos.

Oficialmente, o WEP não é considerado um padrão desde 2004, quando a Wi-Fi Alliance encerrou o suporte a ele. É altamente recomendado que você **não use esse protocolo**.

Mecanismos de Criptografia (WPA)

WPA (Wi-Fi Protected Access): adotado formalmente em 2003, a novidade trazia encriptação 256 bits e uma segurança muito maior para as redes. Além disso, sistemas de análise de pacotes e outras ferramentas foram implementadas para melhorar a segurança.

O problema aqui é que a arquitetura WPA foi produzida de forma a não tornar os dispositivos WEP obsoletos, e sim atualizáveis. Com isso, uma série de elementos do protocolo antigo foi **reaproveitada** e, diversos dos problemas do antecessor também acabaram presentes na nova versão.

A descoberta de senhas por meio de processamento também é uma ameaça aqui, mas não acontece exatamente da mesma maneira que no antecessor. Em vez de usar a força bruta para descobrir senhas, os criminosos podem atingir **sistemas suplementares**, herdados do protocolo WEP, que servem para facilitar a configuração e conexão entre dispositivos antigos e modernos.

Mecanismos de Criptografia (WPA2)

WPA2 (Wi-Fi Protected Acces II): é o padrão atual e também o mais seguro. A diferença aqui é a maneira como o sistema lida com senhas e algoritmos, excluindo completamente a possibilidade de um ataque de força bruta.

O **AES (Advanced Encryption Standard)**, um novo padrão para a segurança das informações, e o **CCMP (Counter Cipher Mode)**, um mecanismo de encriptação que protege os dados que passam pela rede. O WPA2 é tão complexo que muitos dispositivos, mesmo recentes, não são compatíveis com ele.

Exige que o atacante possua acesso normal à rede sem fio. Uma vez conectado, o hacker poderia assumir o controle de outros dispositivos ligados à rede, incluindo dados contidos neles ou transferidos a partir das máquinas. Mais uma vez, isso se deve a **programações de compatibilidade** para ligação de roteadores antigos e modernos.

Qual o melhor mecanismo?

A melhor opção sempre é a **mais segura**. Mas, em alguns casos, aparelhos que você possui em casa podem não funcionar com o protocolo WiFi escolhido.

Por isso, eis um **ranking de segurança** para que você possa configurar sua rede da melhor forma possível, da mais protegida até aquela que libera geral:

- WPA 2 com AES habilitado;
- WPA com AES habilitado;
- WPA com AES e TKIP habilitado;
- WPA apenas com TKIP habilitado;
- WEP;
- Rede aberta.

Atividade Prática

Ir á página 34 da monografia abaixo, e seguir a atividade do tópico 4.

http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf