

Mobile Security

Fall 2015

Patrick Tague

#7: Personal Area Networks

Announcements

- Assignment #2 is due today
- Assignment #3 will be posted today
 - Due Oct 22

Class #7

- Activity
- Personal Area Networks
- Some Bluetooth threats, past and present

First, a brief activity

How to Read a Paper Quickly

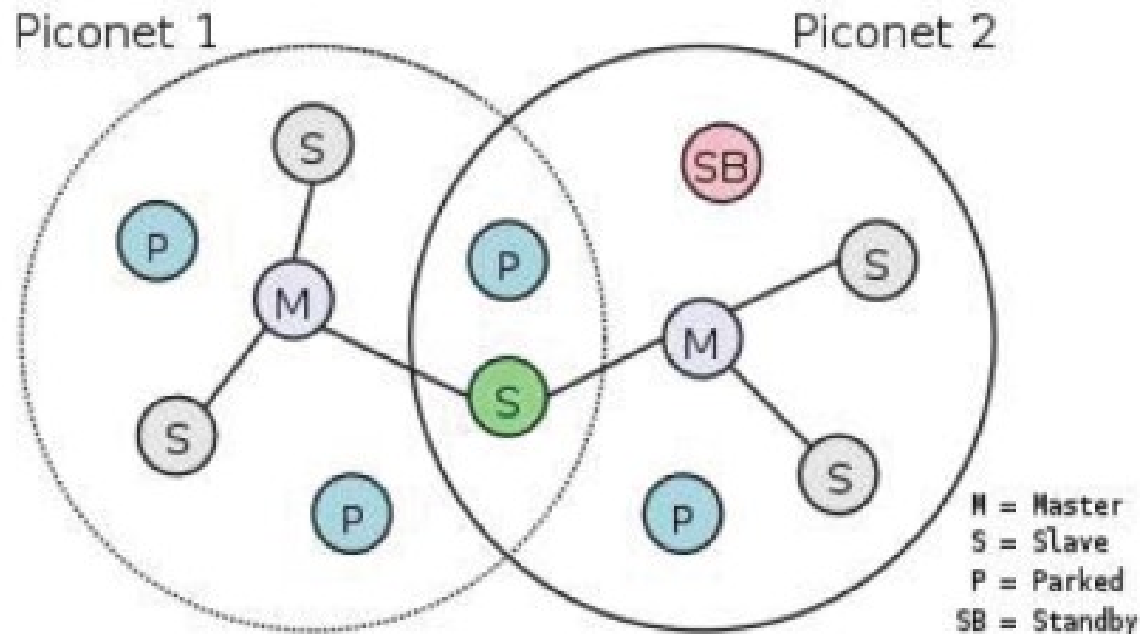
- Basic idea:
 - You can understand a paper at a high level in 3 minutes
 - Maybe more if it's not a wonderfully well-written paper...
- After 3 minutes?
 - If you decide it's relevant to your work, you can understand the paper deeply in 20-30 minutes
 - Again...if it's done well
- Android Permissions Demystified

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)
 - 802.15 TG8: peer-aware communications
 - 802.15 TG9: key management
 - 802.15 TG10: L2 routing

