Northeastern University

Wireless and Mobile Security
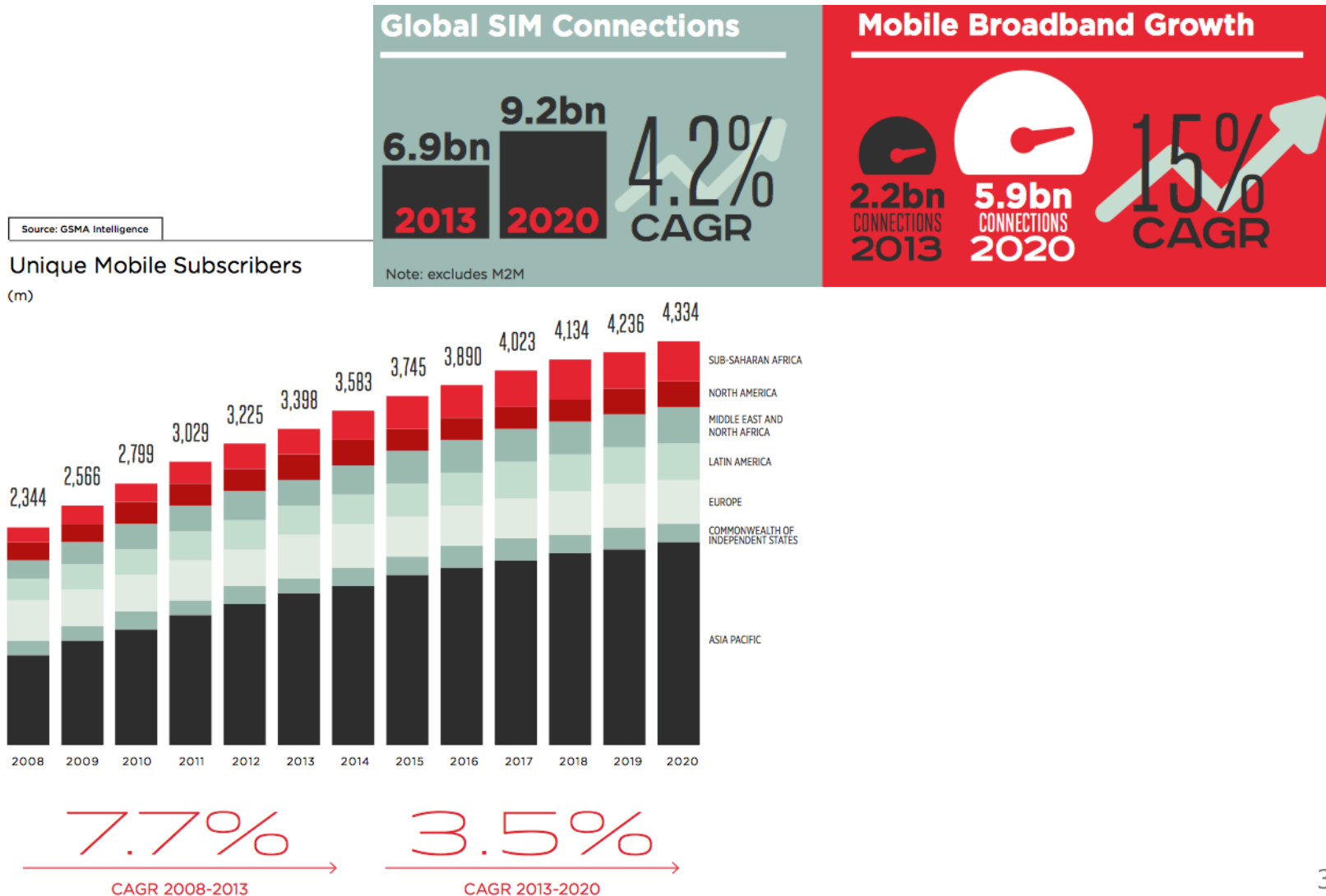## -- an introduction

Guevara Noubir

Northeastern University
noubir@ccs.neu.edu

Outline

- Introduction to the topics

- Structure of lectures

- Logistics

Wireless Communications

- Key technology of the Mobile Revolution

Ubiquity of Wireless & Mobile

- Mobile Phones

- Power Grid
  - Wireless Remote Terminal Units
  - GPS signals provide time synchronization information to timestamp samples.
- Vehicle to Vehicle (DSRC)
- Air Traffic Control
- Home Automation
- Wireless Sensor Networks / Internet of Things
- Biomedical devices
- Military Communications

