



Instituto Infnet

Segurança Da Informação

FABIANO GISBERT

Segurança na Rede Sem Fio

Ondas Eletromagnéticas

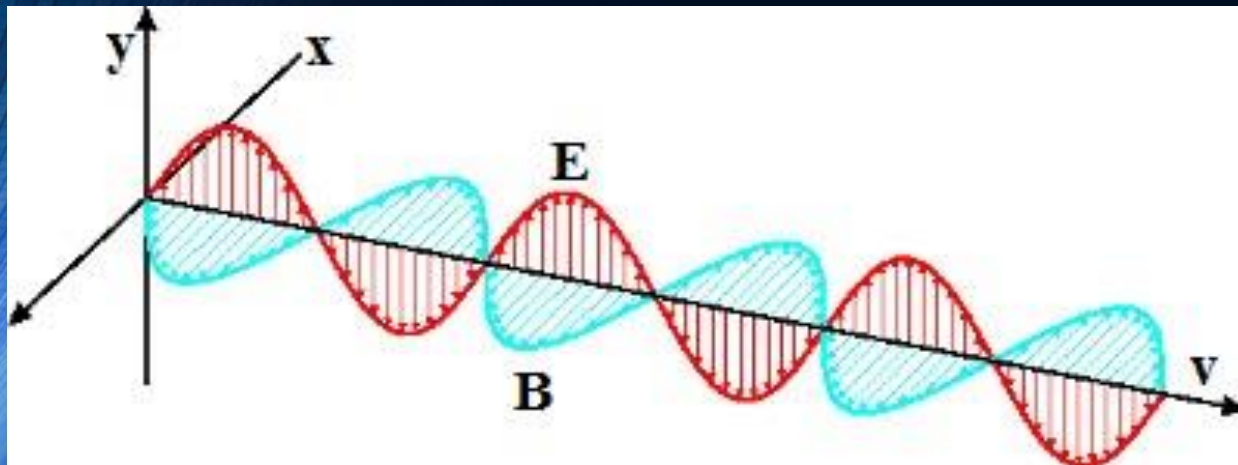


Instituto Infnet

Introdução

As ondas eletromagnéticas são resultado das combinações de campos elétricos e campos magnéticos. Foi graças à descoberta das propriedades dessas ondas que hoje em dia podemos ouvir músicas ou notícias nos rádios, assistir a programas de TV, aquecer alimentos em micro-ondas, acessar à internet e mais uma infinidade de coisas.

As ondas eletromagnéticas resultam da combinação de um campo elétrico e de um magnético que se propagam no espaço.



A oscilação de uma carga elétrica dá origem a campos magnéticos. Esses campos, por sua vez, produzem campos elétricos, assim como a variação de fluxo de campos elétricos origina campos magnéticos.

A interação entre esses campos é responsável pelo surgimento das ondas eletromagnéticas.



Ondas Eletromagnéticas

Características das ondas eletromagnéticas

- São formadas pela combinação de campos elétricos e magnéticos variáveis;
- O campo elétrico e o campo magnético são perpendiculares;
- O campo elétrico e o magnético são perpendiculares à direção de propagação, o que significa que são ondas transversais;
- A velocidade de propagação dessas ondas no vácuo é $c = 3 \cdot 10^8 \text{ m/s}$;
- Ao propagar em meios materiais, a velocidade obtida é menor do que quando a propagação ocorre no vácuo.

Energia



Instituto Infnet

O que é?

Energia é a capacidade da matéria de produzir trabalho na forma de movimento, luz, calor etc. É uma quantidade física escalar e pode vir de várias formas.

É uma medida única de várias formas de movimento e interação da matéria, uma medida da transição da matéria de uma forma para outra.



A lei de conservação de energia anuncia que: "a energia não é criada nem destruída", só pode ser transformada. Só é possível converter um tipo de energia em outro tipo.

Um sistema fechado é um sistema que não troca energia com o exterior. Portanto, em sistemas físicos fechados, a quantidade total de energia sempre permanece constante.

