CMSec
Conscious Mind & Security

SEGURANÇA EM REDES SEM FIO

Atanaí Ticianelli - Diretor
atanai@cmsec.com.br
www.cmsec.com.br

APRESENTAÇÕES

- Eu
- A CMSec
  Mente e Segurança Conscientes
- Vocês

Redes sem fio

Ouvido
(LF 20Hz a 20KHz)

Rádio AM
(MF 300KHz a 3MHz)

Rádio FM
Telefone SF
Ctrl Garagem
(VHF 30MHz a 300MHz)

Infravermelho
(300GHz a 400THz)

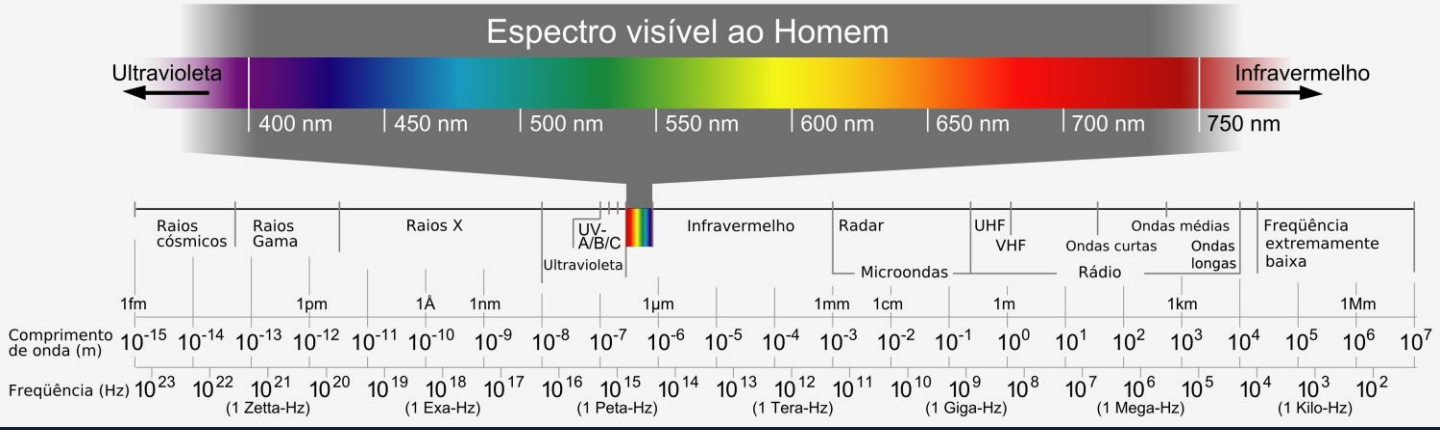
Satélites
(EHF 30GHz a 300GHz)

WLAN a
(SHF 5GHz)

1G-4G, Bluetooth,
WLAN, TV Digital
(UHF 300MHz a 3GHz)

