segurança

7

Projeto Um Computador por Aluno

Ministério da Educação

projetouca@mec.gov.br
http://www.mec.gov.br

Cartilhas Projeto UCA: Segurança

Copyright © 2010, Escola Superior de Redes RNP

Autor
Equipe do Laboratório de Pesquisas
MídiaCom, vinculado ao Departamento
de Engenharia de Telecomunicações
e ao Instituto de Computação da
Universidade Federal Fluminense (UFF)

Produção Editorial

Escola Superior de Redes RNP

Versão
1.0.1

Esta obra é distribuída sob a licença
Creative Commons: Atribuição e Uso Não-Comercial 2.5 Brasil

Segurança

Esta cartilha tem o objetivo de informar noções básicas de segurança de redes sem fio, descrevendo os principais mecanismos de segurança utilizados atualmente.

A importância da segurança em redes sem fio

Segurança é um tópico de extrema importância em redes de computadores. Os procedimentos e técnicas de segurança existem para combater o mau uso dos recursos compartilhados, afastar usuários mal intencionados, garantir a integridade e a privacidade dos dados trafegados e armazenados, e também a autenticidade dos agentes, isto é, confirmar se um indivíduo ou programa é de fato quem afirma ser.

Os objetivos acima são comuns a todas as redes de computadores, mas de implementação mais difícil em redes sem fio. Quando a conexão entre os computadores em uma rede é feita através de cabos (figura 1), a sua invasão só é possível através do acesso direto aos cabos. Com isso, o controle sobre o acesso à rede é relativamente fácil. Já em redes sem fio (figura 2), onde a comunicação é feita pelo ar, a segurança se torna mais importante e complexa.

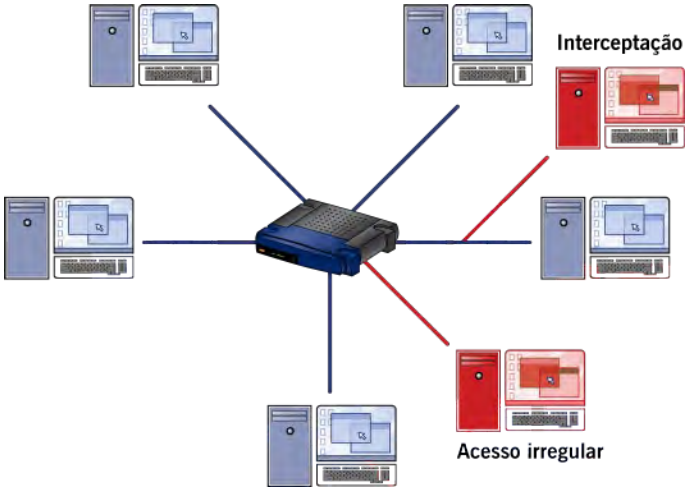


Figura 1
Rede cabeada

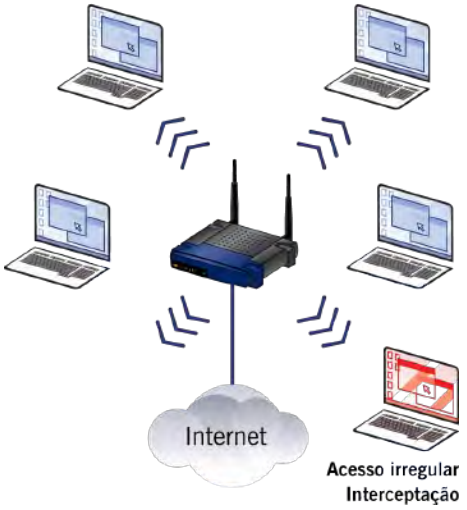


Figura 2
Rede sem fio

Na ausência de um mecanismo de segurança, qualquer indivíduo com uma antena e um receptor de rádio sintonizado na frequência de operação correta pode interceptar a comunicação ou utilizar os recursos dessa rede. Nossa análise sobre o problema da segurança partirá de uma classificação das ameaças.

Interceptação

Acontece quando um usuário não autorizado consegue acessar e manipular as informações transmitidas pelos usuários regulares da rede. Este tipo de invasão compromete questões de segurança relacionadas a:

- **Integridade:** Uma mensagem íntegra é aquela que não sofreu nenhuma alteração, intencional ou acidental, sem o conhecimento do emissor. Exemplo: se um e-mail enviado pelo professor com as notas da turma tiver seu conteúdo modificado por outra pessoa, estaremos diante de um problema de integridade.

- **Autenticidade:** Sem um mecanismo que forneça autenticidade, um invasor pode se passar por outra fonte para gerar informações ilegítimas. Exemplo: se uma pessoa enviar um e-mail aos professores da escola se fazendo passar pelo diretor, estaremos diante de um problema de autenticidade.

- **Privacidade:** Um mecanismo de segurança que provê privacidade garante que a mensagem enviada somente será lida pelo destinatário escolhido. Exemplo: se uma mensagem de e-mail trocada por dois professores for lida por um aluno não autorizado, estaremos diante de uma falha de privacidade.

Acesso irregular

O acesso irregular acontece quando um usuário não autorizado se conecta ao ponto de acesso para usufruir de recursos desta rede, como, por exemplo, o acesso à Internet. Este é um problema recorrente nas redes sem fio. Limitar o acesso à rede sem fio apenas para usuários autorizados é importante por dois motivos:

- Evitar que usuários desconhecidos utilizem a rede sem fio para cometer crimes.
- Evitar que usuários não autorizados consumam recursos compartilhados da rede, prejudicando os usuários legítimos.

