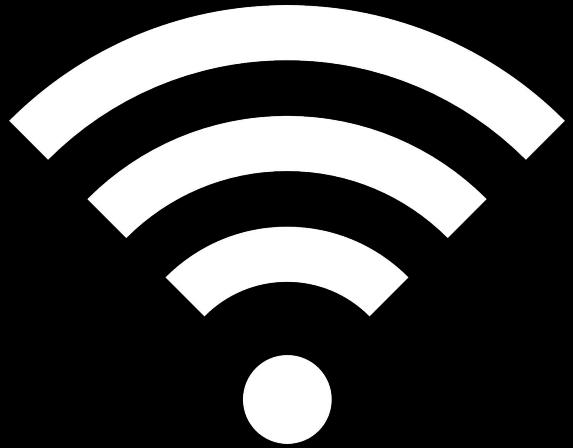
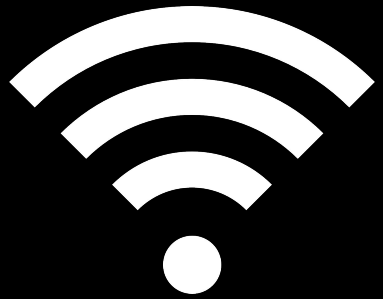
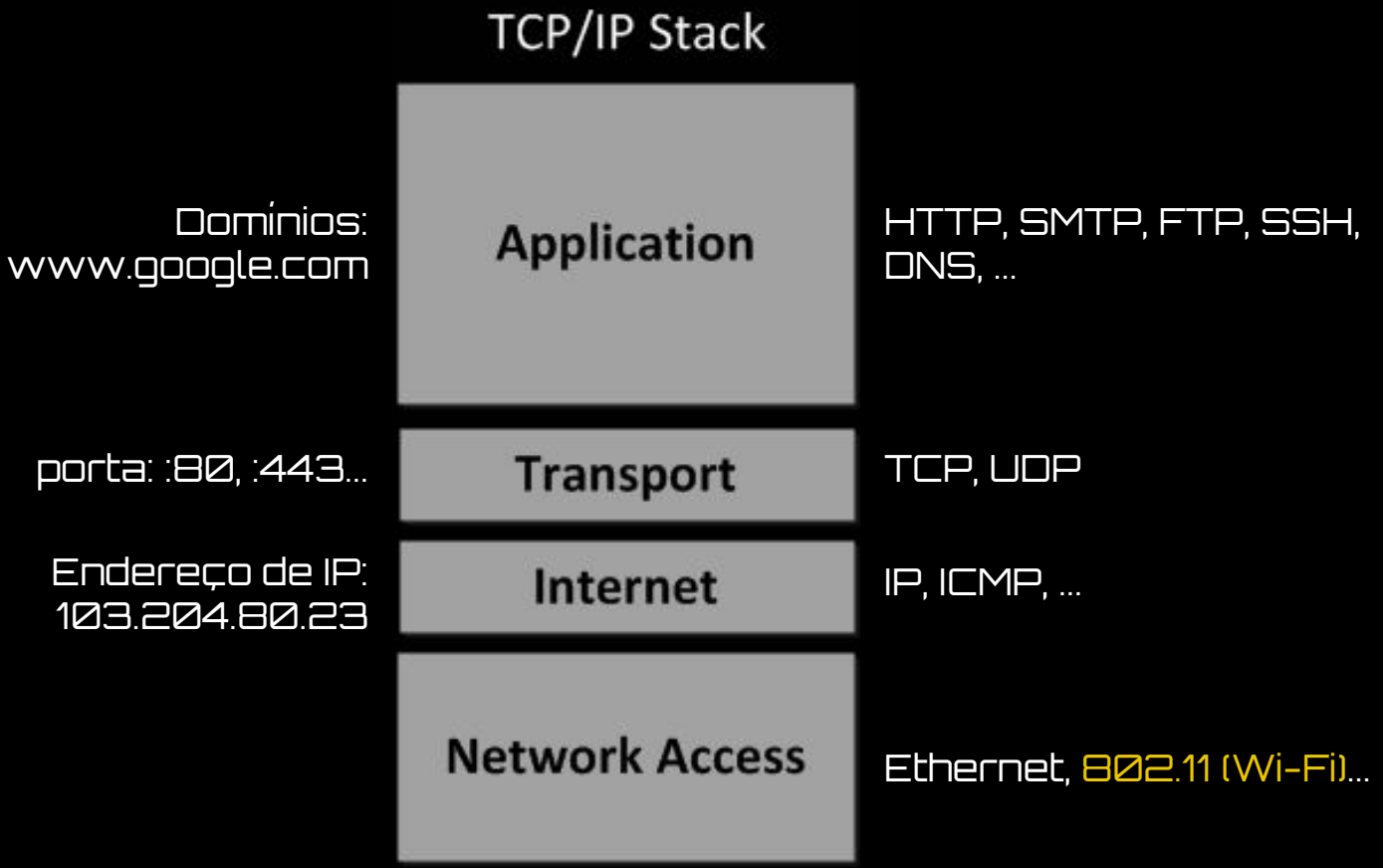


