Redes sem Fio: uma introdução

Prof. Felipe Oliveira

fdoprof@gmail.com

Ameaças Wireless

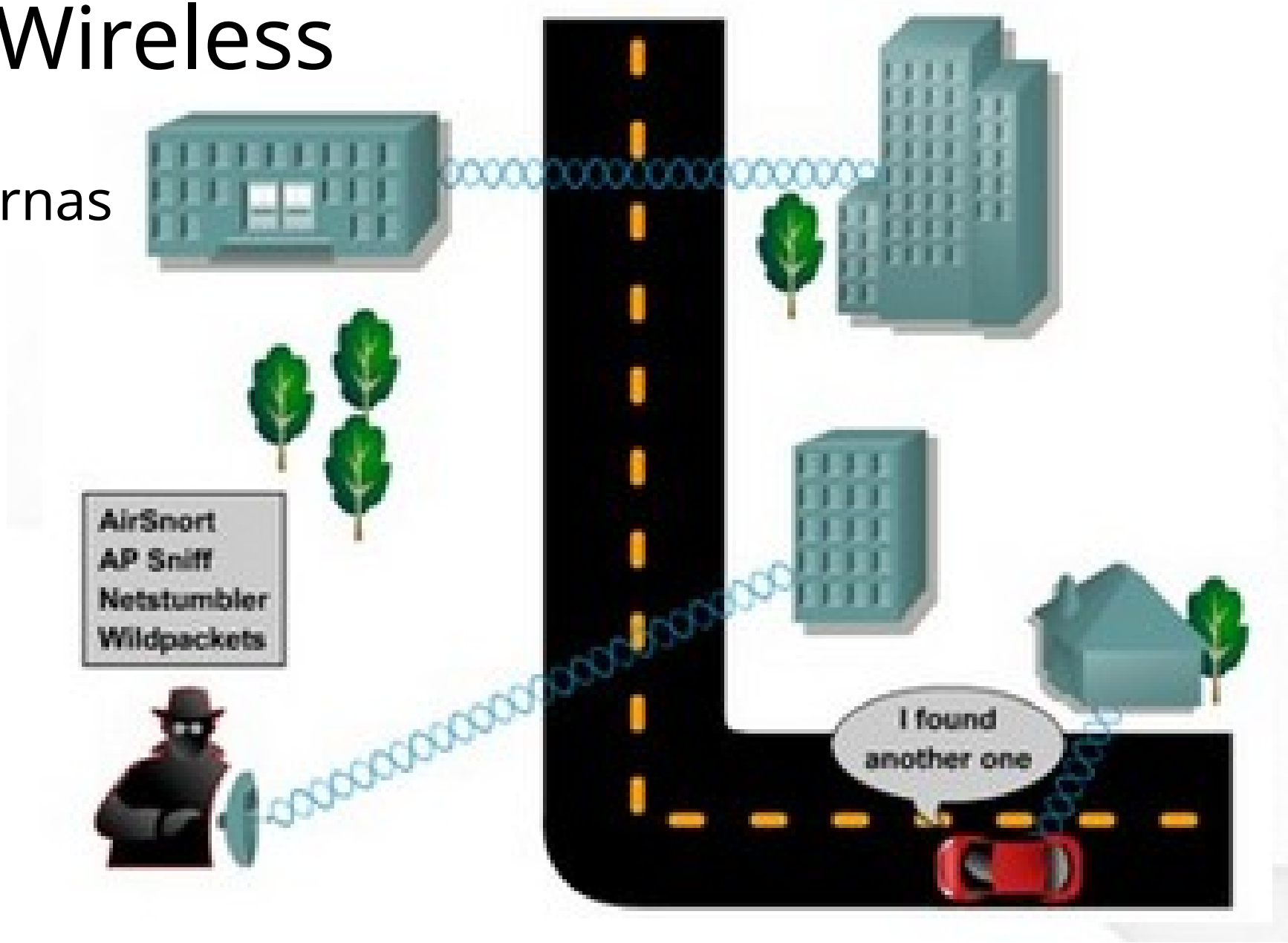
- Ameaças Externas
  - Hackers criam um **modo para invadir a rede principalmente fora das edificações**, tais como estacionamentos, construções próximas ou áreas comuns.

Ameaças Wireless

- Ameaças Externas

Ameaças Wireless

- Ameaças Externas



O que um hacker faz exatamente?

- Metodologia básica dos ataques às redes sem fio
- Podem ser divididos em 3 categorias:
  1. Reconhecimento
  2. Ataque de acesso
  3. Negação de Serviço (DoS)

Reconhecimento

- É o descobrimento não autorizado e o mapeamento de sistemas, sinais
- Conhecido como coleta de informações
- Precede a tentativa de acesso ou ataque DoS
- Similar ao ladrão rondando a vizinhança
- Em segurança de redes sem fio, o reconhecimento é chamado de *wardriving* ou *warchalking*.

