Mobile Privacy and Identity

JCP EC F2F Meeting

Werner Keil

Redwood City, California
11 / 01 / 12
Goal

LIMITING WHO CAN ACCESS YOUR INFORMATION.
Terms

• **Privacy** – the right (of an individual or organization) to be “left alone” (interference / government intrusion)

• **Data Protection** – the right of an individual to control dissemination and use of their personal information

• **Confidentiality** – the right (of an individual or organization) to keep a secret

• **Security** – umbrella terms for many concepts: confidentiality, availability, integrity, authenticity, non-repudiation, …
The Tradeoff between Personalization and Privacy

- Personalization involves
  - Collection of profile and location information raising privacy concerns

- Studies\(^1\) show
  - Consumers do not opt-in to online services when they do not trust merchants for their profiles.
  - Consumers are willing to tradeoff their information with trusted vendors for convenience.
  - Even among more privacy-concerned consumers.

\(^1\) by Chellappa et al., Harn et al., and Spiekermann et al.
The Tradeoff between Personalization and Privacy (2)

- Change in the attitude of 3/4 of American consumers towards privacy from a *modest* to a *high intensity* matter

- Three segments of consumers
  - Fundamentalists
  - Unconcerned
  - Pragmatic

- The size of the pragmatic group is 125 Million.

- The challenge for businesses is to address the needs of this group
  - Provide convenience
  - Protect Privacy
Privacy issues of Location based Services

• Location of individuals must be considered a constituent of privacy data, because
  • By data matching of location data with user ID or device ID, the location of a specific person would be specified.
  • The location of a specific person may be regarded as private, except if such data has been opened to the public, it might be not private data.

• Real time privacy intrusion
  • Inter-access to location based services may cause real time privacy intrusion
Privacy issues of Location based Services (2)

• Misuse of Collected location data stored on servers
  • Misuse of such data would cause serious privacy issues, especially by data matching with other privacy data.

• Communication could be intercepted
  • Vulnerability included in such service systems may permit some types of illegal interception of data.
  • Specific location data of specific person may be involved in this communication.
Social Engineering

“Getting people to do things that they wouldn’t ordinarily do for a stranger”

– The Art of Deception, Kevin Mitnick
(earlier Sherlock Holmes)
Identity Theft

Using another’s identity for ones benefit (usually financial gain)

- Social security number
- Credit card account numbers
- Date of birth
- Driver’s license
- Passport
- Mother’s maiden name,…
- Addresses
Threats

- **Spyware** - computer software installed on a computer to intercept the user's activities on the computer, without the user's informed consent.

- **Phishing** - attempt to fraudulently acquire sensitive information by masquerading as a trustworthy entity.

- **Botnets** - collection of software robots (bots), which run autonomously and automatically on groups of remotely controlled zombie computers.
Incidents

• **T-Mobile Data Scandal** – T-Mobile reveal that potentially millions of customer records have been stolen and sold on by rogue employees.

• **iPhone/Pandora/Dictionary.com** – A proposed class-action lawsuit alleges that Apple and a handful of app makers are invading user privacy by accessing personal data from customers’ smart phones without permission and sharing it with third-party advertisers.
Incidents (2)

• **Carrier IQ**
  
  • Discovery by Android security researcher Trevor Eckhart that some Android, Nokia and BlackBerry smart phones, later also other vendors were identified contain **Carrier IQ**, a software that even tracks mobile users' keystrokes.
  
  • Google CEO Eric Schmidt distanced his company from the scandal surrounding the Carrier IQ software in remarks at an internet freedom conference in **The Hague**. During his talk he called Carrier IQ a key-logger. “[I]t actually does keep your keystrokes,” he said, “and we certainly don’t work with them and don’t support it.”

  • Apple, HTC, Samsung, Motorola, AT&T, Sprint, T-Mobile and Carrier IQ have been sued in a federal court by what the lawyers involved have deemed a “cell phone tracking software scandal.”

  • As of Jan 10, 2012, Carrier IQ website reports nearly **142,000,000** installed devices!
The DarIQ Knight ?!
“YOU HAVE ZERO PRIVACY ANYWAY. GET OVER IT.”

(Scott McNealy, CEO, Sun Microsystems, 1999)
Let's talk

Q & A