Palestra 3 - 09/05

IMEsec

O que é o Wi-Fi?




TCP/IP Stack
Domínios:
www.google.com
Application
HTTP, SMTP, FTP, SSH,
DNS, ...
porta: :80, :443...
Transport
TCP, UDP
Endereço de IP:
103.204.80.23
Internet
IP, ICMP, ...
Network Access
Ethernet, 802.11 (Wi-Fi)...

Propriedades da Wi-Fi

Propriedades da Wi-Fi

- Requer Hardware especial (roteador, ponto de acesso)

Propriedades da Wi-Fi

- Requer Hardware especial (roteador, ponto de acesso)
- Protocolo de proximidade

Propriedades da Wi-Fi

- Requer Hardware especial (roteador, ponto de acesso)
- Protocolo de proximidade
- Possibilita camadas acima (protocolo IP)

Propriedades da Wi-Fi

- Requer Hardware especial (roteador, ponto de acesso)
- Protocolo de proximidade
- Possibilita camadas acima (protocolo IP)
- Mas não necessariamente - é possível se conectar a um roteador sem se conectar à internet

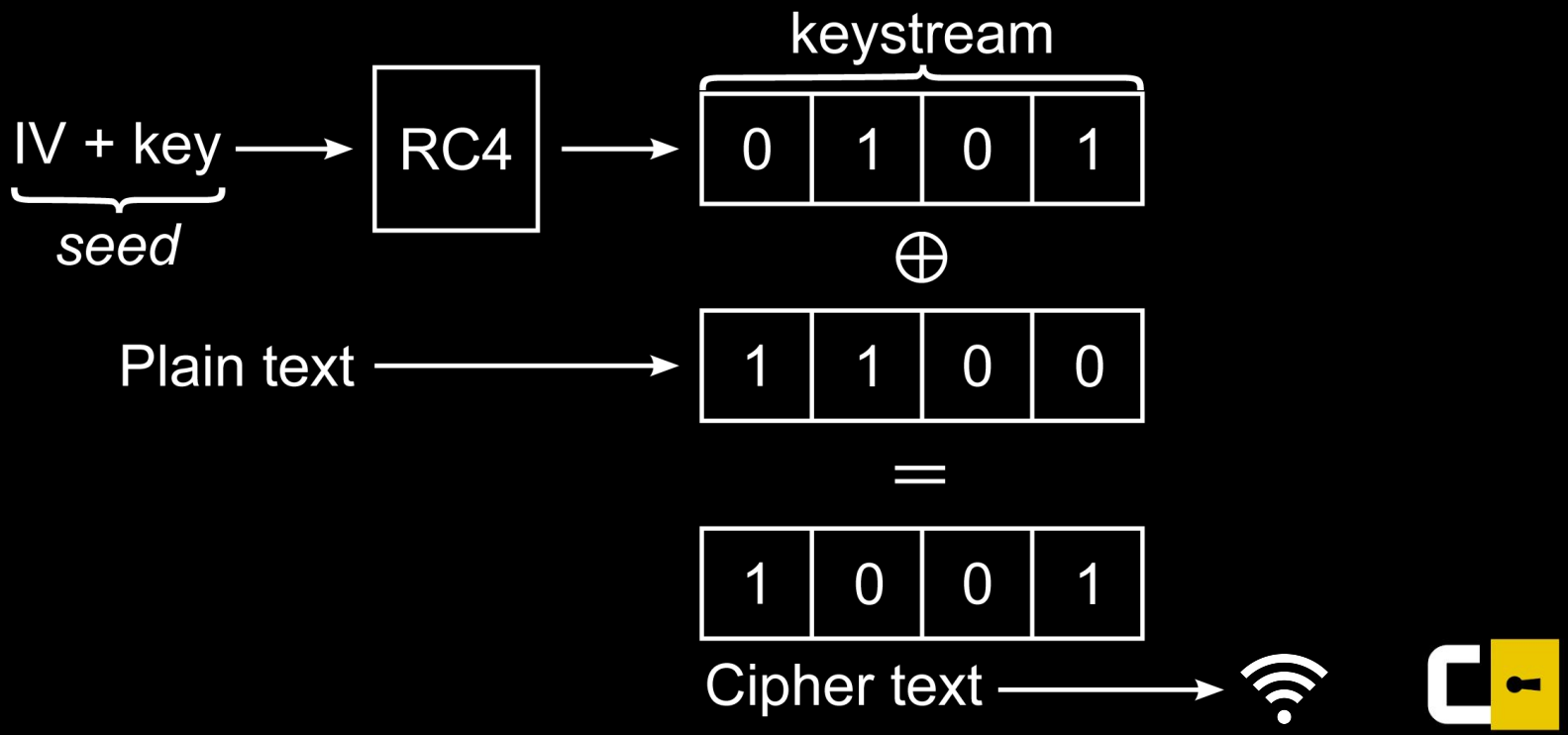
Mas e a segurança?