Ondas



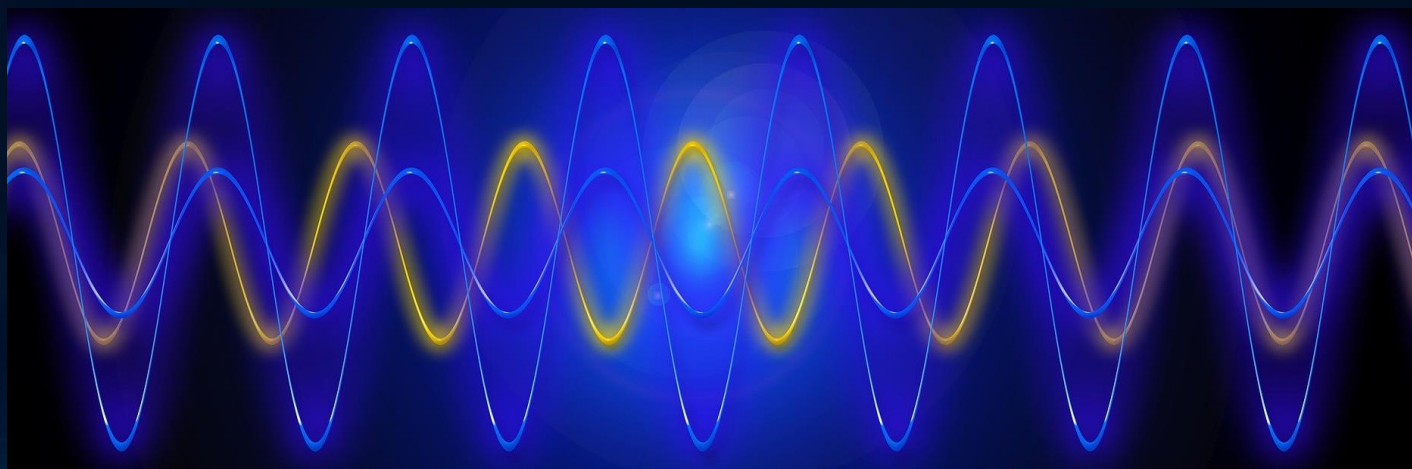
Instituto Infnet

O que é?

As ondas são perturbações que se propagam pelo espaço sem transporte de matéria, apenas de ENERGIA.

O elemento que provoca uma onda é denominado fonte, por exemplo, uma pedra lançada nas águas de um rio gerarão ondas circulares.

São exemplos de ondas: ondas do mar, ondas de rádio, som, luz, raio-x, micro-ondas dentre outras.



Ondas



Instituto Infnet

Métricas das Ondas

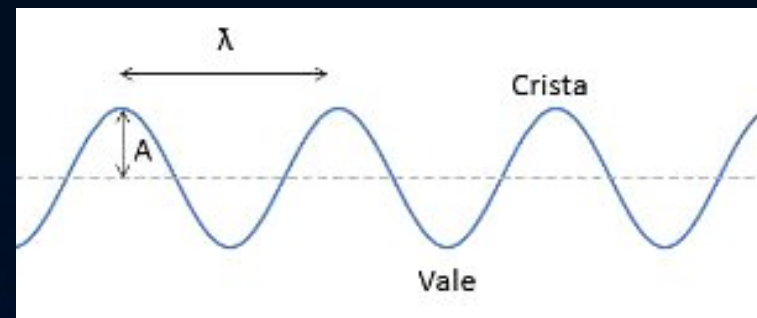
Amplitude: corresponde à altura da onda, marcada pela distância entre o ponto de equilíbrio (repouso) da onda até a crista. Note que a “crista” indica o ponto máximo da onda, enquanto o “vale”, representa a ponto mínimo.

Comprimento de onda: Representado pela letra grega lambda (λ), é a distância entre dois vales ou duas cristas sucessivas.

Velocidade: representado pela letra (v), a velocidade de uma onda depende do meio em que ela está se propagando. Assim, quando uma onda muda seu meio de propagação, a sua velocidade pode mudar.

Frequência: representada pela letra (f), no sistema internacional a frequência é medida em hertz (Hz) e corresponde ao número de oscilações da onda em determinado intervalo de tempo. A frequência de uma onda não depende do meio de propagação, apenas da fonte que a produziu.

Período: representado pela letra (T), o período corresponde ao tempo de um comprimento de onda. No sistema internacional, a unidade de medida do período é segundos (s).



Ondas



Instituto Infnet

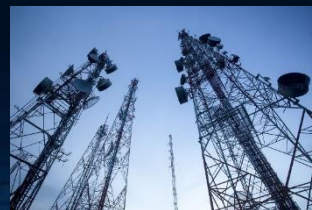
Tipos de Ondas

Quanto à natureza, há dois tipos de ondas:

Ondas Mecânicas: Ondas mecânicas são perturbações que transportam energia cinética e potencial através de um meio material. Essas perturbações acontecem na forma de pulsos, os quais são ondas de curta duração que se repetem com intervalos de tempo iguais. Exemplos: Ondas do mar, som nas cordas de um violão.



Ondas Eletromagnéticas: são as oscilações que acontecem como resultado da libertação de energia elétrica e magnética. Nesse caso, não é necessário que haja um meio material para que a onda se propague, por exemplo, as ondas de rádio e a luz.



Ondas Eletromagnéticas



Instituto Infnet

Espectro eletromagnético

O espectro eletromagnético diz respeito a toda gama de possíveis frequências que uma onda eletromagnética pode apresentar, como a luz visível, as micro-ondas, as ondas de rádio, radiação infravermelha, radiação ultravioleta, raios x e raios gama.



A distinção entre elas é fenomenológica, por exemplo: apesar de tratarem-se de ondas eletromagnéticas, o raio x e a luz visível são bastante distintos no modo em que interagem com a matéria.



Ondas Eletromagnéticas

Tipos de ondas

Não Ionizantes:

Ondas de rádio: apresentam a menor frequência entre as ondas eletromagnéticas e, conseqüentemente, o maior comprimento de onda. São comumente usadas para transmissão de sinal de televisão, rádio e celular.

