



# **COMPUTER SECURITY**

**Wireless System**

**Pertemuan VIII**

**Rianto, S.Kom., M.Eng.**

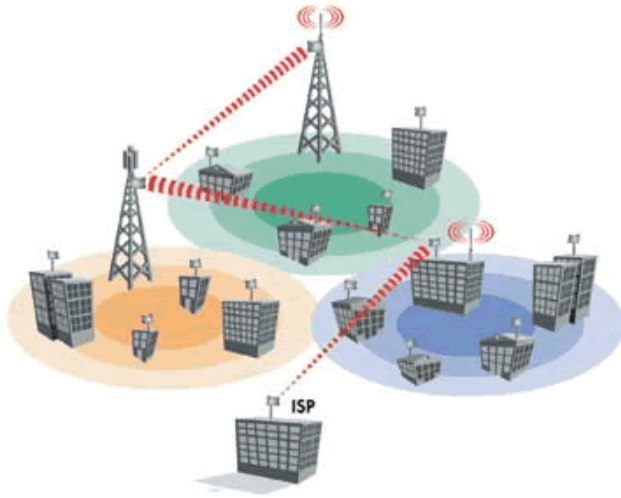
Fakultas Sains dan Teknologi

Universitas Teknologi Yogyakarta

Email : [me@rianto.com](mailto:me@rianto.com) Website : <http://www.rianto.com>

Mobile : 0815 787 02873

# Definisi



Sebuah teknologi yang memungkinkan pengiriman data dengan kecepatan antara 11- 54 Megabyte per second. Teknologi ini dikenal dengan sebutan Wireless Fidelity (Wi Fi), yang bekerja pada jaringan 3G dan dapat membantu pengguna internet berkomunikasi data secara nirkabel.

# Mengapa Wireless

- Sudah banyak digunakan. Bahkan jumlah perangkat telepon wireless sudah mengalahkan jumlah fixed
- Aplikasi baru:
  - SMS, MMS, ringtone, dll
- SMS merupakan killer application.
  - M-banking, bagaimana sistem keamanannya ?

# Mengapa Wireless

- Kemudahan wireless:
  - Kenyamanan: bergerak (mobile) & always connected, roaming
  - Lebih murah dan cepat untuk dimiliki dan diluncurkan
  - Kecepatan mulai nyaman
  - Mulai muncul aplikasi wireless

# Teknologi Wireless

- Cellular-based wireless data solutions
  - Mempergunakan saluran komunikasi celluler yang sudah ada untuk mengirimkan data (CDMA/GPRS)
- Wireless LAN (WLAN) solutions
  - Hubungan wireless dalam lingkup area yang terbatas, biasanya 10 s/d 100 meter dari base station ke Access Point (AP)
  - Mulai meningkat sampai ke 15 mil (WiMax)
  - Ditambah dengan Mesh technology

# Masalah Dengan Keamanan

- Cloning handphone AMPS untuk curi pulsa
- Cloning SIM card?
- Aircsnort dapat menyadap paket WLAN. Tools lain seperti Netstumbler, WEPcrack, dll mulai banyak tersedia
- NIST di Amerika melarang menggunakan WLAN untuk sistem yang memiliki data-data confidential
- Bluetooth jacking, bluestumbler: mencuri data-data melalui bluetooth
- Pencurian fisik (perangkat wireless yang biasanya kecil ukurannya) dan data
- Penyadapan, man-in-middle attack, passive attack dapat dilakukan. Contoh: informasi seperti daftar nomor telepon, calendar, dan data-data lainnya bisa dibaca melalui bluetooth tanpa pengamanan

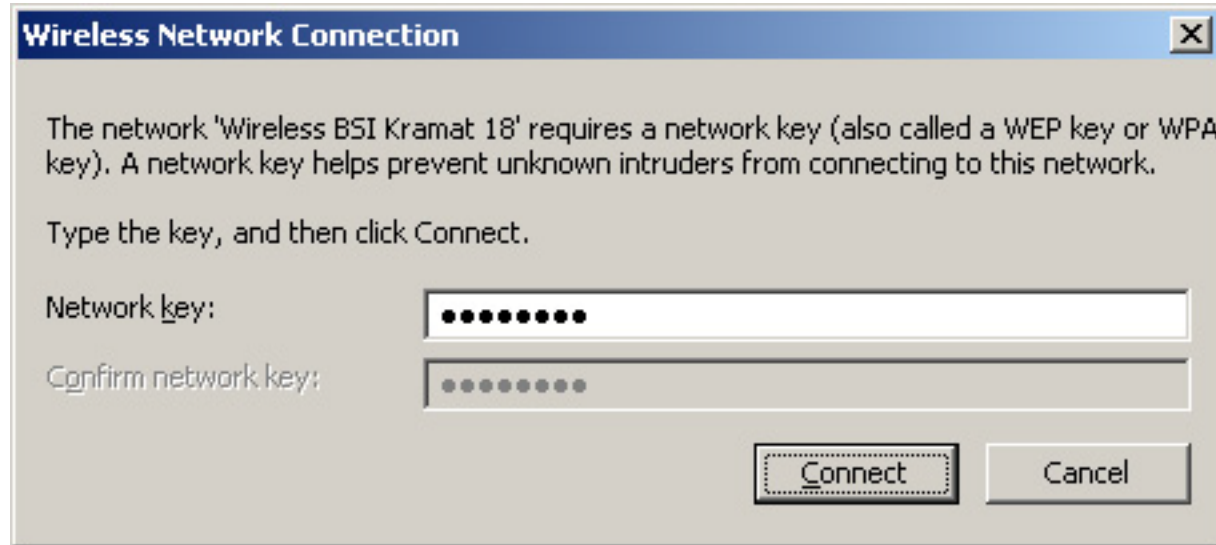
# Masalah Dengan Keamanan

- Resource perangkat wireless yang terbatas (CPU, memory, kecepatan) sehingga menyulitkan pengamanan dengan encryption misalnya
- Pengguna tidak dapat membuat sistem sendiri, bergantung kepada vendor
- Dos, active attack, injection of new (fake) traffic, mengirim pesan sampah (bluejacking), hijacking information
- Fokus utama dari wireless adalah transfer data secepat mungkin. Speed! pengamanan dengan enkripsi (apalagi dengan resources terbatas) menghambat kecepatan sehingga menjadi nomor dua
- Pengguna tidak tahu ada masalah keamanan

# Teknik Pengamanan

- Segmentasi jaringan. Masukkan wireless ke sisi extranet.
- Pembatasan akses berdasarkan MAC address
- Encryption: WEP (Wireless Equivalency Protocol)
  - Masih ada masalah dengan Initial Vector (IV)
- Penggunaan end-to-end encryption pada level aplikasi

# Contoh Pengamanan Dengan WEP



# Penutup

- Penggunaan wireless tidak dapat dihindari
- Teknologi wireless masih “bayi”, membutuhkan perkembangan lebih lanjut
- Kesadaran akan masalah keamanan wireless ini masih perlu disosialisasikan