R

- E
- C
- F
- S
- E

Reconhecimento

- Sugestão de Vídeo:

Projeto War Driving Day:

Acesso

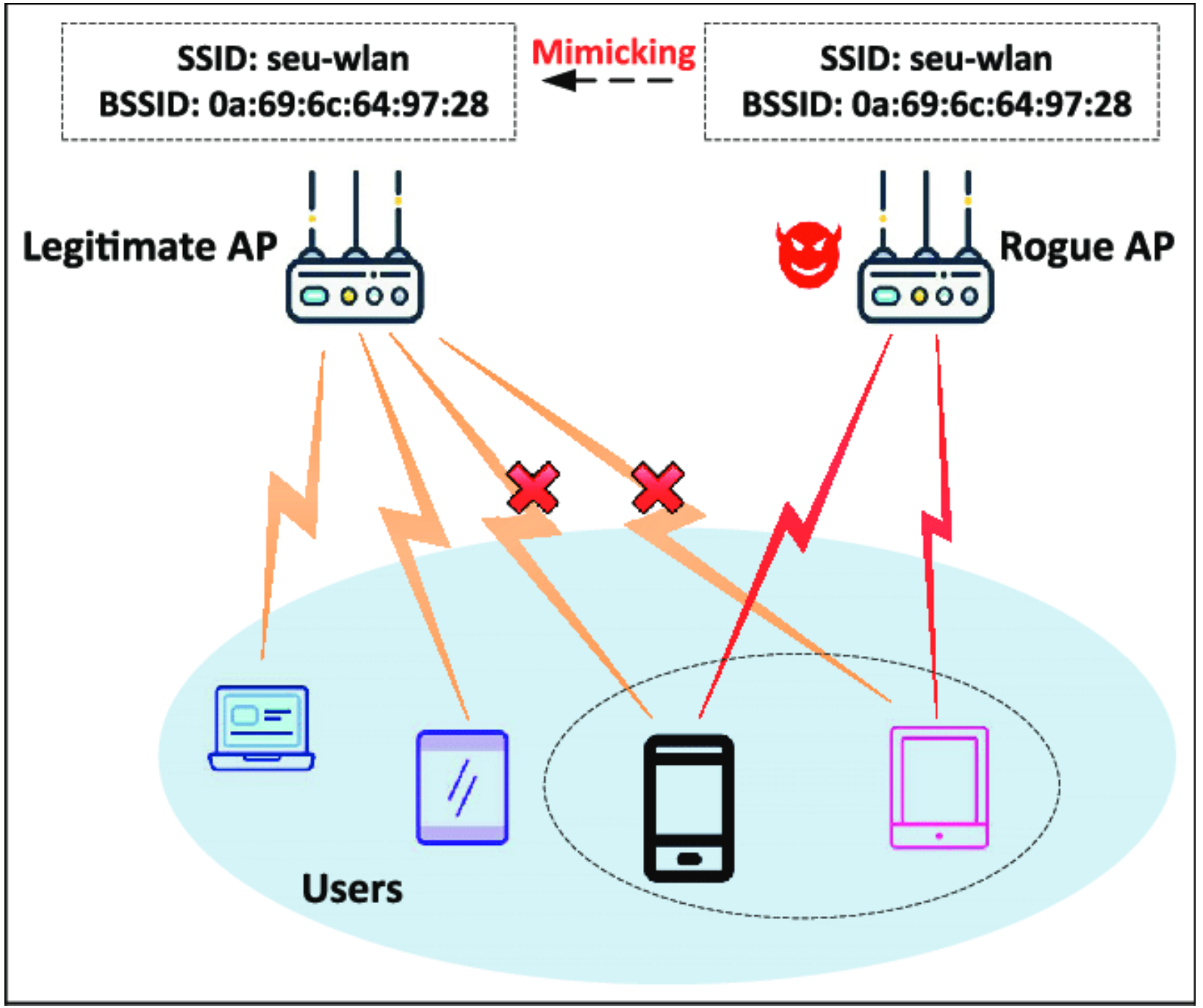
- Sistemas de acesso e/ou intrusão trazem a habilidade para um intruso não autorizado ganhar acesso ao dispositivo ao qual não tem permissão.
- Geralmente envolve processar um script ou ferramentas de exploração de vulnerabilidades conhecidas
- Incluem:
  - Exploração de senhas fracas ou inexistentes;
  - Exploração de serviços (HTTP, FTP, Telnet, etc)
  - Engenharia social.
- São práticas ilegais.

Acesso

- Sistemas de acesso e/ou intrusão trazem a habilidade para um intruso não autorizado ganhar acesso ao dispositivo ao qual não tem permissão.
- Geralmente envolve processar um script ou ferramentas de exploração de vulnerabilidades conhecidas
- Incluem:
  - Exploração de senhas fracas ou inexistentes;
  - Exploração de serviços (HTTP, FTP, Telnet, etc)
  - Engenharia social.
- São práticas ilegais.

Acesso

- Ataque rogue AP



Negação de Serviço (DoS)

- DoS ocorre quando um atacante desabilita ou corrompe a rede wireless, sistemas ou serviços com a intenção de negar os serviços a usuários autorizados
- Ataques DoS podem ter várias formas
- Na maioria das vezes envolve apenas rodar um script ou utilizar uma ferramenta.

Negação de Serviço (DoS)

- Interferência intencional
  - Frequência 2.4GHz possui apenas 3 canais não sobrepostos, com isso canais 802.11b/g e n em 2.4GHz são especialmente suscetíveis a este tipo de ataque.

Negação de Serviço (DoS)

Ataques adicionais

- Man-In-The-Middle
- MAC Spoofing
  - Explora fraquezas no filtro de endereços MAC.
- Engenharia Social.

Dúvidas?