Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #7 – Personal Area Networks

Carnegie Mellon University
Silicon Valley

Early Project Tasks

- Topic Survey Presentation
  - Background summary of your topic area
  - Not too broad, and not too specific to your project goals, but background that prepares the class to understand your project scope
  - 20 minute presentation in class
  - Dates available: 9/23, 9/25, 10/2, 10/7, 10/9
  - Up to three presentations per class day

Early Project Tasks

- Project Proposal
  - Presentation of your project goals and deliverables
  - Builds on what you presented in your survey
  - 1 slide, 5 minute presentation in class, October 14
  - Your slide will be due October 13 via email
  - We'll post a “quad chart”-like slide template
  - Presentation order will be randomized

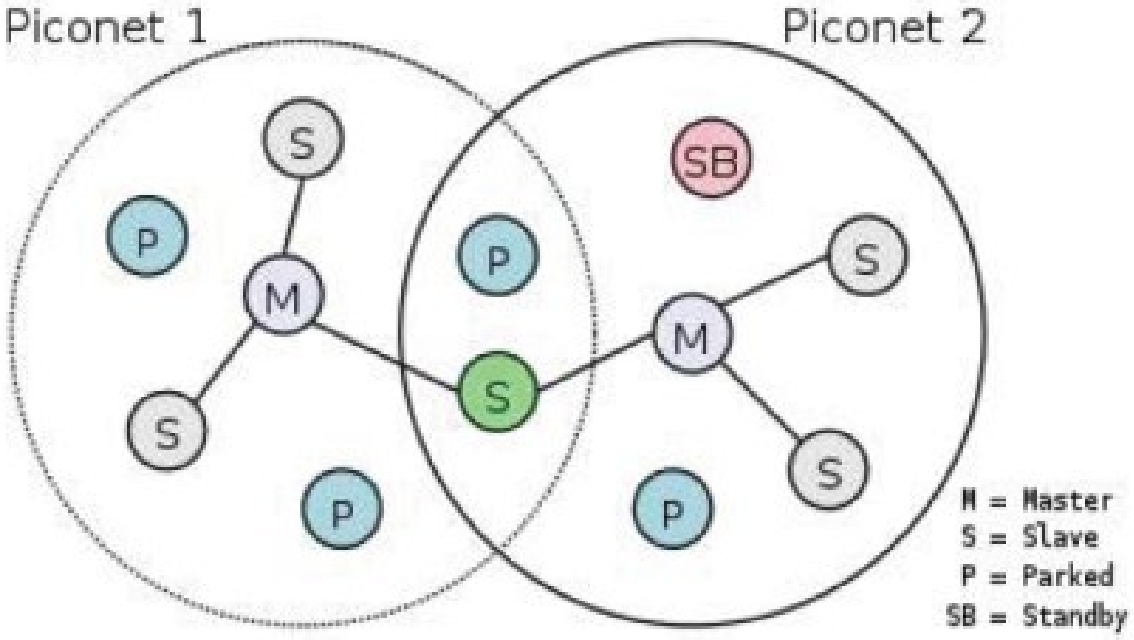
Personal Area Networks

- Personal area networks enable device-to-device communication without relying on the Internet

- The IEEE 802.15 family
  - 802.15.1: Bluetooth
  - 802.15.2: coexistence with other wireless systems
  - 802.15.3: High-rate WPAN, including UWB
  - 802.15.4: Low-rate WPAN, including ZigBee
  - 802.15.5: mesh networking
  - 802.15.6: body area networks (BAN)
  - 802.15.7: visible light communication (VLC)

