Mobile Security
14-829 – Fall 2013

Patrick Tague

Class #8 – NFC & Mobile Payment

Carnegie Mellon University
Silicon Valley

In Case You Missed It…

- If you were at the TOC last week and missed Wednesday's class:
  - Please watch the video to catch up on material
  - Early project deliverables were discussed
  - Please email me to sign up for your survey presentation (schedule on BB)

HW Clarification

- Common questions on Assignment #1
  - **Q:** Can I just request permission X, then use permission X to collect private information?
  - **A:** That's not stealing, that's asking. If you need to ask for a permission, there needs to be another reason to do so. In other words, hide the fact that you're stealing info.

  - **Q:** So, all we have to turn in is the application, right?
  - **A:** No. The assignment has two deliverables. Please read it again.

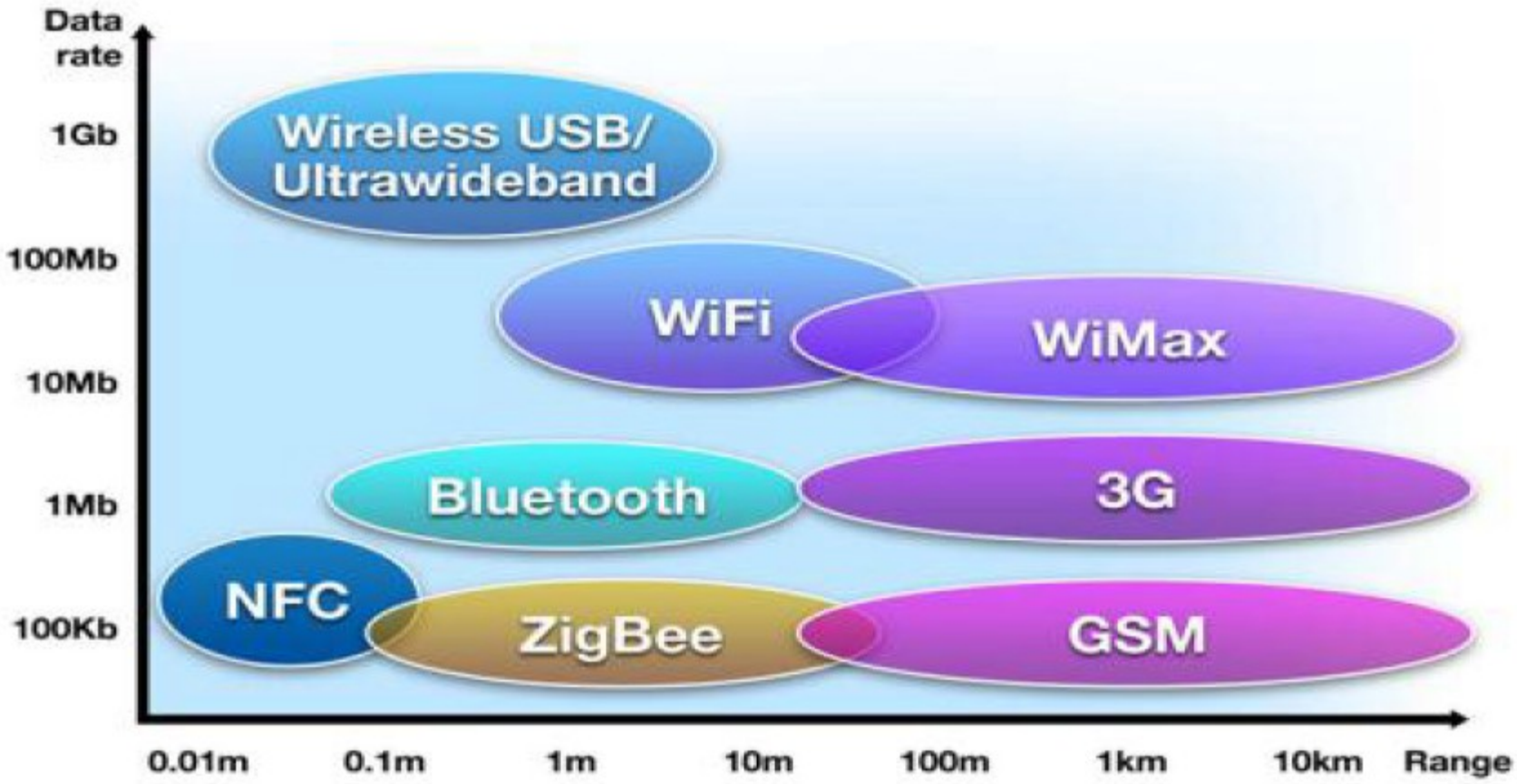
Android Phones

- For those in Pgh still waiting for phones:
  - Sorry for the delay.
  - Please update the spreadsheet to let us know if a tablet (e.g., Nexus 7) would suffice, or if a phone is needed. Email is ok, but direct doc edit is better.
  - Once everyone replies, I'll ship another box to Yuan.
- If you still haven't made a request in the doc, please do so immediately, else more delay.