- Wireless Energy Transfer

Software Defined Radios

- Wireless & Mobile, a traditionally EE discipline, is increasingly driven by CS (algorithms & applications)
- Information Theory was founded by Claude Shannon (1948)
  - In his MS Thesis "electrical applications of boolean algebra could construct and resolve any logical, numerical relationship" (1937)
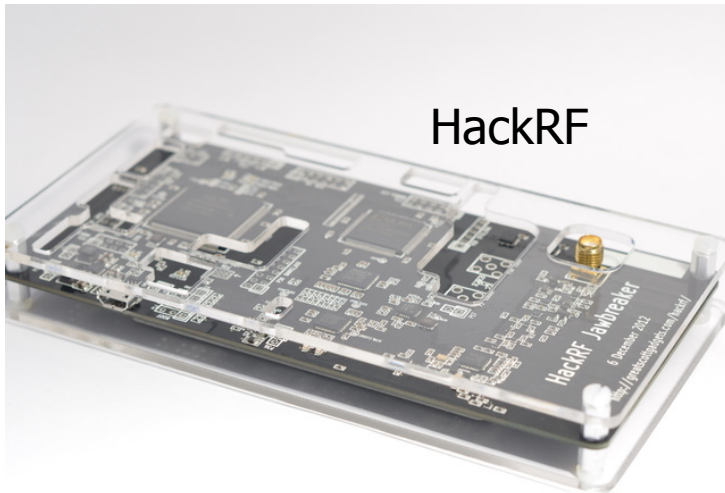
HackRF

USRP N210

Technology

- Radio
  - Architectures/Protocols: Cellular, WLAN, PAN, WSN/IoT, RFID, GPS, Satellite, etc.
  - Building Blocks: Antenna, Power Amplifier, Filters, Mixers (Down/Up conversion), Modulation, Coding, access control, link adaptation, encryption, etc.
- Devices
  - Sensors
  - Security modules e.g., USIM
  - Operating System
  - Applications

Unique Characteristics

- Wireless
  - Broadcast medium
  - Limited RF spectrum

- Mobile
  - Architectures & Protocols that support access from anywhere
  - Limited energy

- Emergence of Mobile + Cloud architectures

Security Risks & Challenges

- Information leakage
  - Data
  - Traffic patterns
  - Location

- Denial of service
  - Limited resources => complex control mechanisms

- Challenges
  - Large attack surface, numerous sensors, significant PII, limited battery & computation, coupling of networks, critical infrastructure

Long history of attacks

- Great Seal Bug (Aug. 4, 1945)
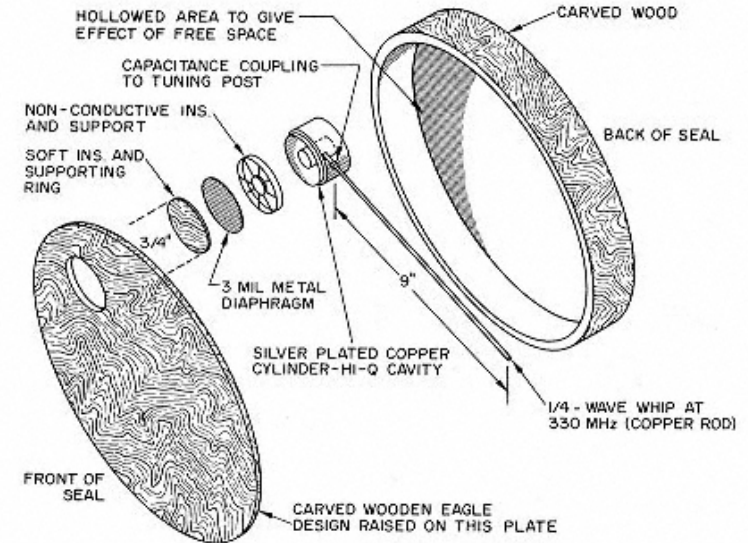
- Cordless phones
- GSM
- WEP, WPA Enterprise, WPS
- GPS
  – Power grid, air traffic

Course Lectures

- **Part I**
  - Review of Network Security: from Crypto to Security Protocols
  - Fundamentals of Wireless & Mobile Systems: key features and mechanisms of wireless and mobile systems
  - Security Standards in current Wireless & Mobile Systems: WiFi Security (WEP, WPA, WPA-Enterprise); Cellular Security (GSM, 3G, LTE); Internet of Things / Wireless Sensor Networks / RFID
  - Emerging Privacy concerns: location, tracking, traffic analysis, mobile and the cloud
- **Part II**
  - Wireless and Mobile as a Cyber Physical Infrastructure (CPS)
  - Denial of Service and Spoofing Attacks Cellular, WiFi, GPS
  - Implications to CPS: e.g., Electricity grid, Internet of Things
- **Part III**
  - Security of Mobile Computing Platforms
  - Android and iOS security models
  - Threats and emerging solutions (e.g., side channel attacks)