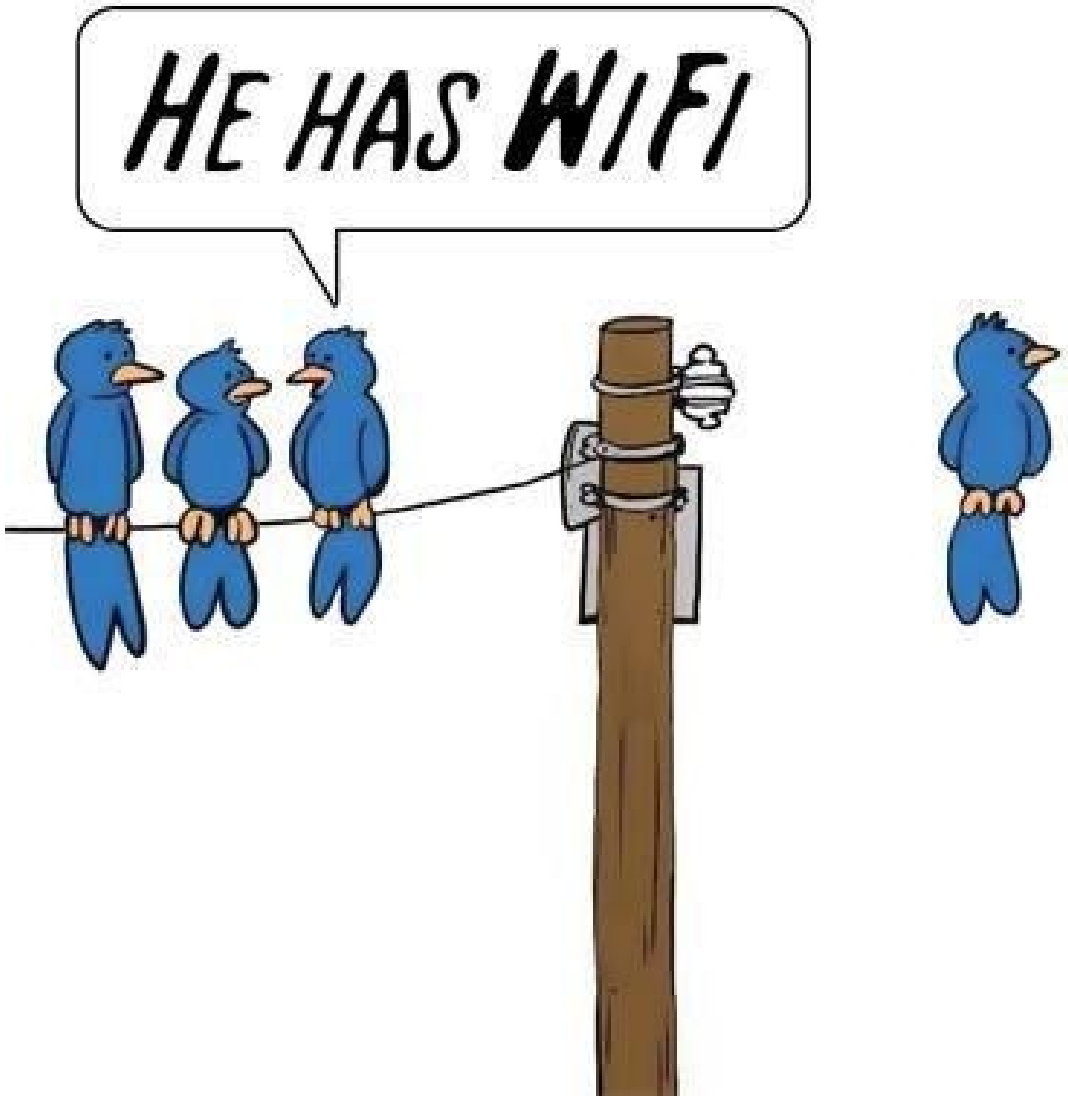
# Redes sem Fio: Uma Introdução

Prof. Felipe Oliveira

fdoprof@gmail.com

# Agenda

- Redes Cabeadas
- Redes sem fio
- Tecnologias de redes sem fio
  - Família 802.11
- Principais aplicações de redes sem fio
  - Facilidade de utilização
  - Redução de custos