Micro-ondas: têm frequência um pouco maior que as ondas de rádio, são bastante usadas nas telecomunicações (no wi-fi, por exemplo) e também em radares que captam a velocidade de veículos em movimento.

Infravermelho: apresenta frequência pouco inferior à da luz visível, esse tipo de onda, também conhecido como onda de calor, é capaz de aumentar a agitação térmica de átomos e moléculas. Quando nos aproximamos de uma fogueira e sentimos o seu calor, parte da energia transmitida para nós vem em forma de radiação térmica, transportada pelas ondas de infravermelho.

Luz visível: é aquela que pode sensibilizar os olhos dos seres humanos, uma vez que existem animais capazes de enxergar diferentes tipos de ondas eletromagnéticas, como o infravermelho e o ultravioleta, por exemplo. A luz visível compreende uma estreita faixa de comprimentos de onda no espectro eletromagnético, entre 700 nm e 400 nm (nanômetros = 10^{-9} m).

Ondas Eletromagnéticas



Instituto Infnet

Tipos de ondas

Ionizantes:

Ultravioleta: é considerada uma radiação ionizante, isto é, durante a sua interação com a matéria, ela é capaz de arrancar elétrons dos átomos, causando danos a moléculas importantes, como aquelas presentes no DNA das células epiteliais. Devido à sua capacidade ionizante, a radiação ultravioleta é usada na esterilização de utensílios médicos, por exemplo.

Raios x: são ondas eletromagnéticas ionizantes com grande poder de penetração. Esse tipo de onda é capaz de atravessar diversos tipos de tecidos, graças ao seu pequeno comprimento de onda. São largamente utilizadas em exames de imagens, como radiografia e tomografia.

Raios gama: são as ondas eletromagnéticas de maior frequência em todo o espectro eletromagnético, podem ser obtidas em reações nucleares e durante a aniquilação de pares (quando há contato entre matéria e antimatéria). No entanto a maior parcela de raios gama que incidem sobre a Terra tem origem em estrelas, como o nosso Sol. Esse tipo de radiação é extremamente penetrante e possui grande capacidade de ionização.

Ondas Eletromagnéticas



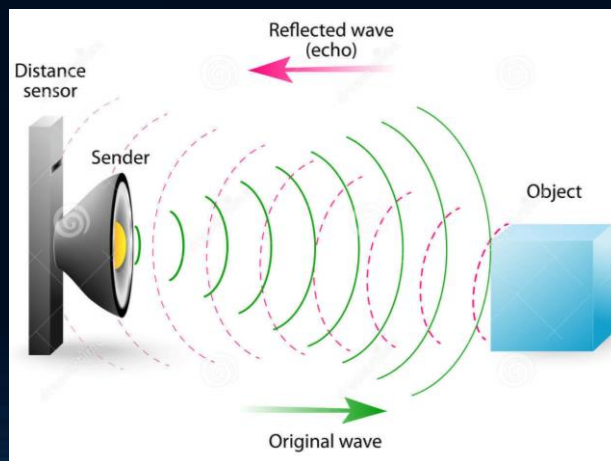
Instituto Infnet

Fenômenos Ondulatórios

Reflexão:

Uma onda se propagando em um determinado meio ao se deparar com um obstáculo pode sofrer reflexão, isto é, inverter o sentido da propagação.

Ao sofrer reflexão, o comprimento de onda, a velocidade de propagação e a frequência da onda não se alteram. Um exemplo é quando uma pessoa grita em um vale e escuta alguns segundos depois o eco da sua voz.



Ondas Eletromagnéticas



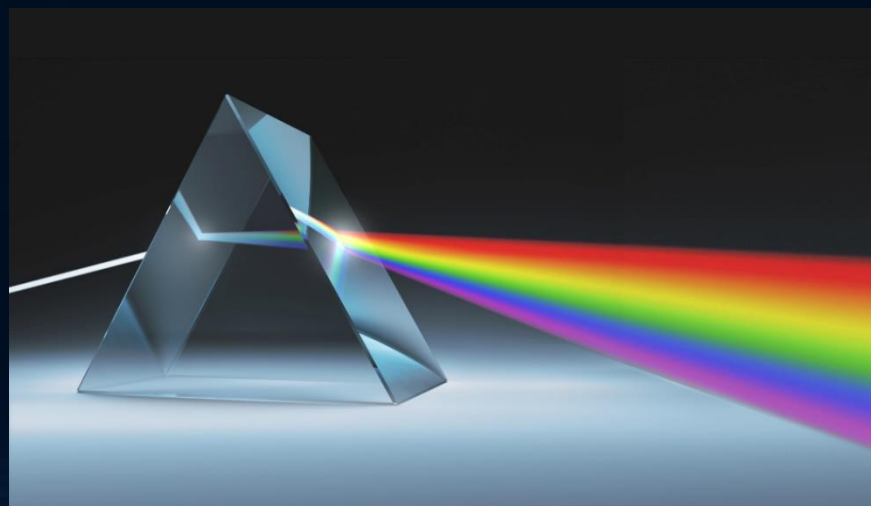
Instituto Infnet

Fenômenos Ondulatórios

Refração

A refração é um fenômeno que acontece quando uma onda muda o meio de propagação. Nesse caso, poderá ocorrer uma mudança no valor da velocidade e na direção de propagação.