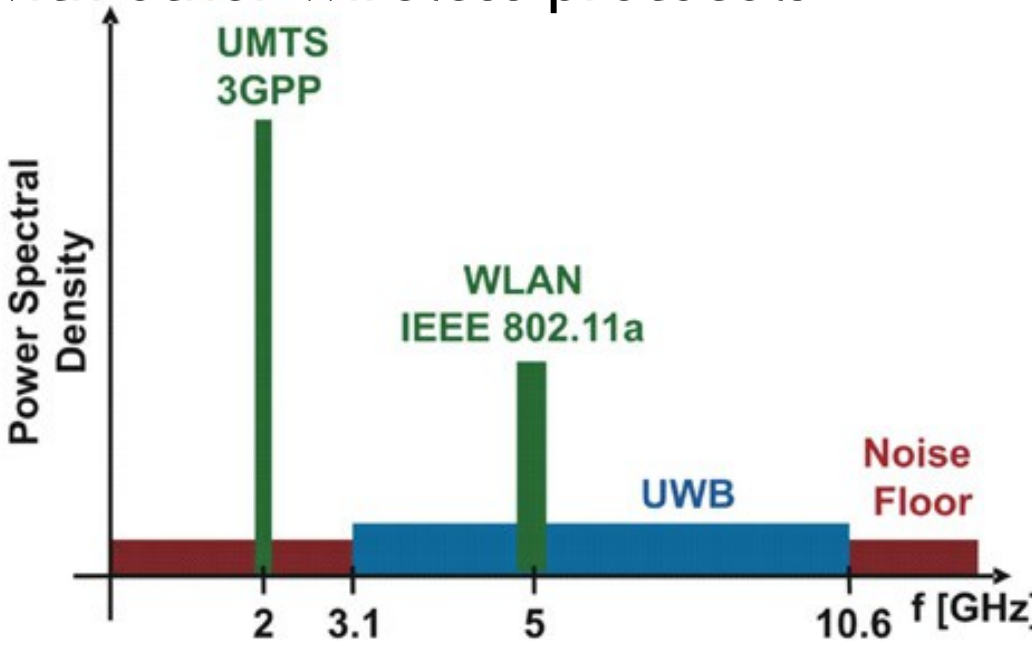
Bluetooth

- 802.15.1 provides Bluetooth PHY
  - Short range, few devices, low power, cheap
  - Commonly used for home, personal, office networks
  - Bluetooth piconet is similar to WLAN (1 server, n clients) → (1 master, n slaves), only no back-end



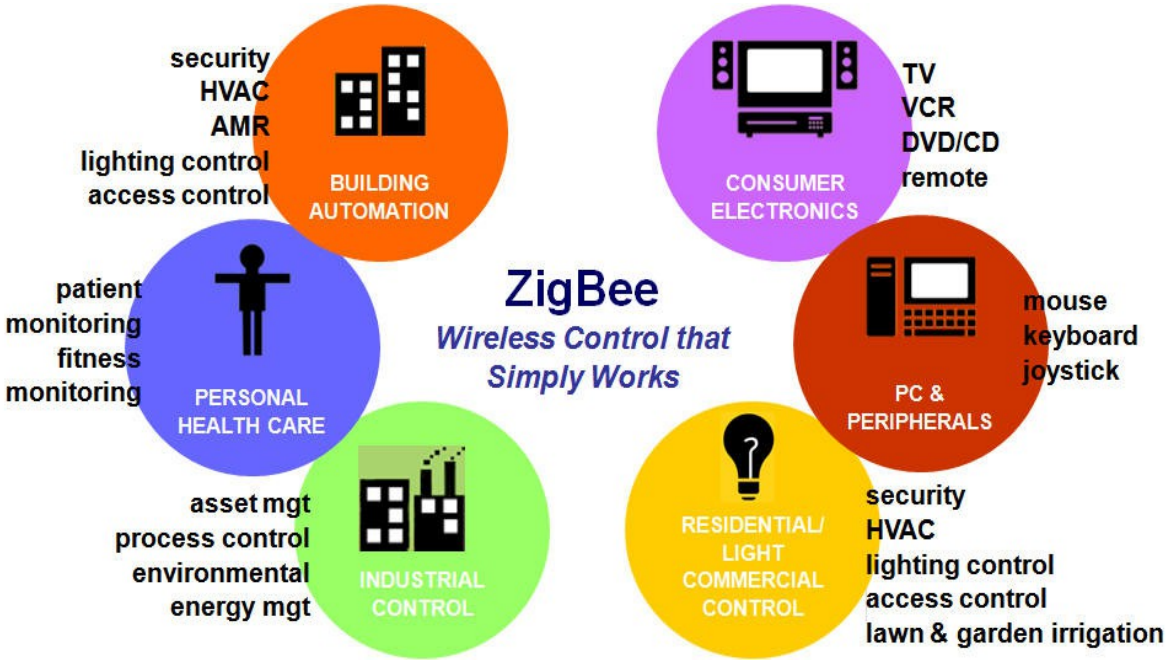
Ultra-Wideband

- Based on 802.15.3 standard
  - Very high data rate (~Gbps), very low power, very short distances (10-100cm)
    - High-rate file transfer, streaming audio/video, wireless display, wireless printing, …
  - Coexists with other wireless protocols



