Mobile Security
Fall 2015

Patrick Tague

#9: NFC & Mobile Payment

Announcements

- Reminder: assignment #3 due Oct 22
- Assignment #4 will be assigned Oct 22, due Nov 5

Class #9

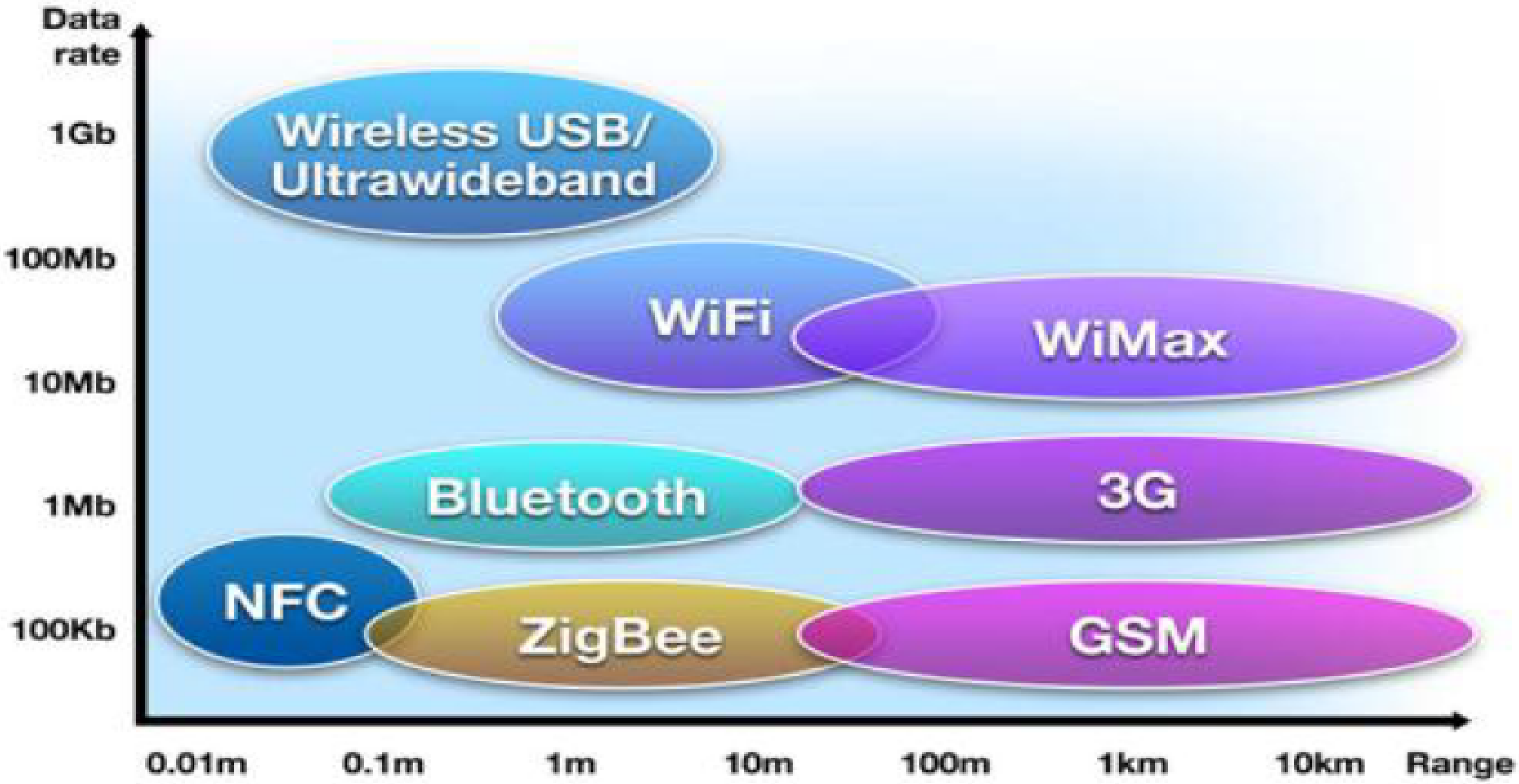
- Near Field Communication

- A few case studies
  - Google Wallet
  - Smart Posters (time permitting)

