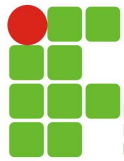
Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 11
Segurança em Redes Sem Fio

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"Tudo aquilo que precisares aprender, discernir e compreender chegará em tua existência repetidas vezes até dares a devida atenção, efetuando assim a aprendizagem necessária." (Hammed)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Conhecer os principais protocolos de segurança do protocolo IEEE 802.11;
- Aprender as principais características do protocolo WEP e suas vulnerabilidades;
- Entender como surgiu o WPA e suas principais características;
- Compreender o protocolo IEEE802.11i (WPA2) e WPA3, suas características e funcionalidades.
- Conhecer algumas ferramentas relacionadas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

As principais ameaças à transmissão *wireless* são captura, alteração ou inserção de mensagens e interrupção. Para minimizar estes poblemas podemos:

- Técnicas de ocultação de sinal: podemos esconder o *broadcasting* do identificador (SSID) nos pontos de acesso *wireless*;
- Encriptação: criptografando toda a transmissão *wireless* visando garantir a confidencialidade;
- Utilizar senhas fortes de administração do roteador e chaves forte de criptografia;
- Permita somente que computadores específicos acessem sua rede *wireless*, por exemplo, com filtros de endereços MAC;
- Realizar atualizações periódicas nos equioamentos da rede visando corrigir falhas ou adicionam funcionalidades;
- Utilizar protocolos de segurança do IEEE 802.11 (WPA2 ou WPA3).

Protocolos de Segurança do IEEE 802.11

O Wi-Fi Alliance desenvolveu vários procedimentos de certificação para padrões de segurança IEEE 802.11, entre eles temos o WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*). Estes protocolos visam garantir a autenticidade e a confidencialidade dos dados.

Entretanto, o padrão WEP está em desuso devido a diversas vulnerabilidades de segurança. Atualmente, o protocolo de segurança para redes sem fio é o WPA. Atualmente ele possui três versões WPA, WPA2 e WPA3.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

WEP - *Wired Equivalent Privacy*

A especificação 802.11 original incluía um conjunto de medidas de segurança (chamados de Wired Equivalent Privacy - WEP) para privacidade e autenticação que eram muito fracas. Ele contia pontos falhos, entre eles, chaves de 40 bits, criptografia de fluxo RC4, não protegia quadros de gerenciamento e controle. Como resultado, surgiram ataques e o WEP foi oficialmente abandonado pela Wi-Fi Alliance em 2004.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

WPA - *Wi-Fi Protected Access*

Em 2003, o Wi-Fi Alliance em conjunto com o IEEE desenvolveu um protocolo de segurança temporário para sanar as vulnerabilidades do WEP enquanto um novo padrão definitivo não era concluído. Este protocolo temporário foi chamado de WPA.

O desenvolvimento do WPA teve dois requisitos:

- Implementável por meio de *upgrade* de *software*, de forma que não fosse necessário *upgrade* de *hardware*. Essa condição limitou a escolha de mecanismos de segurança;
- Limitação de processamento dos dispositivos, uma vez que dispositivos de rede como interfaces de rede e *Access Points* não possuem poder de processamento significativo.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

WPA - *Wi-Fi Protected Access*

O WPA apresenta dois modos de operação, de acordo com o porte e as necessidades:

- *Personal*: voltado para o mercado doméstico e de pequenas empresas. Recomenda-se a utilização de autenticação por chave pré-compartilhada (PSK), ou seja, a distribuição das chaves é feita manualmente entre as estações;
- *Enterprise*: voltado para implantações de redes maiores. Recomenda-se neste modo Servidor de Autenticação (SA) baseado no protocolo 802.1x (LDAP ou RADIUS).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