As ondas propagadas no vácuo possuem velocidades e direções distintas quando propagada pela atmosfera terrestre.



Ondas Eletromagnéticas



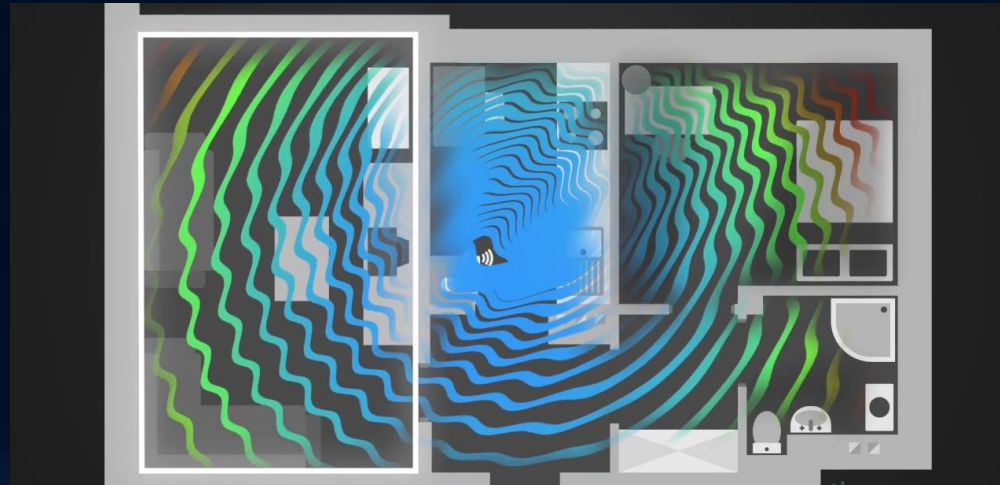
Instituto Infnet

Fenômenos Ondulatórios

Difração

As ondas contornam obstáculos. Quando isso ocorre dissemos que a onda sofreu difração.

A difração acontece, por exemplo, na propagação de um sinal de wi-fi por um local com várias salas.



Ondas Eletromagnéticas



Instituto Infnet

Fenômenos Ondulatórios

Interferência

Quando duas ondas se encontram, ocorre uma interação entre suas amplitudes chamada de interferência.

A interferência pode ser construtiva (aumento da amplitude) ou destrutiva (diminuição da amplitude).

No transporte de dados, a interferência altera o resultado independente do fenômeno.



Ondas Eletromagnéticas



Instituto Infnet

Frequência na prática

Sinal de Wi-fi 2G e 5G

Quando falamos em frequências de rádio, precisamos entender um princípio básico: quanto mais alta a frequência do sinal transmitido, mais forte ele vai ser, contudo, menor será o seu alcance. Isso significa que o sinal de 5 GHz (5G) possui mais intensidade a curta distância; já a frequência de 2,4 GHz (2G) pode carregar menos dados de uma única vez, mas pode chegar a distâncias maiores.

Além disso, os 2,4 GHz também são mais eficientes na hora de atravessar objetos sólidos, como paredes, algo que o sinal de 5 GHz não consegue fazer com muita eficiência.

Por outro lado, a frequência 5 GHz é mais ampla e possui 23 canais de transmissão que não se sobrepõem, contra apenas 3 canais nos 2,4 GHz. Isso faz com que exista menos interferência na frequência mais alta. E como a frequência é maior, a perda é menor em ambientes com muita difração.



Segurança na Rede Sem Fio

Redes Wi-Fi

As redes Wi-Fi ou conexões sem fio estão cada vez mais populares por conta do crescimento da tecnologia. Milhares de pessoas vão a cafés, bibliotecas, museus, restaurantes, entre outros, e se conectam à rede com seus smartphones ou laptops. Com certeza você já fez isso, talvez pela necessidade de se comunicar com alguém próximo, para verificar seu e-mail ou outra coisa.

Quando nos conectamos a uma rede Wi-Fi, quase nunca pensamos sobre sua segurança. Mas será que isso é necessário? A resposta é sim, se conectar a uma rede sem fio insegura pode facilitar o roubo de arquivos pessoais, senhas de banco ou de rede sociais.

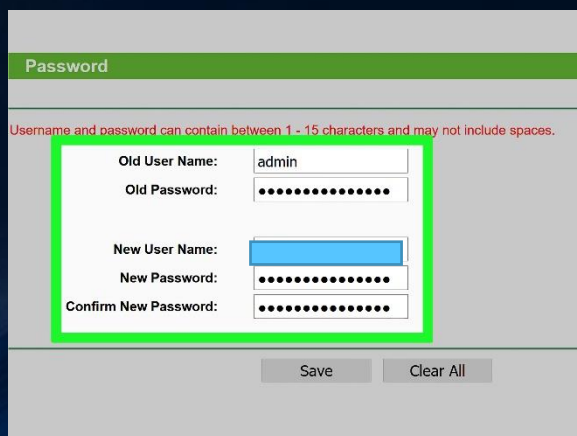


Segurança na Rede Sem Fio

Redes Wi-Fi Domésticas

Os roteadores usados para prover o sinal deve ter uma senha de acesso privativa e sob o controle do administrador da rede. Também é recomendado configurar o acesso roteador através do protocolo HTTPS para impedir o roubo da senha, ocultar o nome que identifica a rede Wi-Fi para que as pessoas próximas a rede não a vejam quando buscam uma conexão com a internet.