Wired Equivalent Privacy

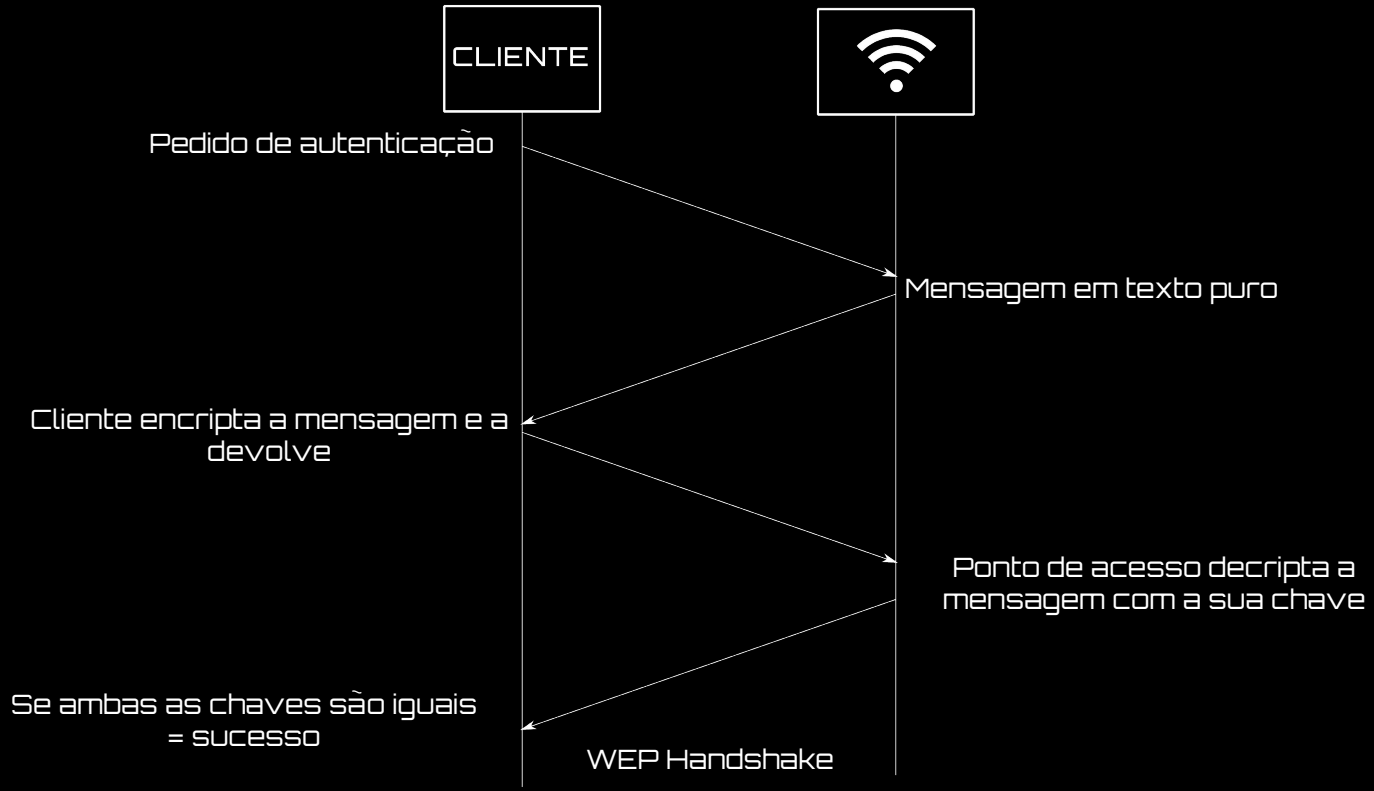
WEP

Objetivo: Prover o mesmo nível de segurança de uma conexão cabeada tradicional.

Wired Equivalent Privacy



Wired Equivalent Privacy



Wired Equivalent Privacy

Mas tem um problema....

Wired Equivalent Privacy

Mas tem um problema....

WEP é quebrado!

Então surgiu....

Wi-Fi Protected Access

WPA

Objetivo: Resolver aquele monte de problemas do WEP

Wi-Fi Protected Access

WPA

Como?

Wi-Fi Protected Access

WPA

Como?

Através do Temporal *Key Integrity Protocol (TKIP)*, onde cada pacote enviado tem uma chave diferente

Wi-Fi Protected Access

WPA

Como?

Através do Temporal *Key Integrity Protocol (TKIP)*, onde cada pacote enviado tem uma chave diferente

E também de um *handshake* mais seguro (PSK)