Near Field Communication

- NFC is a short-range, low-rate wireless connectivity that enables communication between devices in close proximity without initiation

Wireless Comparison



NFC Characteristics

- Uses 13.56MHz RF signal
- Communication over distances up to 4”
- Data transfer speeds of 106, 212, 424 kbps
- NFC chip/tag can store small amount of data (e.g., 96B, 512B tags)

Modes of Communication

- Active Mode:
  - Initiator and target devices have power supplies and can communicate with each other by alternate signal transmission
  - Both parties use half duplex

- Passive Mode:
  - Initiator device generates a signal that the target observes and modulates data on
  - Initiator: full duplex

Modes of Interaction

- Reader/Writer:
  - Use an active NFC device to read/write a passive NFC tag

- Peer-to-Peer:
  - Active NFC devices interact with each other bidirectionally

- Card Emulation:
  - An NFC device takes the role of a passive NFC tag to be read by an active NFC device

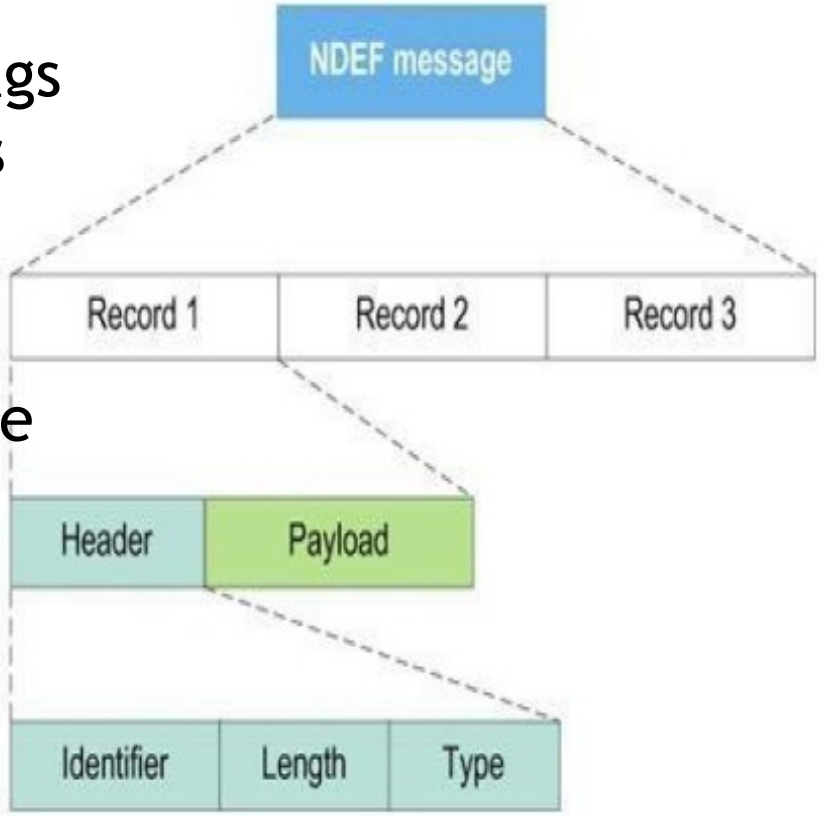
NFC Comm Standards

- ISO/IEC 18092 / ECMA-340:
  - Standards for communication modes for NFC Interface and Protocol NFCIP-1 such as modulation schemes, coding, transfer speeds, frame format, collision control parameters, transport protocol