Para a emissão da rede sem fio, recomenda-se que o tipo de criptografia da rede seja WPA2 que é mais seguro do que WPA, WEP e TKIP. Assim, a informação que circula na rede estará mais segura se alguém quiser acessá-la.



Username and password can contain between 1 - 15 characters and may not include spaces.

Old User Name: admin

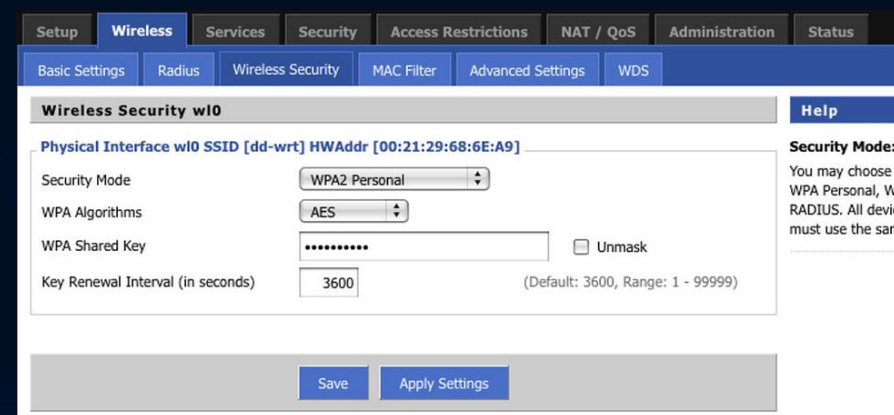
Old Password:

New User Name:

New Password:

Confirm New Password:

Save Clear All



Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

Basic Settings Radius Wireless Security MAC Filter Advanced Settings WDS

Wireless Security w10 Help

Physical Interface w10 SSID [dd-wrt] HWAddr [00:21:29:68:6E:A9]

Security Mode: WPA2 Personal

WPA Algorithms: AES

WPA Shared Key: Unmask

Key Renewal Interval (in seconds): 3600 (Default: 3600, Range: 1 - 99999)

Save Apply Settings

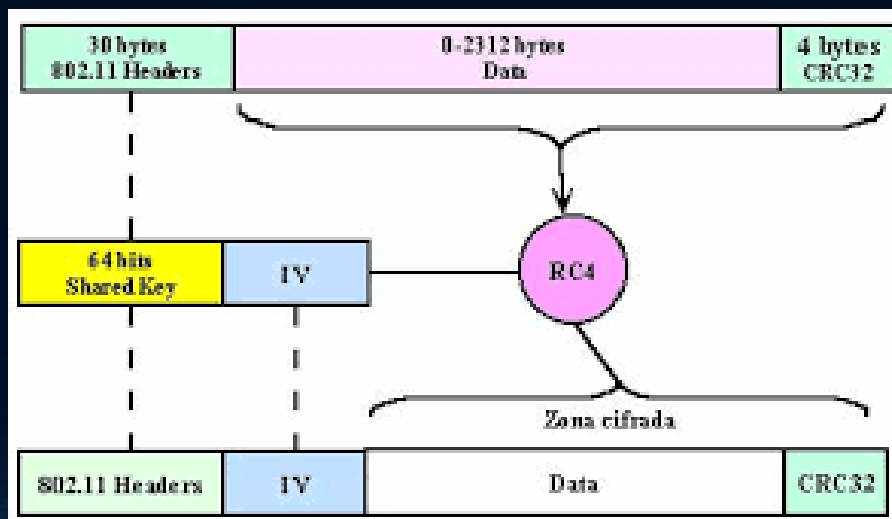
Security Mode: You may choose from WPA Personal, WPA RADIUS. All devices must use the same

Segurança na Rede Sem Fio

Padrão WEP

O WEP (Wired Equivalent Privacy) criptografa o tráfego usando uma chave de 64 ou 128 bits em hexadecimal. Esta é uma chave estática, o que significa que todo o tráfego, independentemente do dispositivo, é criptografado usando uma única chave.

Um dos principais objetivos do WEP era evitar ataques Man-in-the-Middle, o que fez por um tempo. No entanto, apesar das revisões do protocolo e do aumento do tamanho da chave, várias falhas de segurança foram descobertas no padrão WEP ao longo do tempo.