CMSec
Conscious Mind & Security

PAUTA DE HOJE



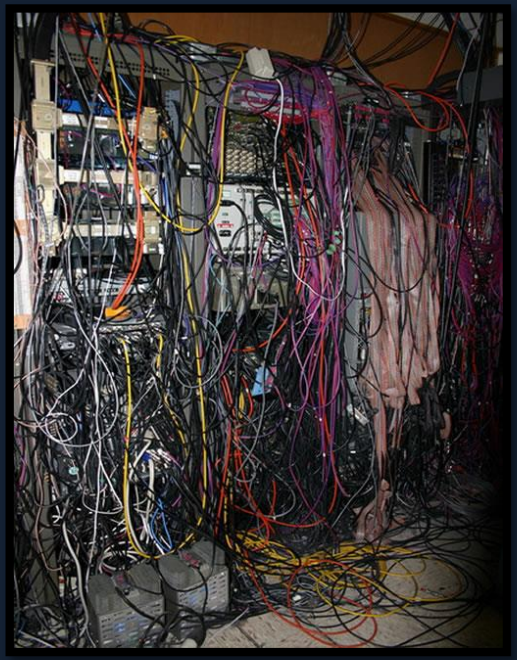
Redes sem fio

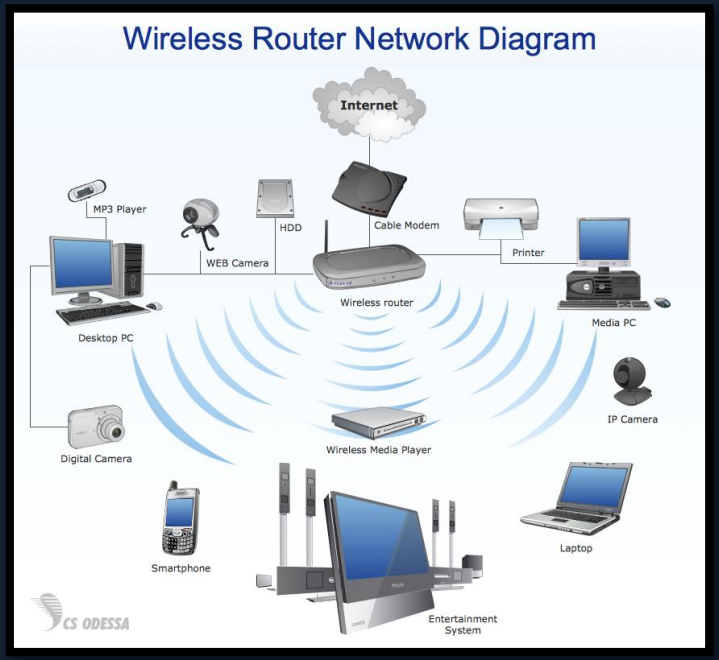
Como construir uma BTS GSM portátil, de baixo custo

https://iopub.org/phreaking-is-alive-14c7ec37d787#.iz9dq0oez

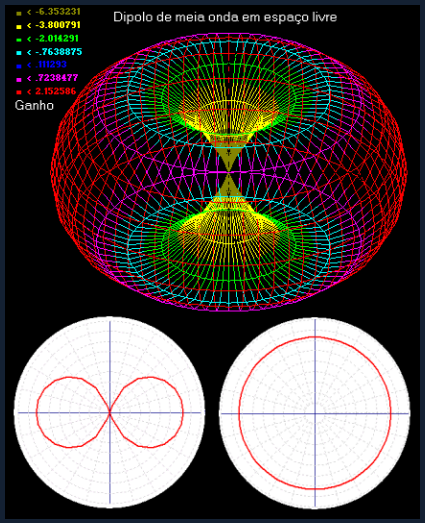
2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf

Escolha agora

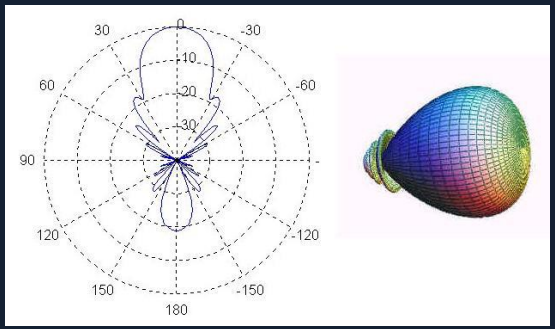




Omnidirecional



Semi-direcional



Direcional

Rede Local sem Fio

Especificada no padrão 802.11 criado pelo IEEE
Institute of Electrical and Electronics Engineers

Camada física e Controle de Acesso ao Meio sem fio

Regulamentação de frequências:
Federal Communications Commission (FCC)
Agência Nacional de Telecomunicações (Anatel)

Wi-Fi Alliance: WPA/WPA2

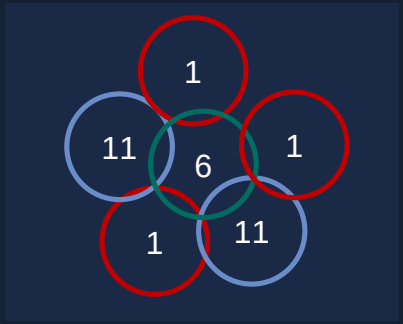
802.11 – Padrões principais

802.11	2.4 GHz
802.11a	54 Mbps a 5 GHz
802.11b	11 Mbps a 2.4 GHz
802.11g	54 Mbps a 2.4 GHz
802.11n	600 Mbps a 2.4 e 5 GHz
802.11ac	1 Gbps a 5 GHz
802.11i	Melhorias na segurança
802.1X	Controle de Acesso a Redes baseado em Portas