Wi-Fi Protected Access

WPA

Features novas:
WPS
WPA-Enterprise

WPA-Personal vs. WPA-Enterprise

Enterprise - login e senha para cada pessoa

Personal - senha única para todo mundo

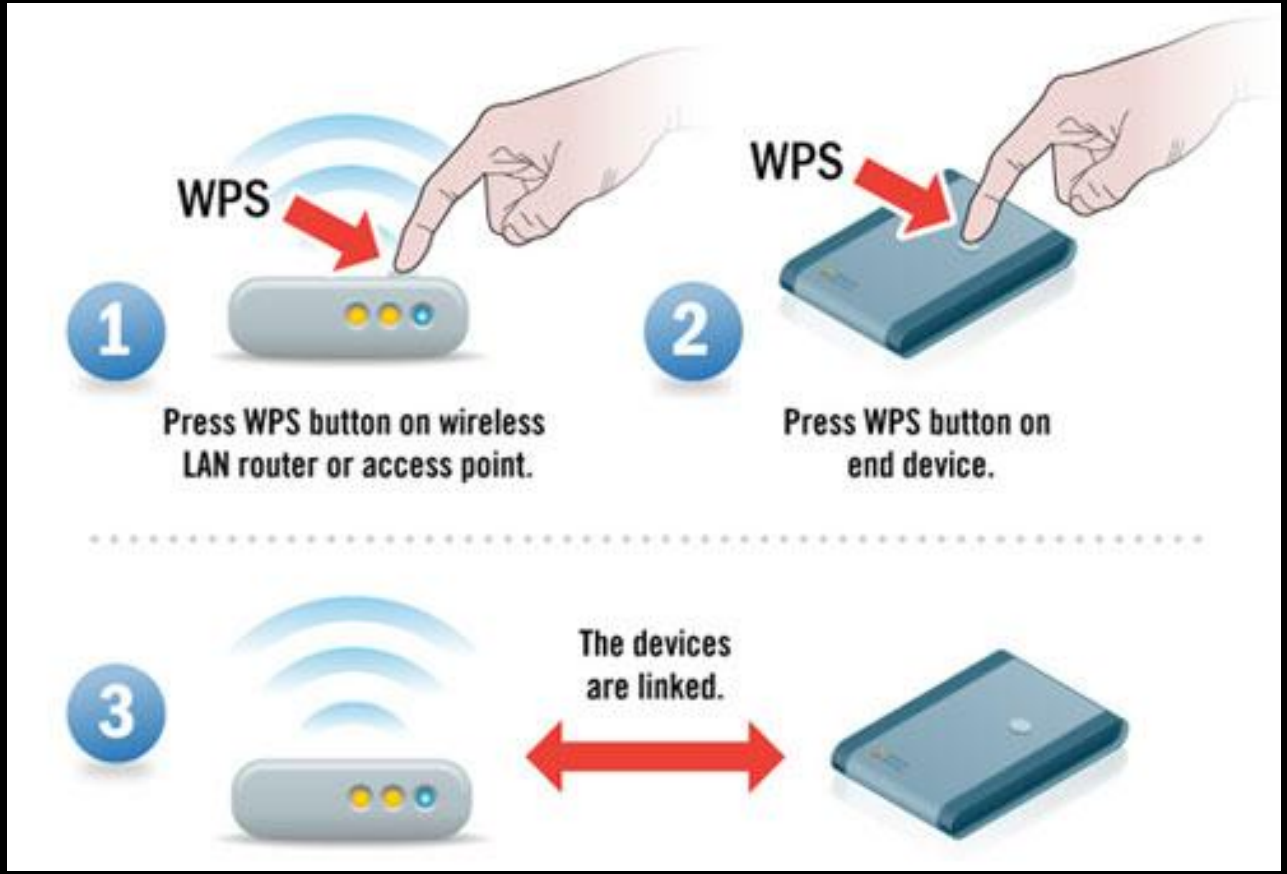
WPA-Personal vs. WPA-Enterprise

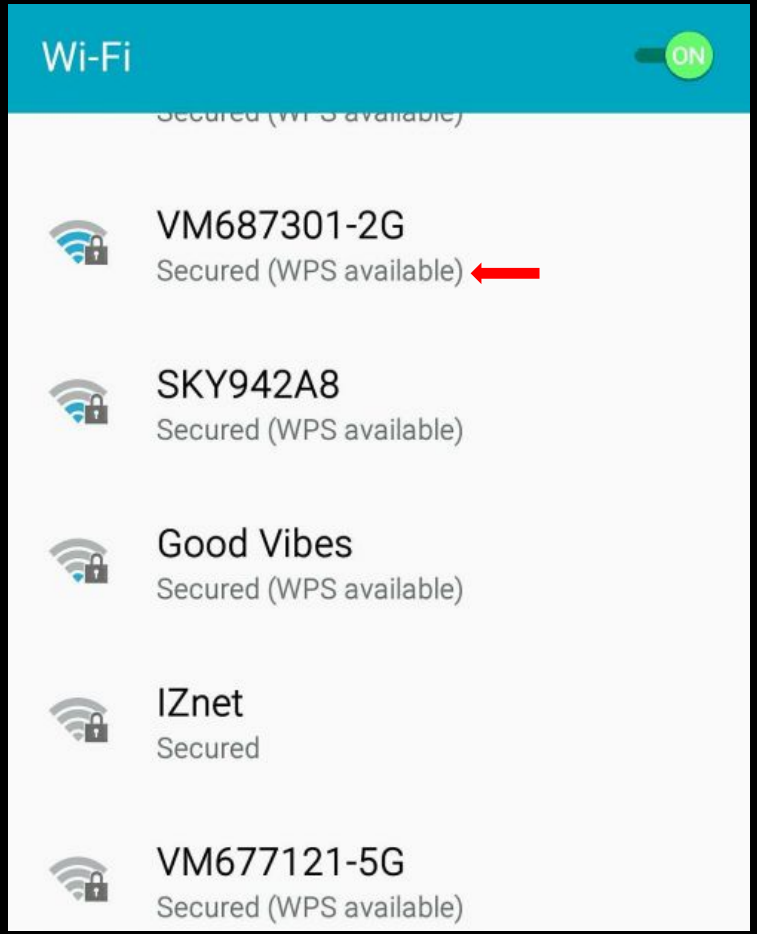
Enterprise - login e senha para cada pessoa