Segurança na Rede Sem Fio

Padrão WPA

WPA (Wi-Fi Protected Access) foi o substituto da Wi-Fi Alliance para WEP. Ele compartilhava semelhanças com o WEP, mas oferecia melhorias no modo como lida com as chaves de segurança e na forma como os usuários são autorizados. Enquanto o WEP fornece a cada sistema autorizado a mesma chave, o WPA usa o protocolo de integridade de chave temporal (TKIP), que altera dinamicamente a chave que os sistemas usam. Isso evita que invasores criem sua própria chave de criptografia para corresponder à usada pela rede segura.

Além disso, o WPA incluiu verificações de integridade de mensagens para determinar se um invasor capturou ou alterou pacotes de dados. As chaves usadas pelo WPA eram de 256 bits, um aumento significativo em relação às chaves de 64 e 128 bits usadas no sistema WEP.

O WPA2 foi introduzido em 2004 e era uma versão atualizada do WPA. O WPA2 é baseado no mecanismo de rede de segurança robusta (RSN).

WPA3 é a terceira iteração do protocolo Wi-Fi Protected Access. A Wi-Fi Alliance lançou o WPA3 em 2018. O WPA3 introduziu novos recursos para uso pessoal e empresarial.



Segurança na Rede Sem Fio

Ameaças

Interceptação de dados – Os dados sem fio abertos trafegam dados não criptografados, permitindo que sejam interceptados e lidos por pessoas não autorizadas.

Intrusos sem fio – Os usuários não autorizados que tentam acessar os recursos da rede podem ter seu objetivo alcançado por meio de técnicas de autenticação, quebra da senha WAP ou acesso ao access point.

Ataques de negação de serviço (DoS) – O acesso aos serviços de WLAN pode ser comprometido acidental ou maliciosamente. Existem várias soluções, dependendo da origem do ataque DoS.

APs invasores – APs não autorizados instalados por um usuário bem-intencionado ou para fins mal-intencionados podem ser detectados usando um software de gerenciamento. Uma vez conectado, o AP não autorizado pode ser usado por um invasor para capturar endereços MAC, capturar pacotes de dados, obter acesso a recursos de rede ou lançar um ataque man-in-the-middle.

Segurança na Rede Sem Fio

Redes Wi-Fi Públicas

As conexões públicas são as entramos como convidados e as vezes não pensamos nas consequências de se conectar a uma rede sem as devidas precauções. Assim como você se conecta a essa rede, centenas de pessoas também fazem o mesmo e não podemos saber quais são suas intenções.

Por isso, quando você acessar uma rede pública pela primeira vez, alguns dispositivos vão lhe perguntar que tipo de conexão é: escolha Rede pública, porque assim, as medidas de segurança que o aparelho terá serão maior.

Quando você acessar um site, verifique se tem o protocolo de dados seguros HTTPS para estar mais seguro.

Evite ao máximo manipular dados pessoais e efetuar transações financeiras quando estiver numa conexão pública. Se for necessário estabelecer uma sessão com sistemas da empresa, utilizar um serviço de VPN corporativo ou de confiança



Segurança na Rede Sem Fio

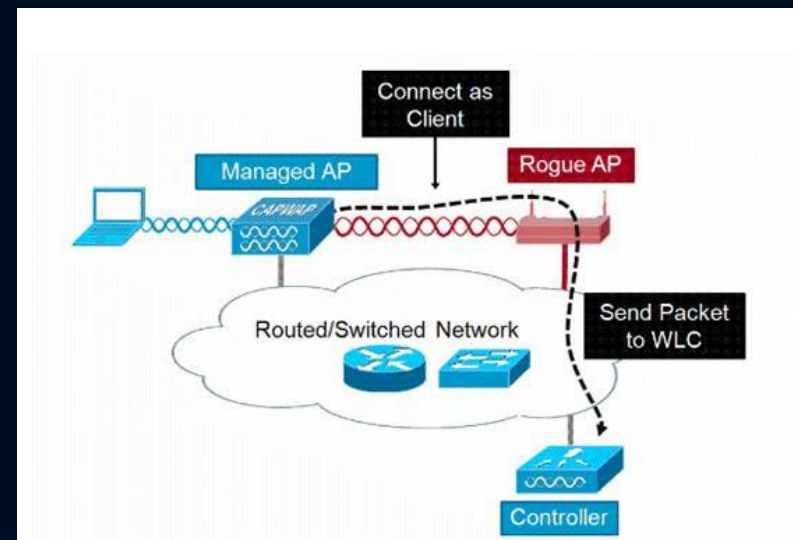
Redes Wi-Fi Públicas

Ameaças

Ponto de acesso não autorizado

Um ponto de acesso não autorizado (AP) é um ponto de acesso que foi instalado em uma rede sem autorização explícita de um administrador do sistema.

Os pontos de acesso invasores representam uma ameaça à segurança, pois qualquer pessoa com acesso à área pode instalar um ponto de acesso sem fio que pode permitir o acesso de partes não autorizadas à rede.