HE HAS WIFI

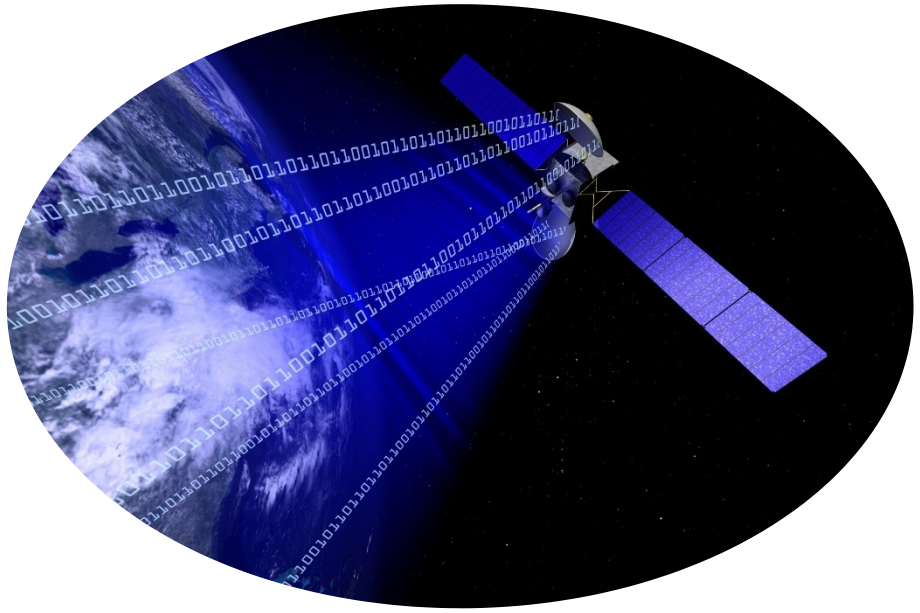
# Redes de Computadores

- As tecnologias de redes cabeadas e sem fio se desenvolveram de forma paralela
- Anos 50: Primeira utilização de protocolos de redes e as primeiras transmissões extraterrestres (Satélite SPUTNIK)
- Anos 60: Aparecimento das primeiras redes de computadores até a ARPANET
- Anos 70: Tecnologia Ethernet e o crescimento da utilização de redes locais – Berkeley

# Redes de Computadores

- Barateamento das soluções de conectividade
- Atualmente: utilização massiva das redes locais em empresas e instituições de ensino de todos os segmentos

# Redes de Computadores



- Surgimento das transmissões sem fio
  - Transmissões por ondas de rádio, radar
- Maior comodidade, porém maior custo
  - Equipamentos de conectividade até 20 vezes mais caros que os de redes cabeadas
- Princípio de segurança das redes sem fio, equivalente as cabeadas – WEP
  - Método falho desde sua concepção
- A segurança física das redes cabeadas
  - É necessário acesso ao meio físico ao meio de transmissão
- Ar como meio físico de transmissão
  - Qualquer equipamento receptor no alcance de transmissão tem acesso ao tráfego

# Redes de Computadores

- Surgimento e popularização do Celular
  - Barateamento de soluções de conectividade sem fio
  - Crescimento da demanda por mobilidade
- Em 2003 nos EUA, pela primeira vez, as vendas de Notebooks superam as de Desktops
- Redes sem fio aparecem hoje tanto em empresas como residências

# A Família IEEE 802.11


- Originalmente conhecida como 802.11
  - Trafega a velocidades de 1 e 2 Mbps
  - Na faixa de 2.4GHz (FHSS e DSSS)
- Seguida pelas extensões:
- 802.11a
  - 54 Mbps, faixa 5GHz (OFDM)
- 802.11b (Wi-Fi)
  - Desde 11 Mbps a 1 Mbps dependendo da potência do sinal, faixa de 2.4GHz(DSSS)
- 802.11g
  - 54Mpbs, 2.4GHz, (OFDM e DSSS por compatibilidade)

# Principais Aplicações

- Representa a área de conectividade que se desenvolve com maior velocidade
  - Facilidade de instalação/configuração mesmo para não-técnicos
  - Substituição de soluções de enlaces de dados antes restritos a redes cabeadas
  - Escalabilidade, desde PDA’s e notebooks até grandes enlaces de dados
  - Surgimento de novas interações entre dispositivos, criando novas oportunidades de serviços
    - Redes de sensores
    - Monitoramento remoto
    - Etc.

# Vulnerabilidades WLAN

- Redes sem fio são vulneráveis a ataques especializados:
  - Exploram fraquezas na tecnologia
  - WLAN 802.11 recebe ataques desde que o atacante esteja no perímetro de alcance
  - Redes cabeadas é possível estabelecer um perímetro de defesa
  - Má configuração, configuração incompleta e os próprios usuários

# Segurança?

**Segurança da informação** refere-se a garantir que os usuários **possam realizar apenas** as tarefas que eles estão **autorizados a fazer** e acessar apenas a informação à qual eles estão **autorizados a ter.**

# Principais desafios

- Novas tecnologias = novas ameaças
- Nem tudo são flores
  - WEP falho em qualquer tamanho de chave
  - WPA e WPA2 dependente da chave e com falhas de implementação
  - TKIP como melhoramento
    - Mais lento que o WEP
    - Não compatível com todas as soluções clientes
  - IPSec
    - Seguro, não padronizado, lento, difícil implementação

# Ameaças Wireless

Existem quatro principais classes de ameaças à segurança em redes sem fio:

1. Ameaças não estruturadas
2. Ameaças estruturadas
3. Ameaças externas
4. Ameaças internas

# Ameaças Wireless


1. Ameaças Não Estruturadas
   - Indivíduos facilmente utilizando ferramentas de hacking.
     - Netstumbler
     - Inssider
     - aircrack-ng
   - Característica:
     - Oportunista por natureza
     - Tipicamente pouco competente tecnicamente e pouco persistente

# Ameaças Wireless

2. Ameaças Estruturadas

- Hackers que são **altamente motivados** e **tecnicamente competentes**.
- Eles **sabem** e **pesquisam** vulnerabilidades nos sistemas wireless
- Eles entendem e desenvolvem códigos de exploração, scripts e programas.

# Ameaças Wireless

2. Ameaças Estruturadas

- Hackers que são **altamente motivados** e **tecnicamente competentes**.
- Eles **sabem** e **pesquisam** vulnerabilidades nos sistemas wireless
- Eles entendem e desenvolvem códigos de exploração, scripts e programas.