Introdução a Segurança da Informação – Parte 5

13 de abril de 2015 / maximoz

Segurança Wireless

Em sistemas Wireless (sem-fio), o ar (radiofrequência) é usado para transmitir os dados ao invés de fios. Os sistemas Wireless são menos seguros seguros que sistemas cabeados porque os dados podem ser interceptados em trânsito e mal usados. Para proteger os dados, os controladores sem fio usam o Service Set Identifiers (SSID), WAP e WEP.

SSID são números de identificação nas placas de rede para garantir a segurança. WAP é para o uso com dispositivos móveis comos os PDAS e telefones celulares. Ele funciona semelhante ao TCP/IP e tem a mesma finalidade, mas para comunicações sem fio. WEP é um protocolo de privacidade especificado em IEEE 802.11 para fornecer comunicação segura para usuários de LAN sem fio.

Diversos protocolos de segurança sem fio foram desenvolvidos para proteger a rede Wireless. Dentre esses protocolos, como já vimos, incluem WEP, WPA e WPA2 (versão incrementada do WPA), cada um com seus pontos fortes – e pontos fracos. Além de prevenir convidados indesejados de conectar na sua rede sem fio, os protocolos de segurança Wireless encriptam seus dados privados, uma vez que estão sendo transmitidos por ondas.

Redes Wireless's são inerentemente inseguras. Nos primeiros dias de uso da rede Wireless, os fabricantes tentaram torná-la tão fácil quanto o possível para os usuários finais. A configuração out-of-the-box forneceu a maioria dos equipamentos de rede sem fio um fácil porém inseguro acesso a rede Wireless.

Embora muitos desses problemas tenham sido abordados, redes Wireless geralmente não são seguras como redes com fios. Redes com fio, em sua maioria, enviam dados entre dois pontos, A e B, nos quais são conectados por um cabo de rede. As redes sem fio, por outro lado, transmite dados em qualquer direção para qualquer dispositivo que passa a ser um listener (estar na escuta), dentro de um alcance limitado.

Veja, a seguir, as descrições dos protocolos de rede sem WEP, WPA e WPA2, respectivamente.

1. **Wired Equivalent Privacy (WEP):** O protocolo de criptografia original desenvolvido para redes Wireless. Como o nome traduzido diz, WEP foi projetado para fornecer o mesmo nível de segurança que redes cabeadas. No entano, WEP tem muitas bem conhecidas falhas de segurança, é difícil de configurar e é facilmente quebrada.
2. **Wi-Fi Protected Access (WPA):** Apresentado como um acessório de segurança provisória sobre WEP enquanto o padrão 802.11i estava sendo desenvolvido. A maioria das implementações atuais WPA usam uma chave pré-compartilhada (PSK), comumente referido como WPA Pessoal, e o Temporal Key Integrity Protocol (TKIP, pronunciado tee-kip) para criptografia. A WPA Enterprise usa um servidor de autenticação para gerar chaves ou certificados.
3. **Wi-Fi Protected Access version 2 (WPA2):** Baseado no padrão de segurança sem fio 802.11i, que foi finalizado em 2004. O aumento mais significativo para WPA2 sobre WPA é o uso do Advanced Encryption Standard (AES) para criptografia. A segurança proporcionada pela AES é suficiente (e aprovado) para utilização pelo governo dos EUA para criptografar informações classificadas como top secret – é provavelmente bom o suficiente para proteger os seus segredos tão bem quanto.

Próximo capítulo >>>

Traduzido e adaptado por: Maximoz Sec
Links originais: http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html
http://learnthat.com/introduction-to-network-security/