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

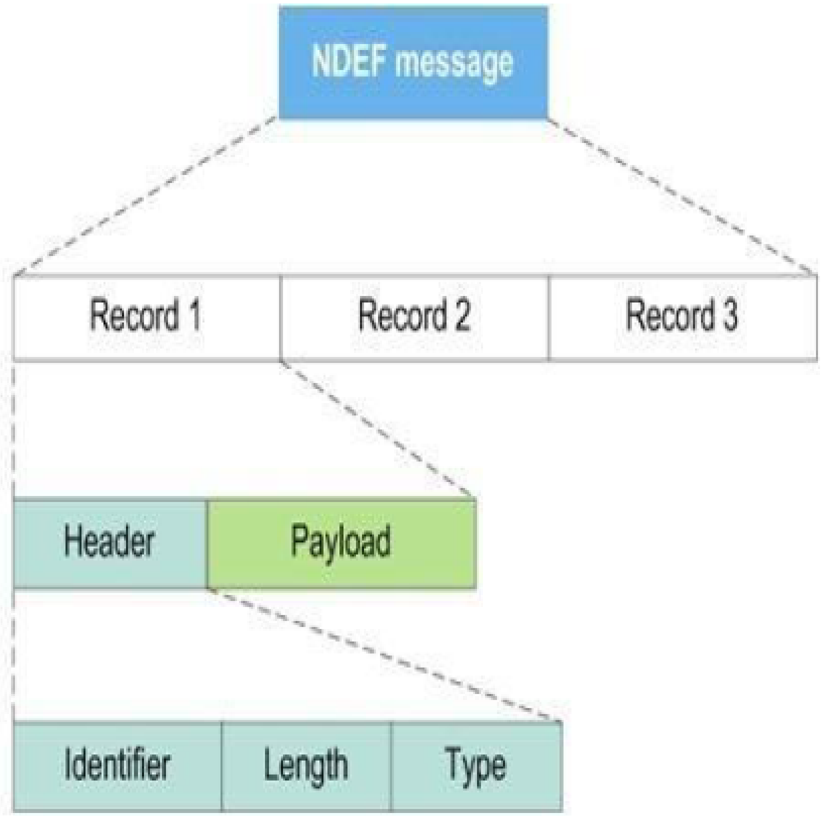
- Card Emulation:
  - An NFC device takes the role of a passive NFC tag to be read by an active NFC device

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


Get information by touching smart posters
Use your NFC phone as an event ticket
Set up your wireless home office with a touch
NFC Consumer Device
Print from your camera by holding it close to the printer
Share business cards with a touch
Get on the bus by waving your NFC phone
Pay for goods with a tap of your NFC phone

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

- Main difference from RF:
  - 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