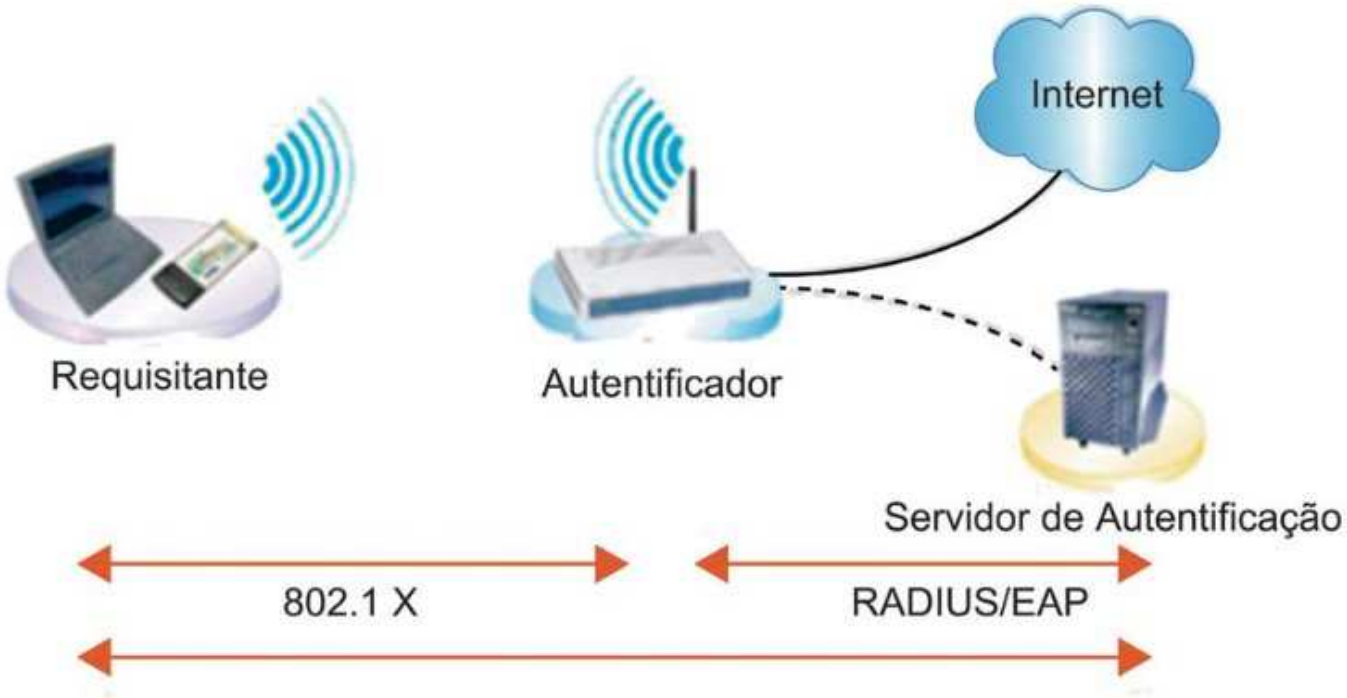
WPA - *Wi-Fi Protected Access*

O protocolo LDAP (*Lightweight Directory Access Protocol*) é um protocolo de gerenciamento de informações de usuários em diretórios no formato hierárquico. O LDAP utiliza o TLS para realizar a criptografia e autenticação das comunicações entre o cliente e o servidor.

O protocolo RADIUS (*Remote Authentication Dial-in User Service*) é um protocolo de autenticação centralizado para aplicações como acesso à rede. Ele facilita a administração dos usuários e os registros de utilização. As mensagens entre um cliente e um servidor RADIUS são criptografadas com chaves simétricas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

WPA - *Wi-Fi Protected Access*



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

WPA - *Wi-Fi Protected Access*

O WPA também utilizava o RC4 para criptografia, entretanto, resolveu as vulnerabilidades de WEP de três formas diferentes:

- Michael: função *hash* que garante a integridade do cabeçalho e *payload*. O *hash* gerado é de 64 *bits*. O objetivo era impedir que um invasor altere e reenvie pacotes de dados;
- TKIP: utilizado para gera chaves únicas por pacote de forma diferente do WEP. O TKIP gera dinamicamente uma nova chave de 128 *bits* para cada pacote e, assim, evita alguns tipos de ataques que comprometem o WEP.

O WPA também se mostrou vulnerável a ataques de dicionário. O uso de senhas fortes, com caracteres variados e com pelo menos 20 caracteres é fortemente recomendado.

WPA2 *Wi-Fi Protected Access Version 2*

Em 2004, surgiu o padrão definitivo para segurança do Wi-Fi, chamado de 802.11i, também é conhecido como WPA2. A implementação desse protocolo foi feita do zero, baseado nos estudos dos protocolos 802.10 e IPsec, não tendo nenhuma relação com WEP. Ele utiliza o protocolo CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol*) que faz uso do algoritmo de criptografia AES com chave de 256 *bits* para garantir a confidencialidade e *Hash* Michael para integridade dos dados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

WPA2 *Wi-Fi Protected Access Version 2*

O WPA2 também apresenta dois modos de operação, de acordo com o porte e as necessidades:

- *Personal*: voltado para o mercado doméstico e de pequenas empresas. Recomenda-se a utilização com chave pré-compartilhada (PSK);
- Enterprise: voltado para implantações de redes maiores. Neste é indicado um servidor de autenticação 802.1x (Radius ou LDAP). Trouxe diversos protocolo EAP (*Extensible Authentication Protocol*) para autenticação, por exemplo, Kerberos, chaves públicas, EAP-TLS. O EAP-TLS que utiliza certificados, chaves públicas e assinaturas digitais é o mais utilizado e considerado o mais seguros.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Em 2018, o Wi-Fi Alliance lançou o WPA3. Ele apresenta como novidades:

- Novos métodos de autenticação (SAE - *Simultaneous Authentication of Equals*) visando proteger contra ataques de força bruta com dicionário *off-line*;
- Novos algoritmos de criptografia e hash visando melhor segurança para ambientes corporativos com criptografia baseada em AES-256 com SHA-384 como HMAC.
- O Easy Connect visando facilitar a conecção com dispositivos sem tela e Internet das Coisas (IoT).
- Implementa novos protocolos: *Transport Layer Security* (EAP-TLS) com *Elliptic Curve Diffie-Hellman* (ECDH) e *Elliptic Curve Digital Signature Algorithm* (ECDSA), *Galois/Counter Mode Protocol* (GCMP).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Ferramentas de Segurança no IEEE 802.11

- Aircrack-ng: permite o monitoramento da rede, captura de tráfego, ataque de repetição e desautenticação, criação de pontos de acesso falsos e quebra de senha nos protocolos WEP e WPA/WPA2 com autenticação baseada em PSK;
- coWPAtty: implementa um ataque de dicionário contra o protocolo WPA/WPA2 usando autenticação baseada em PSK.
- FreeRADIUS: é o servidor RADIUS de código livre mais utilizado. Ele suporta o maior número de tipos de autenticação do protocolo EAP.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE