Mobile and Embedded Device Security

Statistics

- 68% of all health sector breeches were due to a lost or stolen cell phone
- 25% of all laptop theft is from unlocked cars
- 15% in airports and hotels
- 12% from restaurants

Mobile

- Coverage area for cellular telephony in city - *hexagon*

Types of Device Support:

- *BYOD* - bring your own device
- *COPE* - corporate owned, personally enabled
- *CYOD* - choose your own device, you still own it
- *VDI* - virtual desktop infrastructure

Mobile Device Management (MDM)

- *Mobile Application Management* (MAM) - remote install of updates and software
- OEMs and wireless carriers don't like updating everything, becuase it wouldn't distinguish them
- Updates could conflict with their factory settings
- Why update when you could sell more?

Embedded Systems

- IoT - some operated with AI
- Realtime operating systems
- susceptible to act as DDoS bots
- *Controller Area Network* (CAN) - network of microcontrollers communicating without a central authority
- QR code or PIN on each device, using ECDH and TLS - Security 2 (S2) Framework

Supervisory Control and Data Acquisition (SCADA)

the essence of "smart" embedded components

- aka. Distributed Control System (DCS), Industrial Control System (ICS)
- likely involved when they control a physical process
- multiple components networked together
- historically isolated from network, now are integrated
- Stuxnet attack on Iran nuclear facilities

Satcom

- *repeater* - satellites that relay the same information at different frequencies