- ISO/IEC 21481 / ECMA-352:
  - Standards for NFCIP-2, specifies communications modes to minimize interference with other contact-less card devices

NFC Data Standards

- NFC Data Exchange Format (NDEF)
  - Structure for writing data to tags or exchanging between devices
  - NFC tag contains 1+ NDEF messages
  - NDEF message contains multiple records
  - NDEF record contains header (type, ID, length) and payload (MIME, URL, NFC-specific type, etc.)



NFC Tag Standards

NFC Type definition				
	Type 1	Type 2	Type 3	Type 4
ISO/IEC standard	14443 A	14443 A	JIS 6319-4	14443 A / B
Compatible Product	Innovision Topaz	NXP MIFARE	Sony FeliCa	NXP DESFire, SmartMX-JCOP, ...
Data rate	106 kb/s	106 kb/s	212, 424 kb/s	106/212/424 kb/s
Memory	96 bytes, expandable to 2 kbyte	48 bytes, expandable to 2 kbyte	Variable, max. 1Mbyte	Variable, max. 32 kbyte
Anti-collision	No	Yes	Yes	Yes

NFC Uses

NFC Security / Threats

- NFC is a wireless communication interface, so it adopts all of the standard wireless threats
  - Eavesdropping
  - Data corruption / modification / insertion
  - Man-in-the-middle attacks

- NFC Difference:
  - In active mode, both devices are full duplex so they can monitor while transmitting
  - In passive mode, the initiator is full duplex and the respondent/tag is half duplex

Eavesdropping

- NFC itself provides no explicit protection against eavesdropping

- Active-vs-Passive:
  - It's much harder to eavesdrop on passive exchange
  - Mainly because of range (<1m passive, <10m active), but also depends on environment, transmitter's RF field characteristics, quality of attacker antenna and decoder, setup location, …

Data Corruption/Modification

- Attacker can attempt to modify bits in flight based on standardized encoding, e.g., high power pulses can flip 0s to 1s
- In full-duplex mode, this can be detected easily because the pulse needs to be high power
- Difficult to detect in half-duplex mode

Data Injection

- In a message-response mode, an attacker can inject data by responding faster than the intended target
  - Only works if intended target needs time to construct reply, otherwise messages will collide (→ DoS)

- Possible defenses:
  - Secure handshake w/ verifiable response

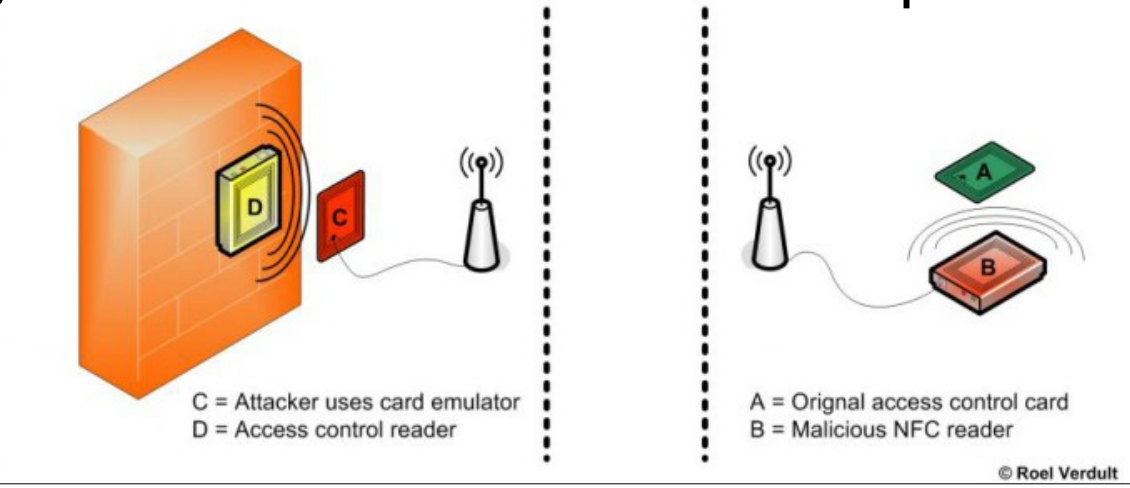
Man-in-the-Middle Attacks

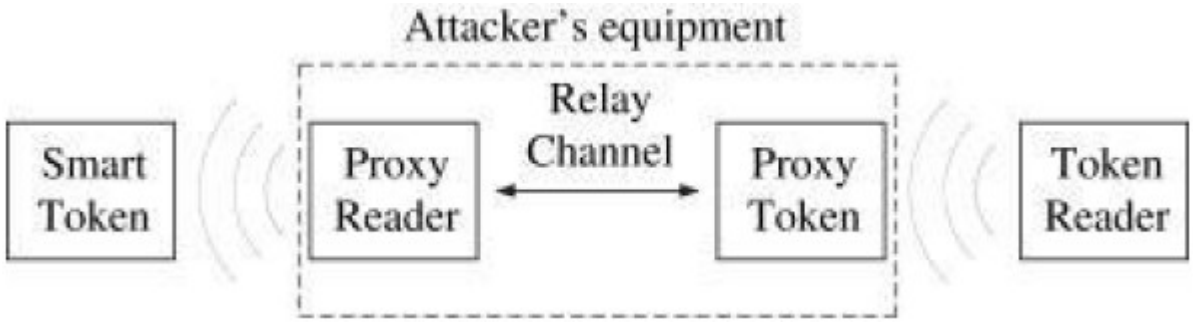
- MitM is difficult in NFC due to:
  - Close proximity (MitM needs to be closer than tag)
  - Full duplex can detect some aspects

- But, what if the MitM attacker modifies the medium?
  - If the attacker blocks the original signal, it can create two sessions needed for MitM attack
  - Turns out that a large-ish sheet of aluminum or a few pieces of paper will block the signal...

NFC Relay Attack

- Modified version of the MitM attack
  - Proximity if assumed but not proven
  - Relay channel used to create two separate sessions





More NFC Issues

- Other than these basic wireless communication concerns, most other NFC security issues are scenario- or application-dependent
  - i.e., how NFC is used introduces vulnerabilities
  - Some apps using NFC don't correctly address basic concerns, which can open up additional issues

- Let's look at a couple special cases

Two Case Studies

- Mobile Payment using NFC

- Smart Posters

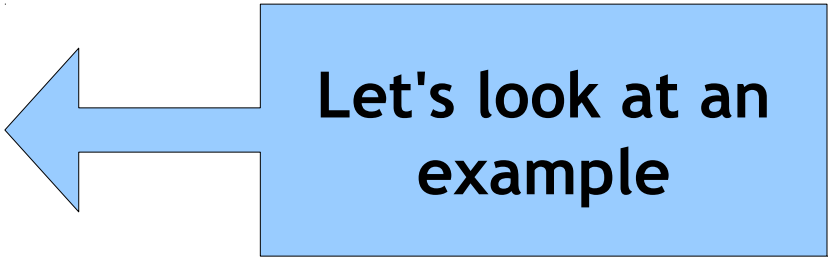
Mobile Payment

- Mobile payment typically uses NFC to initiate the transaction, often using a handshake with the payee before the actual transaction

- Why use NFC?
  - Proximity makes it easier to verify payee
  - Simplifies the transaction process
  - Convenient: store all credentials inside the phone
  - Integrates with other mobile services: eBooks, music downloads, barcodes, etc.