ZigBee

- Based on (and building on) 802.15.4
  - Designed for home automation, low-rate control systems, sensor networks, etc.
  - ZigBee builds a full network stack on top of the 802.15.4 PHY/MAC

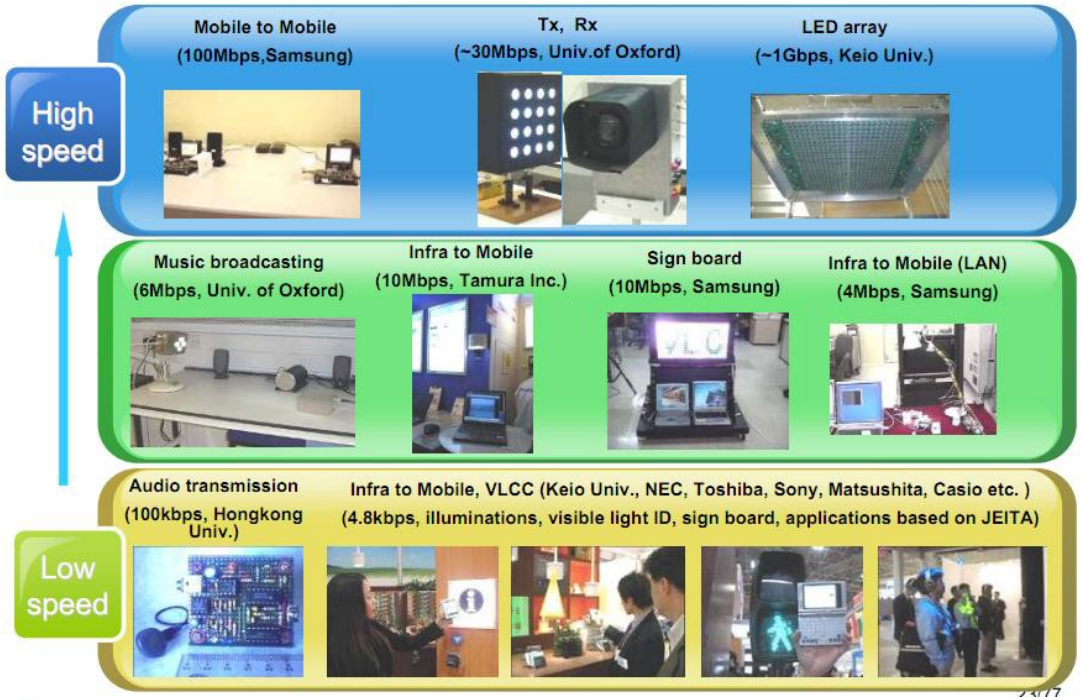


Body Area Networks

- 802.15.6 working group, standardization in prog.
  - Data collection from and control of medical sensors and implanted medical devices
  - Incredibly low power, esp. implanted devices

Visible Light Communication

- Based on 802.15 WG7
  - Device-to-device and device-to-infrastructure communication using visible LEDs / sensors
    - 428-750 THz, unregulated, potential for high-rate and low-rate communication



PAN Challenges

- Most PAN standards specify lower layer (PHY/MAC) functionality for device-to-device communication
  - Higher layer services are not included or needed
  - Security in device-to-device (ad hoc) communications is notoriously difficult
    - Bluetooth security has been a constant struggle
  - How to improve security in ad hoc scenarios?

Case Study: Bluetooth

- Let's focus on the ubiquitously deployed Bluetooth protocol

- Almost every smartphone (and most feature phones) have Bluetooth
- Some people use Bluetooth every day
  - Earpieces, sync, file transfer, etc.

- Some slides courtesy of L. Zoia and Y. Zhang

Bluetooth Security

- Stealth
  - Discoverable / non-discoverable modes
  - Connectible / non-connectible modes
- Frequency hopping
  - 79 channels / bands used for control and data traffic, making it more difficult to eavesdrop or block
- Authentication & encryption
  - Mode 1: none
  - Mode 2: used only for specific services (e.g., transfer)
  - Mode 3: used for all traffic
  - Mode 4: Secure Simple Pairing – service-level security

