Three Significant Trends in Mobile Security: Threats and Solutions

Saurabh Bagchi
The Center for Education and Research in Information Assurance and Security (CERIAS)
School of Electrical and Computer Engineering
Purdue University

Three Big Trends

1. Malware for mobile devices
2. Mixing of sensitive and non-sensitive data
3. Snooping

For each topic, we will discuss:

- Current state
- Emerging trend
- State-of-the-art and emerging solutions

What Mobile Devices Do We Mean

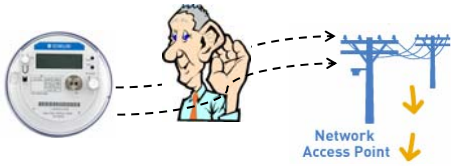
Trend 1: Malware

- Current state:
  - Isolated to small number of mobile devices, no outbreaks spreading wildly as in wired devices
  - Malware packaged as legitimate apps on app stores; releases private data of individuals
- Emerging trend:
  - Trend in medical devices from just monitoring to control; already there for smart meters
  - Drive-by downloads from web browsers
  - Worms spread by near field communication protocols such as Bluetooth
- State-of-the-art and emerging solutions:
  - You
  - Anti-malware products from well-known AV vendors from the desktop world
  - Strengthening the web browsers, which often build on the same code base
  - Single-purpose devices

Trend 2: Mixing of Sensitive and Non-sensitive Information

- Current state:
  - Same device used for multiple purposes: consider radiologist with medical images on her cell phone
  - Lack of non-porous boundary between the applications
  - When data connection is used (3G, etc.), it is not protected in the same way that wired corporate communication is
- Emerging trend:
  - Different applications sharing the same infrastructure, e.g., the location service
  - Information leak from one application to another
- State-of-the-art and emerging solutions:
  - Silos in the form of virtual machines
  - Solutions from the desktop world for preventing privilege escalation: data execution prevention and address space randomization

Trend 3: Snooping



- Current state:
  - Weak or no encryption
  - Static keys for long-lived operation
- Emerging trend:
  - Applications are becoming such that it is worthwhile to snoop
  - Computation capacity is increasing faster than communication capacity
- State-of-the-art and emerging solutions:
  - Stronger and dynamic encryption
  - Data hiding at source
  - Behavior-based detection to handle tampered or compromised sources

Unifying Themes

- We are increasingly living in a mobile world
  - Past economic driver being seen with the mobile world
  - Rush to new functionality before strengthening the functionality
  - However, economics from the dawn of the wired world do not apply here – mobile world is being born surrounded by threats
- Three trends that are motivating security research in the mobile world
  - *Malware*: from the isolated few-node cases to raging in the wild
  - *Mixing of sensitive and non-sensitive data*: co-hosting different kinds of data on a single multi-purpose device
  - *Snooping*: open communication channels, in publicly accessible places – unique challenge in the mobile world

Presentation and references to source data available at:
Dependable Computing Systems Lab (DCSL) web site
engineering.purdue.edu/dcsl