Personal - senha única para todo mundo

Enterprise - senha é vazada: desativa a conta e segue a vida

Personal - senha é vazada: é preciso trocar a senha de todo mundo


WPS
1
Press WPS button on wireless LAN router or access point.
WPS
2
Press WPS button on end device.
3
The devices are linked.


Wi-Fi
ON
VM687301-2G
Secured (WPS available)
SKY942A8
Secured (WPS available)
Good Vibes
Secured (WPS available)
IZnet
Secured
VM677121-5G
Secured (WPS available)

E isso resolveu tudo?

E isso resolveu tudo?

NÃO!

Wi-Fi Protected Access 2

WPA2

Protocolo atualizado com criptografia AES.

Wi-Fi Protected Access 2

WPA2

Protocolo atualizado com criptografia AES.

Utiliza um *handshake* similar ao WPA (PSK)

Isso sim resolveu tudo, né?

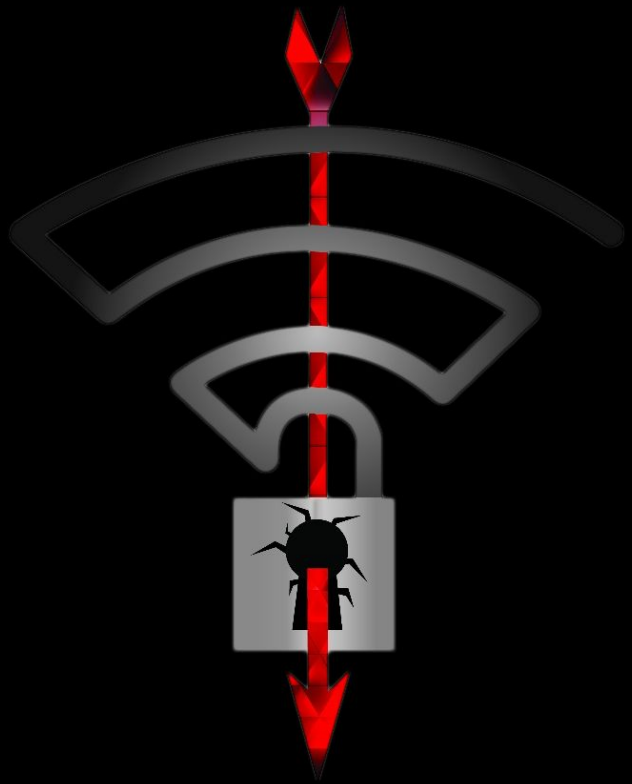
Isso sim resolveu tudo, né?

Claro

Isso sim resolveu tudo, né?

Claro que **NÃO**

Exemplo de exploit de WPA2



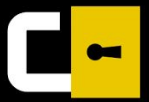
Wi-Fi Protected Access 3

WPA3

Anunciado em Janeiro de 2018, visa resolver esses problemas do WPA2.

E como funciona isso na prática?

Aircrack-ng



E como eu faço pro meu Wi-Fi não ser hackeado?

E como eu faço pro meu Wi-Fi não ser hackeado?

- Use uma senha

E como eu faço pro meu Wi-Fi não ser hackeado?

- Use uma senha
- Use senhas fortes (idealmente longas, com palavras incomuns e símbolos)

E como eu faço pro meu Wi-Fi não ser hackeado?

- Use uma senha
- Use senhas fortes (idealmente longas, com palavras incomuns e símbolos)
- Não use WEP

E como eu faço pro meu Wi-Fi não ser hackeado?

- Use uma senha
- Use senhas fortes (idealmente longas, com palavras incomuns e símbolos)
- Não use WEP
- Não use WPS

E se eu já tiver a senha do Wi-Fi, o que posso fazer?

Parte 2 - 24/05

Obrigado!

DISCLAIMER: Conteúdo apenas para fins educacionais