Segurança na Rede Sem Fio

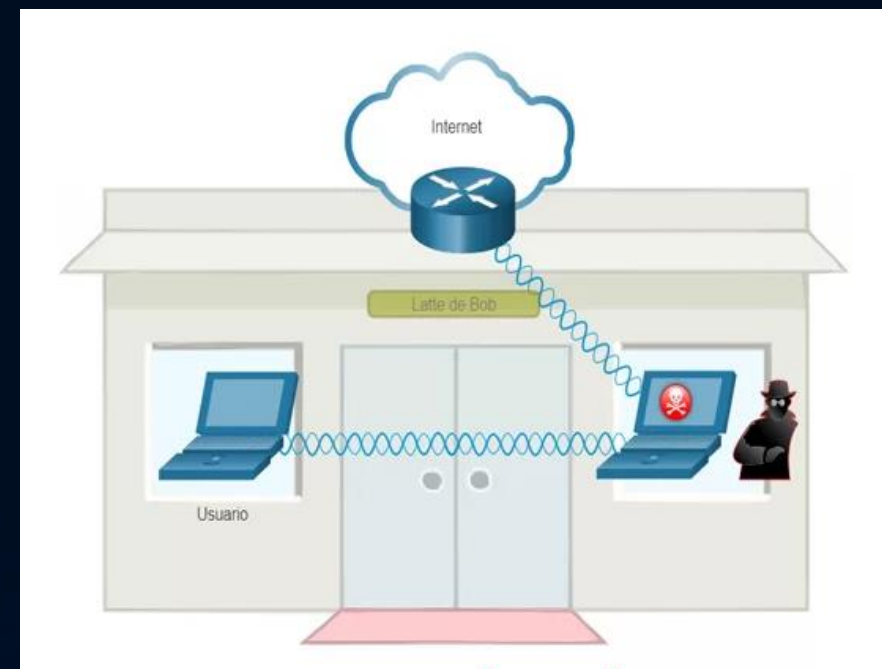
Redes Wi-Fi Públicas

Ameaças

Evil Twin

Um ataque evil twin ocorre quando um invasor configura um ponto de acesso Wi-Fi falso na esperança de que os usuários se conectem a ele em vez de um legítimo. Quando os usuários se conectam a esse ponto de acesso, todos os dados que compartilham com a rede passam por um servidor controlado pelo invasor.

Um invasor pode criar um evil twin com um smartphone ou outro dispositivo compatível com a Internet e algum software prontamente disponível. Ataques evil twin são mais comuns em redes Wi-Fi públicas que não são seguras e deixam seus dados pessoais vulneráveis.





Segurança na Rede Sem Fio

Redes Wi-Fi Públicas

Como funciona o Evil Twin

Etapa 1: Procurando o local certo

Os atacantes geralmente procuram locais movimentados com Wi-Fi gratuito e popular. Isso inclui espaços como cafeterias, bibliotecas ou aeroportos, que geralmente possuem vários pontos de acesso com o mesmo nome. Isso torna mais fácil para a rede falsa do hacker passar despercebida.

Etapa 2: Configurando um ponto de acesso Wi-Fi

O atacante então anota o Service Set Identifier (SSID) da rede legítima e configura uma nova conta com o mesmo SSID. Eles podem usar praticamente qualquer dispositivo para fazer isso, incluindo smartphones, laptops, tablets ou roteadores portáteis. Eles podem usar um dispositivo chamado Wi-Fi Abacaxi para obter um alcance mais amplo. Os dispositivos conectados não conseguem distinguir entre conexões genuínas e versões falsas.



Segurança na Rede Sem Fio

Redes Wi-Fi Públicas

Como funciona o Evil Twin

Etapa 3: Incentivando as vítimas a se conectarem ao Wi-Fi evil twin

O atacante pode se aproximar de suas vítimas para criar um sinal de conexão mais forte do que as versões legítimas. Isso convence as pessoas a selecionarem a rede dele em vez das mais fracas e força alguns dispositivos a se conectarem automaticamente.

Etapa 4: Configurando um portal cativo falso

Antes de entrar em muitas contas Wi-Fi públicas, você deve enviar dados em uma página de login genérica. Os atacantes evil twin criam uma cópia dessa página, na esperança de enganar as vítimas inocentes para que revelem suas credenciais de login. Uma vez que os atacantes as tenham, eles poderão fazer login na rede e controlá-la.



Segurança na Rede Sem Fio

Redes Wi-Fi Públicas

Como funciona o Evil Twin

Etapa 5: Roubando dados de vítimas

Qualquer pessoa que fizer login se conectará através da rede do atacante. Esse é um clássico ataque man-in-the-middle que permite ao invasor monitorar a atividade online da vítima, seja navegando pelas mídias sociais ou acessando suas contas bancárias. Suponha que um usuário faça login em qualquer uma de suas contas. Nesse caso, o hacker poderá roubar suas credenciais de login – o que é especialmente perigoso se a vítima usar as mesmas credenciais para várias contas.



Segurança na Rede Sem Fio

Redes Wi-Fi Públicas

Ponto de acesso não autorizado versus evil twin – qual é a diferença?

Um ponto de acesso não autorizado é um ponto de acesso ilegítimo conectado a uma rede para criar um desvio de fora para a rede legítima.