Bluetooth Threats

- Surveillance - Blueprinting, bt_audit, redfang, War-nibbling, Bluefish, sdptool, Bluescanner, BTScanner
- Range extension - BlueSniping, bluetooone, Vera-NG
- Obfuscation - Bdaddr, hciconfig, Spooftooph
- Fuzzing - BluePass, Bluetooth Stack Smasher, BlueSmack, Tanya, BlueStab
- Sniffing - FTS4BT, Merlin, BlueSniff, HCIDump, Wireshark, kismet
- DoS - Battery exhaustion, signal jamming, BlueSYN, Blueper, BlueJacking, vCardBlaster
- Malware - BlueBag, Caribe, CommWarrior
- Unauthorized direct data access - Bloover, BlueBug, BlueSnarf, BlueSnarf++, BTCrack, Car Whisperer, HeloMoto, btpincrack
- MitM - BT-SSP-Printer-MITM, BlueSpooof, bthidproxy

Surveillance

- Used to acquire specific details about a user / device to assess possible vulnerabilities

- Blueprinting
  - Uses / tracks the device address, available services, and related information to profile the interface, device, host OS, user, etc.

Range Extension

- Extending Bluetooth range (possibly against FCC regulations) allows an attacker to work from a distance

- Bluetooone
  - Attaching a high-gain antenna or directional antenna can extend the range to several km

Attack Obfuscation

- Attackers can use obfuscation tools to achieve a level of anonymity in launching the attack

- Spooftooph
  - Tool for automating spoofing or cloning Bluetooth device Name, Class, and Address

Fuzzing

- Bluetooth packets follow a strict formatting standard
- Input that doesn't follow the format can cause **buffer overflow**, **unauthorized data access**, and **application / system failure**

- Bluetooth Stack Smasher and BluePass
  - Tools for crafting, assembling, and sending packets to a target device to test the ability of an app/service to handle standard and non-standard input

Sniffing

- Sniffing is the process of capturing traffic in transit, just like eavesdropping on a phone call

- Frontline FTS4BT and LeCroy Merlin
  - Combine specialized hardware and software to monitor Bluetooth traffic
  - Matching the connection's frequency hopping pattern
  - Capturing the data transmitted along that pattern

Denial of Service

- DoS attacks can target communication channels or any service the device uses, including the processor, memory, disk, battery, and general system availability

- Blueper
  - Designed to abuse Bluetooth file transfer on select mobile devices
  - Floods the target with file transfer requests

Unauth. Direct Data Access

- UDDA attacks gather private info by penetrating devices through security loopholes

- BlueBug
  - Download contacts, call lists, send / read SMS messages, etc.

- BTCrack
  - Brute-force method for cracking the Bluetooth PIN
    - Milliseconds to crack a 4-digit PIN, several thousand years for a 16-digit PIN

MitM

- MitM attacks in Bluetooth aim to intercept and control connections, often using obfuscation as an intermediate step

- Current Bluetooth implementations thwart a wide variety of MitM attack types

Popularity of Bluetooth Security Issues

- Why do you think all of these Bluetooth threats aren't as well-known as Internet-based attacks?
- What can an attacker achieve through Bluetooth-based attacks?
- Even though Bluetooth has been around for a while, its use in mobile devices has highlighted many of the security issues

Bluetooth Defenses

- Should users be responsible for their own security in Bluetooth services / apps?
- What about chip/radio manufacturers?
  - Input validation testing, disabling unneeded channels, enforcing data format policies, and rigorous testing can certainly help.
- What about standard/specification groups?
  - Maybe mandate stronger security, two-factor authentication, etc.?

Internet-Style Support for Enhancing PAN Security?

- One approach to address some of the PAN challenges is to tether to the Internet
  - Ad hoc agreement can include a trusted 3rd party – web server, cloud service, broker, etc.
  - Ex: Bluetooth exchanges using cloud-based key management, ID verification, etc.

- Hybridization of devices + Internet connectivity allows for a wider variety of services

Tethered PANs

- Tethering PAN devices to the Internet via some sort of gateway device allows a broader scale of device-to-device communications
  - Ex: Sensor gateways
  - Ex: UbiPAN [Albert et al., 2010]
    - Extends Bluetooth networks using IP and SIP services
- Exercise for you: read the UbiPAN paper and think about how this helps / hurts PAN security

Other PAN-like Tech

- WiFi Direct, using SoftAP
  - Sort of a half-way point between WiFi infrastructure and ad hoc modes; devices negotiate to decide which one will take the AP role, and the rest will be clients
  - Supports WPA2
- NFC
  - Device-to-device pairing using EM-coupling
  - Based on RFID, so it's completely different from PAN and WiFi standards
  - More on this later.

Sept 23:
NFC and Mobile Payment