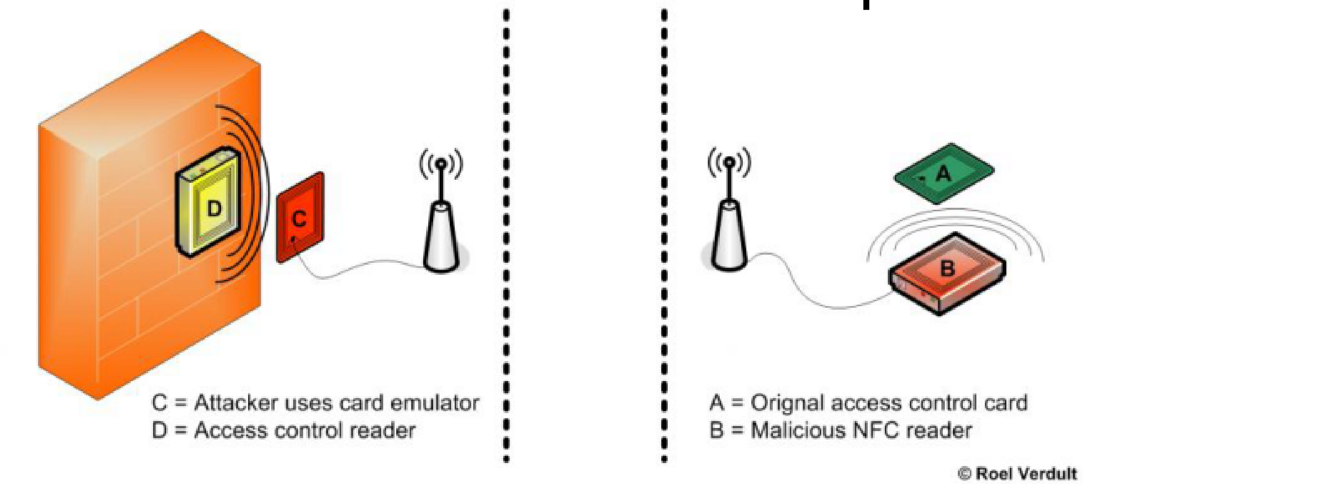
Man-in-the-Middle Attacks

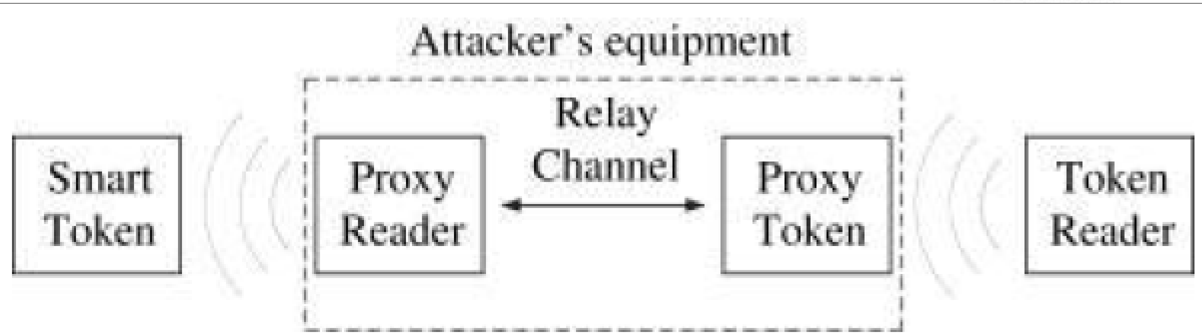
- MitM is difficult in NFC due to:
  - Close proximity (MitM needs to be closer than tag)
  - Full duplex can detect some aspects

- 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 sheet of aluminum or a few pieces of paper will block the signal...

NFC Relay Attack

- Modified version of the MitM attack
  - Proximity is 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 few special cases

Case Studies

- Mobile Payment
- 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
  - Softcard (fka ISIS)
  - Google Wallet
  - Paypal Here
  - Square Wallet
  - Apple Pay
  - ...

Let's look at a couple of examples

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

Why Google Wallet Failed…

- Google Wallet (probably) didn't fail because of security issues / vulnerabilities

- The fact that certain carriers were blocking its installation prevented adoption
  - Verizon was unhappy with Google Wallet's interaction with the specialized hardware (secure element)

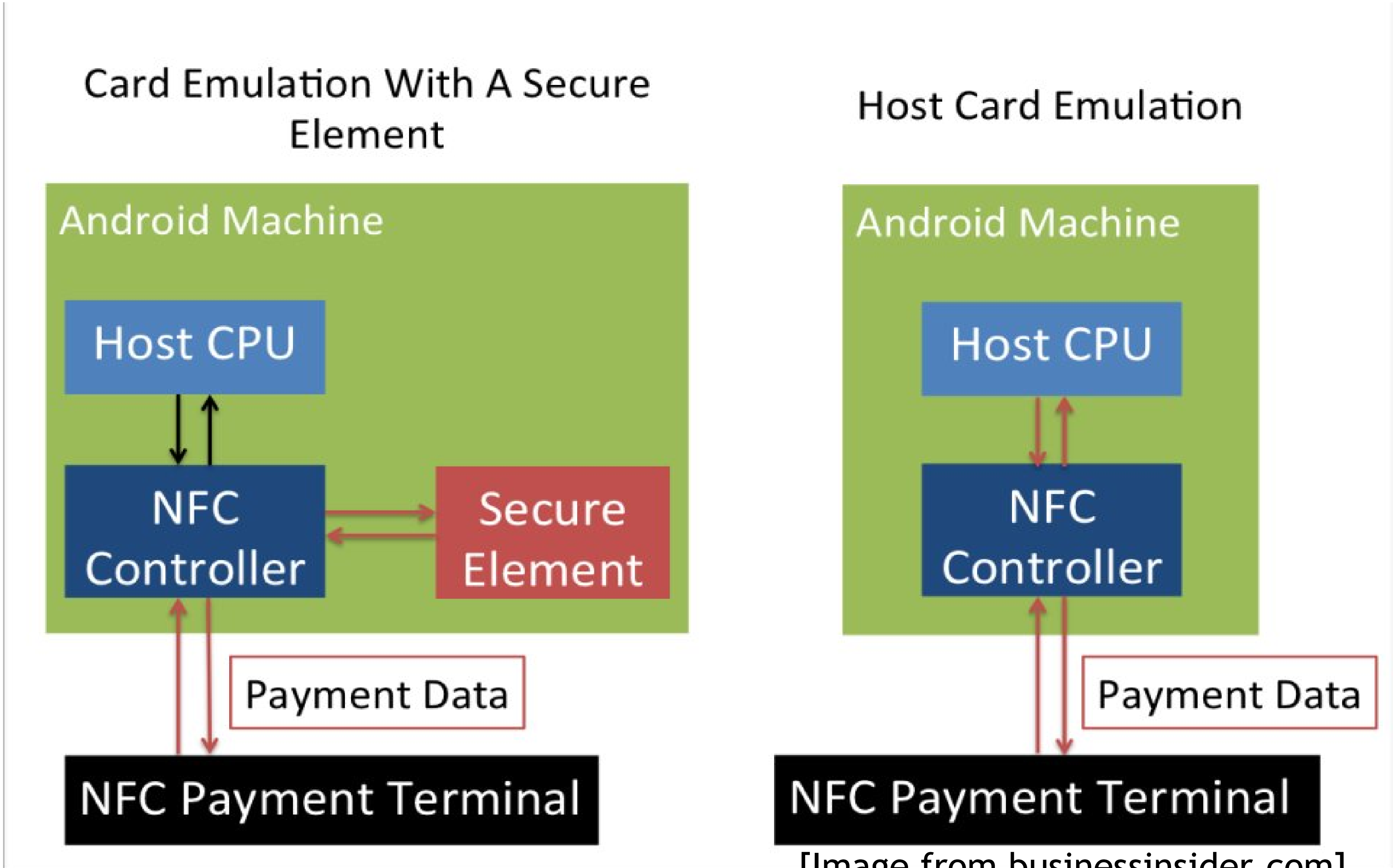
  - Verizon was involved in developing a carrier-provided payment system that was at the time called ISIS
  - ISIS used a hardware secure element