Por outro lado, um evil twin é uma cópia de um ponto de acesso legítimo. Seu objetivo é um pouco diferente: tenta atrair vítimas inocentes para se conectarem à rede falsa para roubar informações.

Embora não sejam iguais, um evil twin pode ser considerado uma forma de ponto de acesso desonesto.

Segurança na Rede Sem Fio

Aparelhos Móveis

Os aparelhos móveis, como os smartphones (telefones inteligentes) ou tablets são muito úteis, porque com eles podemos nos conectar à Internet em praticamente qualquer lugar com um plano de dados ou através de redes wifi.

Basicamente, os usamos como um computador, onde lemos notícias, vemos vídeo, verificamos e-mails, entre outros. Assim, se manter seguro com este tipo de aparelhos é muito importante.





Segurança na Rede Sem Fio

Aparelhos Móveis - Ameaças

Tela de Bloqueio desprotegida:

Se alguém roubar o smartphone ou se você perdê-lo e acabar caindo em mãos de estranhas, pode estar em problemas caso não tenha colocado uma senha forte para acessá-lo, isso porque imediatamente todas as suas informações pessoais estarão nas mãos de um estranho.

Malwares:

Estes software maliciosos podem estar em games, mensagens de texto, e-mails, entre outros, e atacar o sistema do computador para transferir ou alterar arquivos, extrair informações financeiras, instalar outros programas, etc.

Outro tipo de malware são os anúncios publicitários que aparecem em aplicativos gratuitos e que podem chegar a acessar as configurações do telefone e extrair o número de identificação do telefone (IMEI), acessar as chamadas, entre outros. Ao instalar aplicativos, verificar e as permissões que pedem para serem instaladas.



Segurança na Rede Sem Fio

Aparelhos Móveis - Ameaças

Roubo de informações via Bluetooth

Quando Bluetooth ligado há o risco de que alguém próximo se conecte e acesse o telefone usando um pareamento bluetooth. O uso de PIN deve ser considerado como obrigatório, mas ainda assim algumas versões apresentam falhas.

As falhas estão contidas na infraestrutura do Bluetooth 4.2 até a versão 5.4. O padrão foi inaugurado em dezembro de 2014, então afeta uma enorme quantidade de aparelhos, incluindo iPhones, celulares Android modernos, tablets e computadores. Os pesquisadores explicam que as táticas exploram quatro falhas no processo de derivação da chave de sessão, forçando a criação de chave mais curta, mais fraca e acessível.

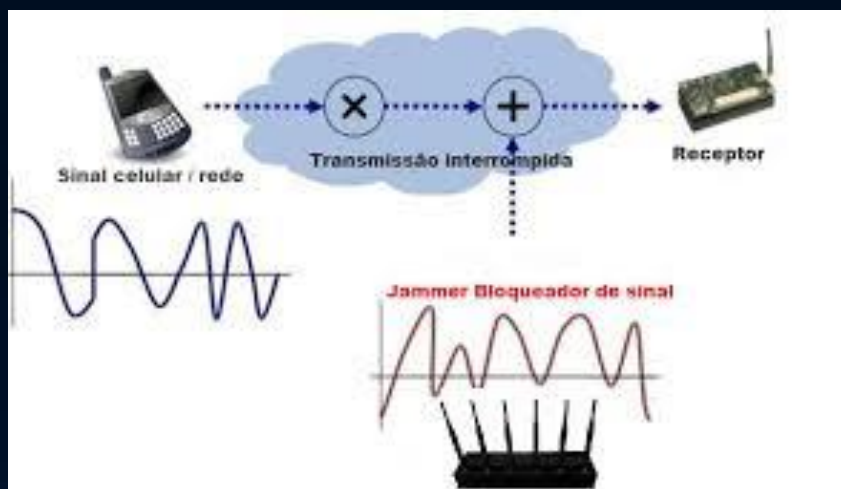
Em termos práticos, é como se o dispositivo fosse induzido a usar uma chave de segurança mais simples e fácil de descobrir. Então, o invasor pode usar um método de força bruta até descobrir a sequência e sequestrar a conexão.

Segurança na Rede Sem Fio

Aparelhos Móveis - Ameaças

Jamming

Jamming, também conhecido como interferência intencional, é uma técnica usada para interromper ou interferir em comunicações sem fio, incluindo redes Wi-Fi, celulares e outros sistemas de rádio. O objetivo do jamming é causar um alto nível de interferência ou ruído no sinal de transmissão para torná-lo inutilizável ou difícil de ser decodificado.





Segurança na Rede Sem Fio

Aparelhos Móveis - Ameaças

Jamming - destrutivo e construtivo

Jamming - Existem dois tipos principais de jamming: destrutivo e construtivo.

O jamming destrutivo envolve a transmissão de um sinal forte e constante na mesma frequência usada pela rede ou dispositivo que está sendo alvo. Isso pode sobrecarregar o receptor e tornar o sinal original inutilizável.

O jamming construtivo, por outro lado, envolve a transmissão de um sinal que imita o sinal original, mas com informações maliciosas inseridas nele, o que pode levar a erros ou mau funcionamento do sistema que recebe o sinal.

FIM