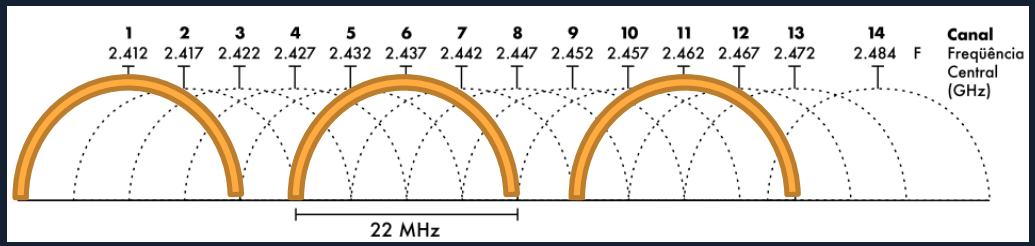
.
.
.
(~20)

CANAIS A 2.4 GHZ

- 22 MHz de largura por canal
- Canais 1, 6 e 11 sem interseção
- Canais 1, 5, 9 e 14 interseção mínima



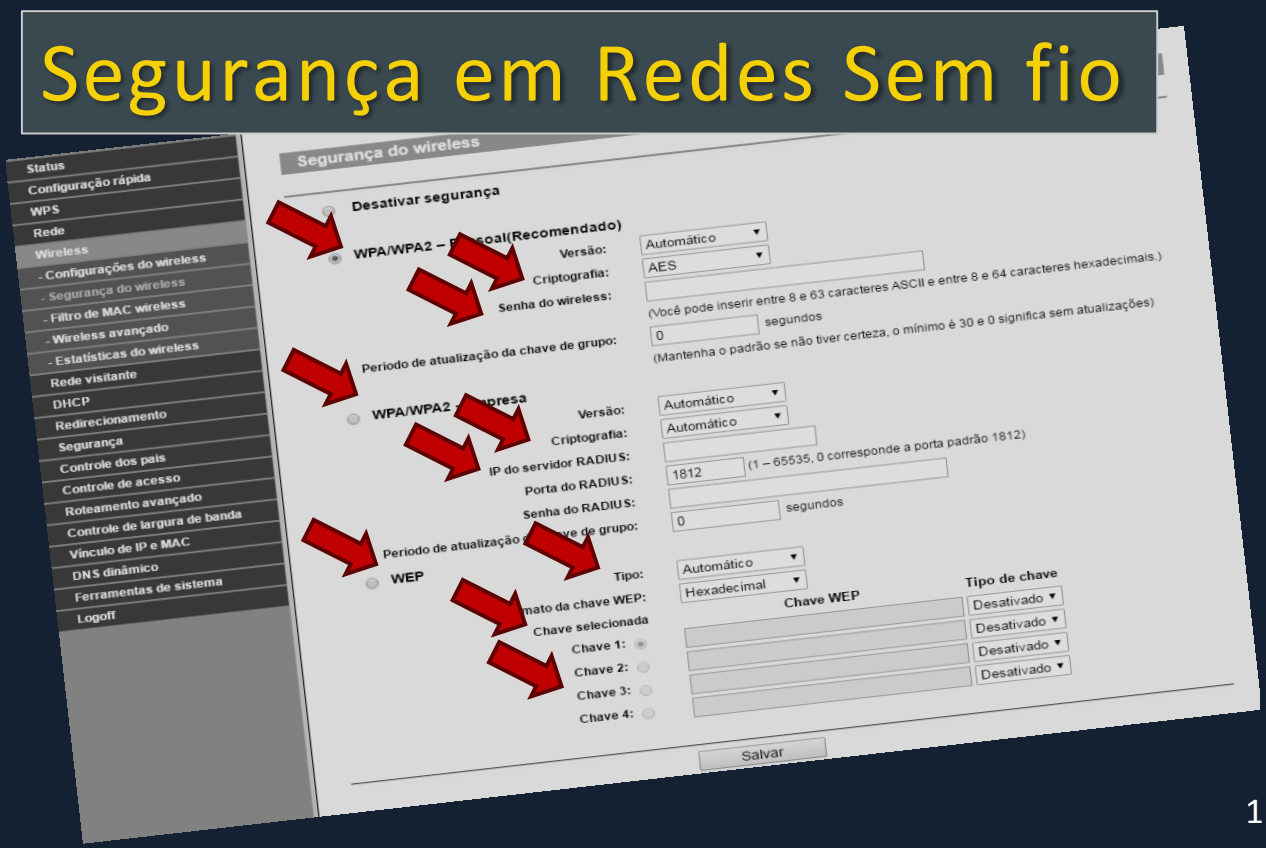
Canal	Freq. Início	Freq. Central	Freq. Fim
1	2.401	2.412	2.423
2	2.406	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.446	2.457	2.468
11	2.451	2.462	2.473
12	2.456	2.467	2.478
13	2.461	2.472	2.483
14	2.466	2.477	2.488