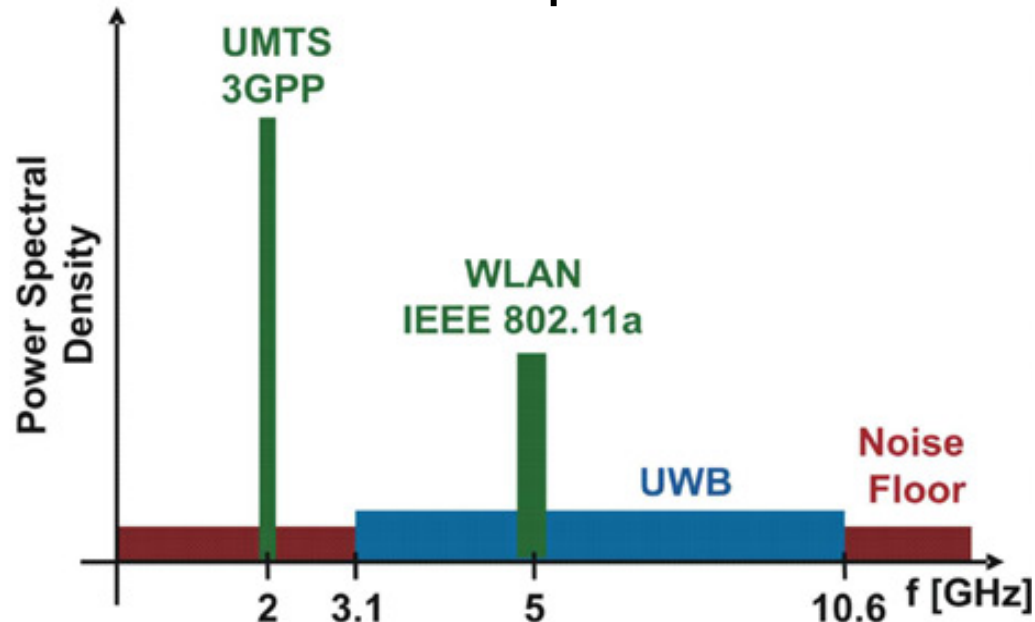
Bluetooth

- 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



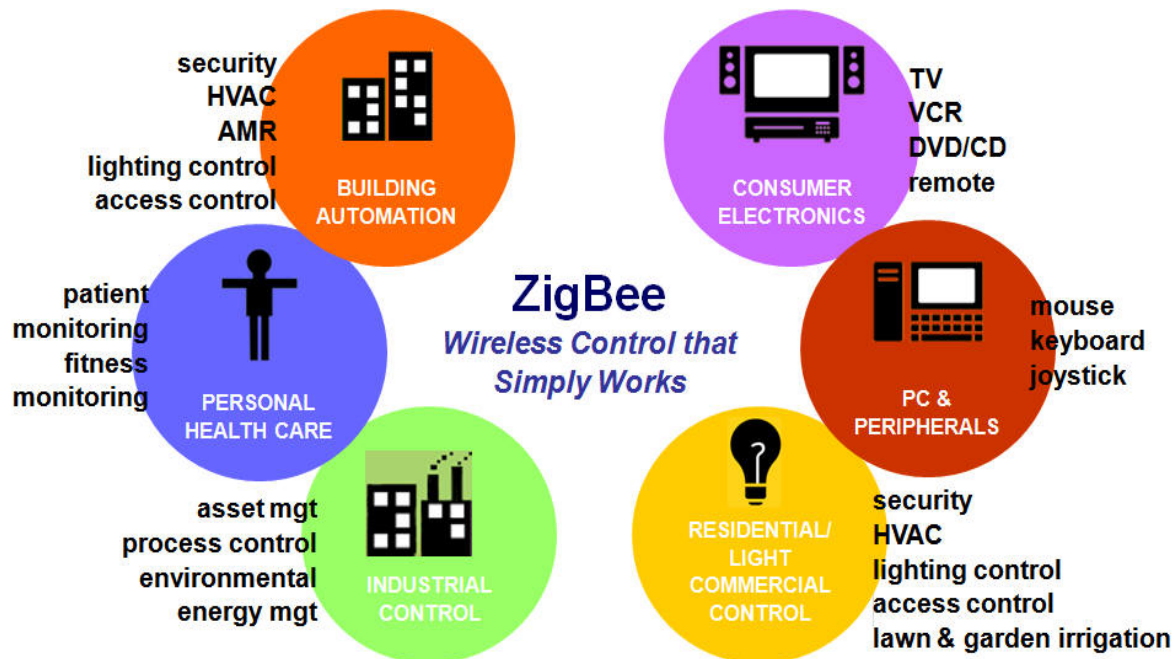
Ultra-Wideband

- 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



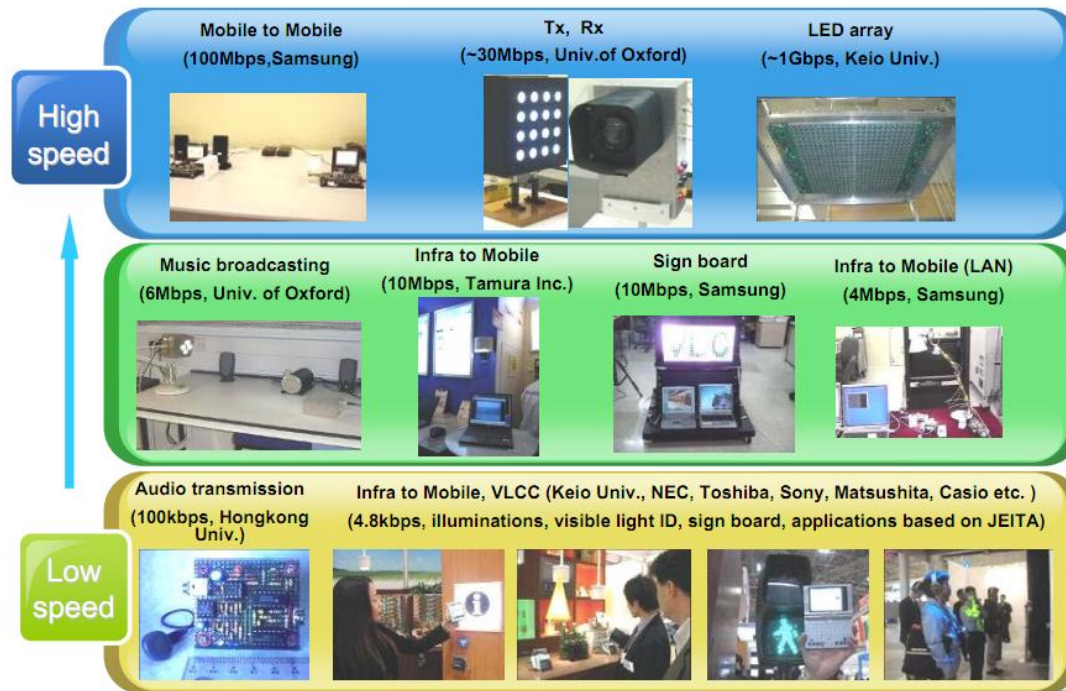
Body Area Networks

- 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.



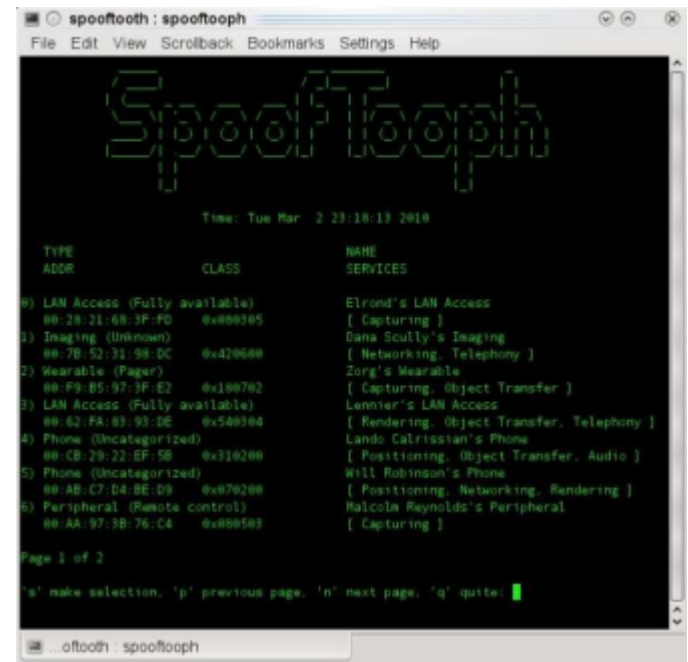
Range Extension

- 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



The screenshot shows a terminal window titled "spooftooth : spooftooph" with a menu bar (File, Edit, View, Scrollback, Bookmarks, Settings, Help). The main display features the "SpoofTooph" logo in a stylized font. Below the logo, the current time is shown as "Tue Mar 2 23:18:13 2018". A table lists discovered Bluetooth devices with columns for TYPE, ADDR, CLASS, NAME, and SERVICES. The table content is as follows:

TYPE	ADDR	CLASS	NAME	SERVICES
0) LAN Access (Fully available)			Elrond's LAN Access	[Capturing]
1) Imaging (Unknown)	00:20:21:69:3F:FD	0x000105	Dana Scully's Imaging	[Networking, Telephony]
2) Wearable (Pager)	00:7B:52:31:98:8C	0x420600	Zorg's Wearable	[Capturing, Object Transfer]
3) LAN Access (Fully available)	00:F9:85:97:3F:E2	0x100702	Legolas's LAN Access	[Rendering, Object Transfer, Telephony]
4) Phone (Uncategorized)	00:62:FA:83:93:8E	0x540304	Lando Calrissian's Phone	[Positioning, Object Transfer, Audio]
5) Phone (Uncategorized)	00:CB:29:22:EF:5B	0x310200	Will Robinson's Phone	[Positioning, Networking, Rendering]
6) Peripheral (Remote control)	00:AB:C7:04:8E:99	0x070200	Halcyon Reynolds's Peripheral	[Capturing]
	00:AA:97:2B:76:C4	0x000503		

At the bottom of the terminal, it says "Page 1 of 2" and provides navigation instructions: "'s' make selection, 'p' previous page, 'n' next page, 'q' quitte: █".

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.?

Current Bluetooth Threats?

- How many of these previous Bluetooth attack tools are still useful against modern BT versions?
 - Not many...
- But, new BT versions have their own issues
 - Ex: in Bluetooth Low Energy (BLE), two of the three options for key setup are vulnerable
 - One is to use a “zero” key...so basically unsecured
 - The other does key setup in the clear, with the assumption that the attacker isn't present during key setup
 - What if the attacker can do something equivalent to deauth?

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.

**Oct 8:
Location Services**

**Oct 13 & 15:
SoW Presentations**