Mecanismos de segurança

Existem vários mecanismos de segurança disponíveis nos pontos de acesso atuais, desenhados para dificultar ou impedir os problemas acima listados. Os mais importantes são:

WEP (Wired Equivalent Privacy)

Foi o primeiro mecanismo de segurança criado para redes sem fio IEEE 802.11 (Wi-Fi). O administrador da rede cria uma senha que deve ser informada a todos os usuários da rede, chamada de chave pré-compartilhada. Somente após a digitação desta senha o usuário está autorizado a utilizar a rede. O WEP possui inúmeras falhas que o tornam vulnerável, devendo ser usado apenas quando as opções mais avançadas (WPA e WPA2) não estiverem disponíveis.

WPA (Wi-Fi Protected Access)

Mecanismo de segurança criado para solucionar as falhas do WEP e ao mesmo tempo manter a compatibilidade com os equipamentos existentes no mercado (notebooks, PDAs etc). O WPA reforça a segurança com a introdução de chaves individualizadas, mas assim como o WEP, também pode usar chaves pré-compartilhadas. Embora seja significativamente mais seguro do que o WEP, novas falhas de segurança foram descobertas.

WPA2

Mecanismo mais completo e seguro que também pode utilizar chaves pré-compartilhadas ou individualizadas. No WPA2, o invasor encontra uma dificuldade significativamente maior para descobrir as senhas dos usuários. Apesar de alguns equipamentos não suportarem o uso do WPA2, este mecanismo de segurança deve ser escolhido sempre que possível.

O modo de operação mais usado com WPA e WPA2 é o Personal, que utiliza chaves pré-compartilhadas e foi projetado para o ambiente doméstico ou para pequenos escritórios. Outro modo de operação ainda mais seguro, e geralmente usado em ambientes corporativos, é conhecido como WPA e WPA2 Enterprise, que utiliza chaves individualizadas. Este método implica o uso de um servidor adicional, dedicado à autenticação dos usuários de forma ainda mais robusta e, em geral, pode ser dispensado em cenários onde as demandas por segurança não são tão severas.

Os três mecanismos apresentados até agora dificultam o acesso irregular. As senhas ou chaves usadas nos três mecanismos também protegem as mensagens enviadas pelos usuários, provendo graus variados de integridade, privacidade e autenticidade.

É importante que as senhas sejam escolhidas de modo a dificultar sua descoberta por tentativa e erro. Por exemplo, utilizar como senha o nome da escola ou do(a) diretor(a) não é uma escolha adequada, por ser uma senha previsível. Palavras como “senha”, “password”, “chave” e “escola” também não são recomendadas, pelo mesmo motivo. Uma senha segura deve conter letras, números e outros símbolos, como por exemplo “e2s6c0la=” (Não usem esta, agora ela se tornou fácil!).

Filtro de MAC

Uma placa de rede presente nos clientes da rede sem fio (notebooks, computadores de mesa, PDAs etc) possui um único identificador chamado "endereço MAC".

Endereço MAC (Midia Access Control): Código que identifica unicamente uma placa de rede

Uma funcionalidade comumente encontrada nos pontos de acesso é a de filtros de MAC, que permite listar os endereços MAC de todos os clientes autorizados a utilizar o ponto de acesso, bloqueando o acesso dos dispositivos não listados.

Esse mecanismo dispensa a digitação de senha pelo usuário, mas não oferece proteção contra interceptação dos dados.

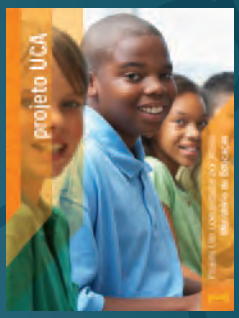
Configuração do ponto de acesso

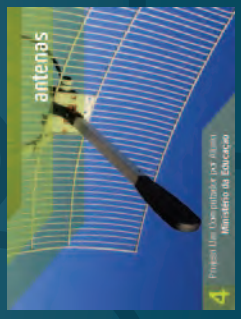
O ponto de acesso é configurado através de uma interface web acessada por navegadores como Internet Explorer, Mozilla Firefox ou Google Chrome. A interface permite configurar o método de segurança (WEP, WPA, WPA2) e a senha de acesso à rede. Para acessar a interface de administração do equipamento são necessários o endereço do ponto de acesso, o usuário e a senha de autenticação.

Assim como é importante a escolha de senhas difíceis para o WEP, WPA e WPA2, o mesmo se aplica para a senha do administrador do ponto de acesso. Usuários e senhas fáceis podem ser descobertos por tentativa e erro. Caso isso ocorra, o invasor poderá configurar o ponto de acesso da maneira que lhe for conveniente, desabilitando os mecanismos de segurança.

A interface de administração deve ser desabilitada para os usuários da rede sem fio, restringindo o acesso aos usuários conectados à rede tradicional cabeada.

Projeto Um Computador por Aluno





Projeto UCA
Segurança

Esta cartilha tem o objetivo de informar noções básicas de segurança de redes sem fio, descrevendo os principais mecanismos de segurança utilizados atualmente.

Ministério da Ciência e Tecnologia
Ministério da Educação