Mobile Payment Systems

- Implementations vary
  - ISIS
  - Google Wallet
  - Paypal Here
  - Square
  - …



Google Wallet

- How to use Google Wallet (initially):
  - Add cards credentials to the app (offline)
  - Approach payment surface (POS terminal)
  - Open Google Wallet app
  - Input 4-digit PIN
  - Put phone very near payment surface

Behind Google Wallet

- NFC radio + “secure element”
  - Stores data / runs programs
  - Encrypted storage, separate from Android phone memory
- When card added, credentials locked in the secure element
- PIN unlocks secure element
- App serves as NFC-based tunnel between secure element and POS terminal

Google Wallet Vulnerability

- PIN Exposure Vulnerability, February 2012
  - Publicized by Zvelo
  - PIN hash stored on phone memory used to validate PIN and give access to secure element
  - SHA256 w/ 4-digit PIN → 10,000 tries to brute force
  - Rooted phone can run Wallet Cracker app, unlock secure element in seconds

- Patched by Google
  - Hash now stored in secure element
  - Managed by banks, so PIN security is banks' responsibility, not Google's

Two Case Studies

- Mobile Payment using NFC

- Smart Posters

Smart Posters

- A smart poster combines a standard visual display with user/mobile interaction and feedback relevant to the specific display, location, context, etc.
  - Achievable using NFC, QR code, …
- In a typical deployment, program a small amount of content or a link on a tag, then stick the tag to the display

Smart Poster Issues

- What if someone reprograms a tag?
- What if someone removes a tag and sticks a new one in its place?
- What if someone covers a tag with a few sheets of paper then sticks a new one in its place?
- What if someone moves a tag to a different location?

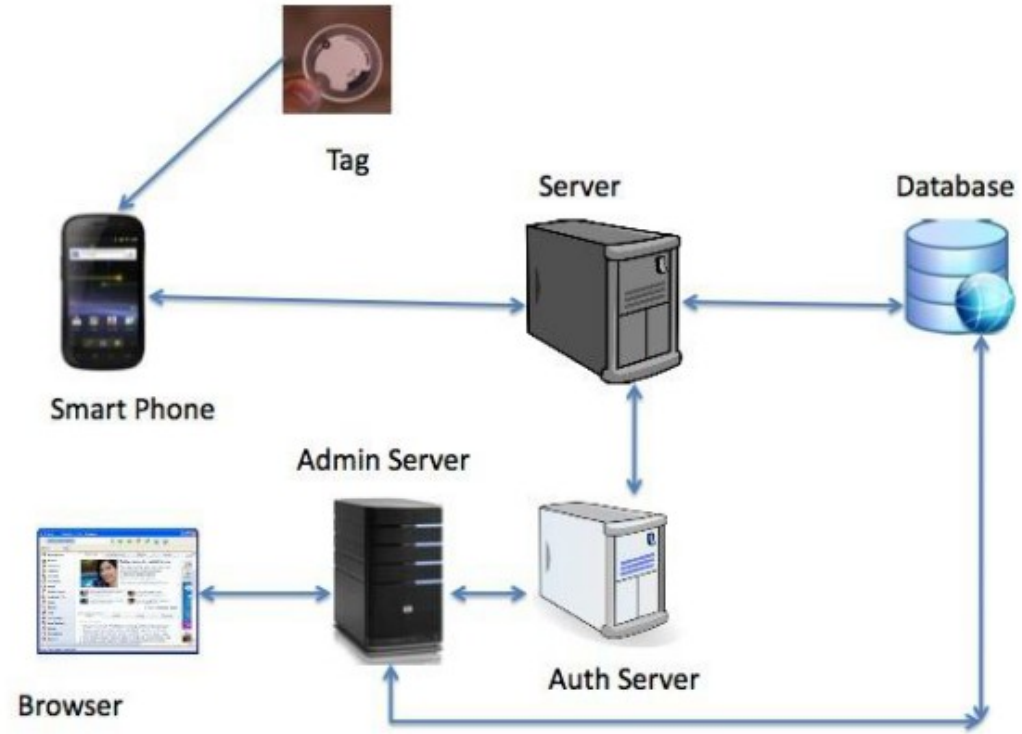
- You get the point...it's really hard to protect tag contents, context, etc.

Challenges

- Very low data rate from tag to reader
- Very small data storage on tag
- Difficult to authenticate tag or validate contents without prior relationship with tag provider

Possible Solution

- S-SPAN: Secure Smart Posters w/ Android NFC
  - Instead of validating the tag or the data programmed on the tag, point the user to something they can validate. It shouldn't matter where the content is.



S-SPAN uses existing web-based mechanisms to validate tag contents, control access to contents, tag revocation / expiry, monitor usage, etc.

Sept 25:
Location Services