Outline

• Nudging *developers* to make better privacy decisions with clean-slate API design
  – (work-in-progress)

• Security & privacy design and analysis for MobilityFirst
Human-Centric Research Agenda

My agenda: Applying *soft paternalistic nudges* to *human behavior* with *computer systems*
Privacy-Preserving API design (w/ M. Gruteser)

- **Insight**: today developers have options
  - take all,
  - or nothing
- **Evidence**: some developers are trying to follow least privilege
- **1. Question**: Can we design a privacy-preserving clean-slate API?
• 1. *Question*: Can we design a privacy-preserving clean-slate API?
  – Yeah, probably

• *What we should be asking*: Can we nudge developers to make better user privacy decisions with novel API designs?
Evaluation: Lo-fi programming

Prototyping for Tiny Fingers

```html
<DOCTYPE html>
<html>
<head>
  <meta charset="utf-8">
  <title>Challenge #2</title>
</head>
<body>
  <h1>The Interesting challenge #2</h1>
  <p>All my attention on Challenge #2 This code is the funniest code I ever wrote</p>
</body>
</html>
```
Expected Results

• Our preliminary studies show promise for the approach

• Contributions:
  – Focus on developers
  – Novel way to evaluate APIs
  – New low-cost framework to evaluate the usability of APIs?
    • Poor API design can cost $$$$$$$$$$
Outline

• Nudging *developers* to make better privacy decisions with clean-slate API design
  – (work-in-progress)

• Security & privacy design and analysis for MobilityFirst
Security and Privacy in MF
(w/ W. Trappe, M. Gruteser)

• In MobilityFirst, we are looking at security and privacy together because they really cannot be separated from each other
  – Introducing a security mechanism can have implications for user privacy
  – Introducing a user privacy mechanism can have implications to security

• For example, without rigorous design, using public keys as identifiers in protocols can potentially identify users better than e.g. IP addresses today
Privacy & Security Stakeholders

- **Users**
- Operators
- Network Providers
- Third-Party Service Providers
- Governments
- Intelligence Agencies
- Law Enforcement
- ...

- Several approaches to privacy, in this presentation focus
  - on user privacy, and
  - on possible technical solutions
Attacks Against User Privacy

- Who you are?
  - Have I seen you before?
- Who do you talk to?
  - Did you talk to them before?
- What are you talking about?
- What is your location?
  - Have you been here before?

- Note that these questions are connected
  - knowing places you go can tell who you are
  - e.g. home/work pairs have been shown highly likely to be unique
Attacker’s Location?
Attacks Today: IP Packets

- can observe
  - Source and Destination IP addresses in all attack locations
  - Resolve and observe names

- You can change your source address, but research has shown that the set of your Destination IP addresses are highly likely to be unique
Attacks Today: IP Packets

- can observe
  - Source and Destination IP addresses in all attack locations
  - Resolve or observe names of destination

- might be interested in who is accessing particular server

Sees what is the source address

Some blog
Today: Solution Tor overlay
MobilityFirst: GUID and NA

- You can observe
  - Source and Destination GUID in all attack locations

- You can change your source address, but research has shown that the set of your Destination IPs are highly likely to be unique, same principle applies to GUIDs
MobilityFirst: GUID, NA at destination

- can observe
  - Source and Destination GUIDs in all attack locations
  - Resolve or observe names of destination

- might be interested in who is accessing particular server

Sees the source GUID, return packet "source" NA

Some blog
MobilityFirst Solution: Disposable Identifiers

- Disposable identifiers have been proposed several times [e.g. Gruteser’03, Lindqvist’05, Lindqvist’08]
- Today, even your disposable identifier is still often tied to your geographic location.
  - Thus, can discover where the packets are coming from

- In MobilityFirst, disposable identifiers do not have geographic or semantic mapping
  - (Unless we add these)
Security & Privacy for MF packets

• Off the record messaging on the network layer
  – Authentication
  – Encryption
  – Deniability
  – Perfect forward secrecy

• We can build non-repudation and e-commerce applications on top of off-the-record network layer
  – The other way round does not work without additional complexity (e.g. overlays)
Summary

• Nudging developers to make better decisions for user privacy

• Security and privacy design and analysis for MobilityFirst
  – In MobilityFirst, we are looking at security and privacy together because they really cannot be separated from each other
  – Presented baseline privacy protections offered by MobilityFirst
Thank you
janne@winlab.rutgers.edu
Ongoing work:

- Analysis on impact of disposable identifiers in MF
  - Today, routing scales because you can request only as many disposable identifiers (IP address) as have been provisioned to the network
  - In MF, you could have arbitrary number of disposable identifiers

- Reachability vs. Privacy

- Privacy by Default, what is the right level of privacy the network should provide?