Direct Sequence Spread Spectrum (DSSS)

CMSec
Conscious Mind & Security

Segurança em Redes Sem fio

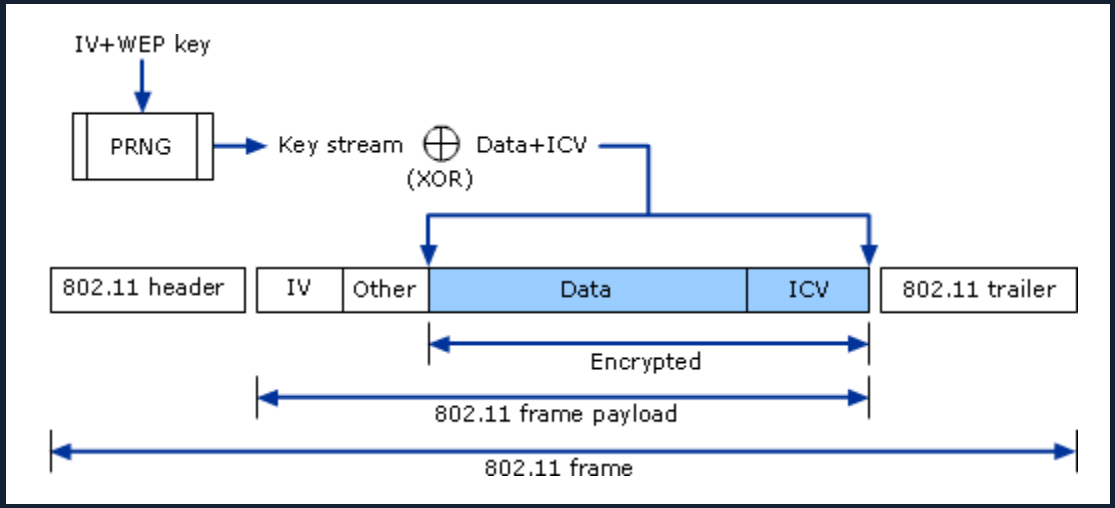


Wired Equivalent Privacy

- Presente na versão original do 802.11 (1997)
- Camada enlace (MAC)
- Integridade e Confidencialidade dos dados
- Autenticação do cliente
- Chaves de 64 e 128 bits