Android Pay

- Google Wallet → Android Pay

- Android Pay will use secure element if it exists or use host card emulation if not
  - Carriers no longer seem to care about apps using secure element, or agreements have been made

How it Works



[Image from businessinsider.com]

Apple Pay

- Apple Pay is Apple's long-awaited dive into NFC-based mobile payment
  - According to Apple, it's perfectly secure
  - According to Forbes.com, it's better than previous NFC payment systems because they're doing revolutionary things like using "a dedicated chip on the device that Apple calls 'Secure Element'"…
- FireEye recently published a blog post with a "security analysis" of Apple Pay
  - While it's not analysis, there's some good insight about complexity of payment ecosystem

A Few Comments

- While the FireEye blog post mentions the whole ecosystem, too much focus is on NFC itself
- Once the sensitive info / control is in the hands of the phone, it's up to the OS and the developer to handle things correctly
- As an example, host card emulation is vulnerable to MitM attacks on a rooted phone
  - A team in class last year helped to expose this

Case Studies

- Mobile Payment

- 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?

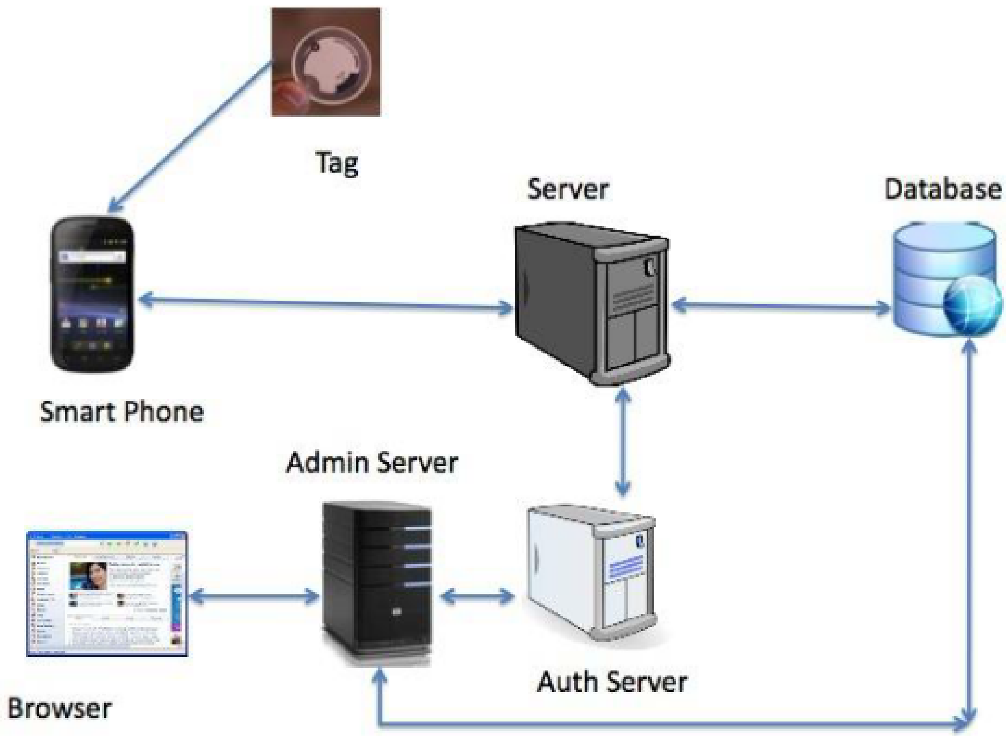
- You get the point...it's really hard to protect tag contents, context, etc.

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.

Oct 22:

Mobile Sensing