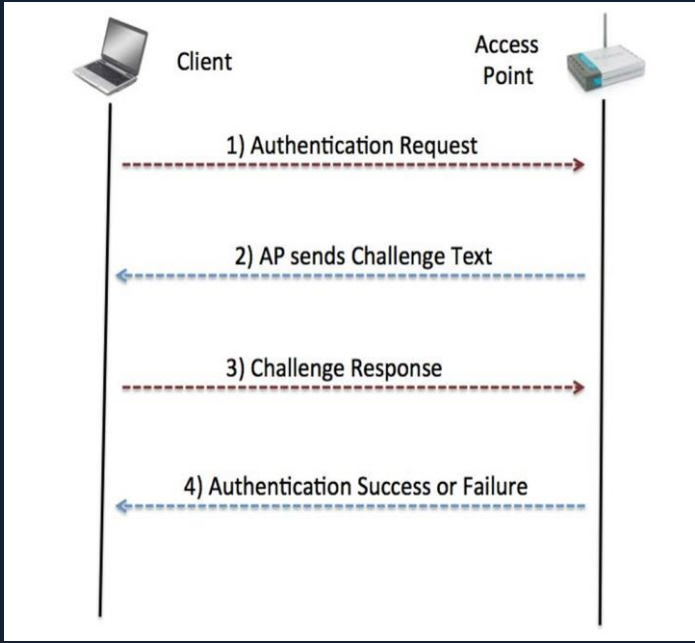
Cifragem dos dados

Stream cipher RC4 (PRNG)



https://technet.microsoft.com/pt-br/library/cc757419(v=ws.10).aspx

Autenticação



Vetor de Inicialização (IV) pequeno

- 24 bits (16.777.215 possibilidades)
- Novo IV a cada pacote
- 5.000 pacotes: possibilidade de repetição do IV

Quebra de senha da chave é trivial

- Gerar grande número de pacotes
- aircrak-ng

Wi-Fi Protected Access

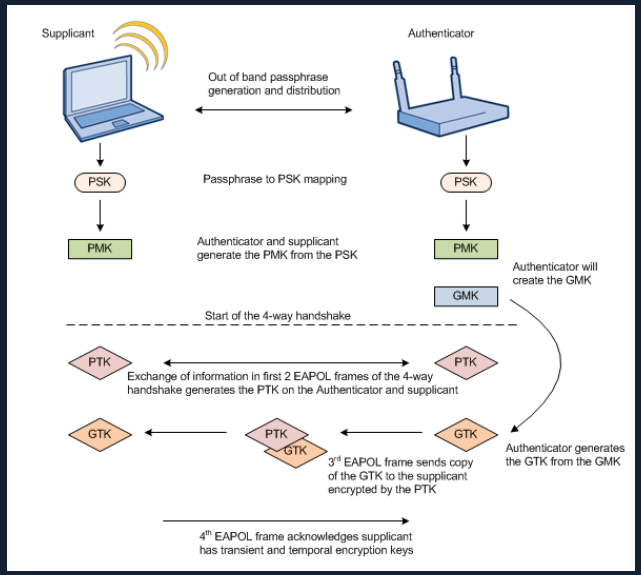
- Solução imediata da Wi-Fi Alliance para o WEP: WPA
- 2004: 802.11i – Robust Security Network – WPA2
- WPA-TKIP (Temporal Key Integrity Protocol)
- WPA2-AES (Advanced Encryption Standard)

Mecanismos implantados no WPA

- WPA-PSK (pre-shared key)
- WPA-Enterprise (RADIUS)
- Wi-Fi Protected Setup (WPS)

Autenticação

- 4 way handshake (802.1x EAPOL)



VULNERABILIDADES WPA/WPA2

WPA – TKIP

- 4 way handshake (necessitava de QoS ativo - Beck-Tews)

WPA/WPA2

- Senhas fracas – ataques de dicionário
- Engenharia social

WPA2 – WPS (Wi-FI Protected Setup)

- Opção de PIN ou botão físico ao invés da senha da rede
- PIN 8 bits, checagem de 4 em 4: 11.000 opções de força-bruta
- Acesso ao botão WPS permite autenticar

CMSec
Conscious Mind & Security

OUTROS TIPOS DE ATAQUE

Redes wi-fi abertas

- Vazamento de dados
- Ataques MiTM + SSL
- Rougue AP
  DNS – Páginas falsas

OUTROS TIPOS DE ATAQUE

Redes wi-fi

- Filtragem por MAC ADDRESS
- DoS – Deauth attacks
- Potência de rádio
- Redes abertas salvas

www.wifipineapple.com

Amanhã: Hands-ON !

1. Redes abertas
2. Filtragem por MAC
3. Quebra WEP
4. Bruteforce WPA
5. Engenharia social WPA

CMSec
Conscious Mind & Security

Obrigado!

Atanaí Ticianelli
atanai@cmsec.com.br