Mobile Device Security

Adam C. Champion and Dong Xuan
CSE 4471: Information Security

Based on materials from Tom Eston (SecureState), Apple, Android Open Source Project, and William Enck (NCSU)
Organization

• Quick Overview of Mobile Devices
• Mobile Threats and Attacks
• Countermeasures
Overview of Mobile Devices

- Mobile computers:
  - Mainly smartphones, tablets
  - Sensors: GPS, camera, accelerometer, etc.
  - Computation: powerful CPUs (≥ 1 GHz, multi-core)
  - Communication: cellular/4G, Wi-Fi, near field communication (NFC), etc.

- Many connect to cellular networks: billing system

- Cisco: 7 billion mobile devices will have been sold by 2012 [1]
Organization

• Quick Overview of Mobile Devices
• Mobile Threats and Attacks
• Countermeasures
Mobile Threats and Attacks

• Mobile devices make attractive targets:
  – People store much personal info on them: email, calendars, contacts, pictures, etc.
  – Sensitive organizational info too…
  – Can fit in pockets, easily lost/stolen
  – Built-in billing system: SMS/MMS (mobile operator), in-app purchases (credit card), etc.
    • Many new devices have near field communications (NFC), used for contactless payments, etc.
    • Your device becomes your credit card
  – Location privacy issues
• NFC-based billing system vulnerabilities
Mobile Device Loss/Theft

• Many mobile devices lost, stolen each year
  – 113 mobile phones lost/stolen every minute in the U.S. [15]
  – 56% of us misplace our mobile phone or laptop each month [15]
  – Lookout Security found $2.5 billion worth of phones in 2011 via its Android app [16]
  – Symantec placed 50 “lost” smartphones throughout U.S. cities [17]
    • 96% were accessed by finders
    • 80% of finders tried to access “sensitive” data on phone
Device Malware

• iOS malware: very little
• Juniper Networks: Major increase in Android malware from 2010 to 2011 [18]
• Android malware growth keeps increasing ( $$$ )
• Main categories: [19]
  – Trojans
  – Monitoring apps/spyware
  – Adware
  – Botnets
• We’ll look at notable malware examples
Device Search and Seizure

• *People v. Diaz*: if you’re arrested, police can search your mobile device without warrant [26]
  – Rationale: prevent perpetrators destroying evidence
  – Quite easy to break the law (overcriminalization) [27]
    • Crime severity: murder, treason, etc. vs. unpaid citations
    • “Tens of thousands” of offenses on the books [26]
  – Easy for law enforcement to extract data from mobile devices (forensics) [28]
Location Disclosure

- MAC, Bluetooth Addresses, IMEI, IMSI etc. are globally unique
- Infrastructure based mobile communication
- Peer-t-Peer ad hoc mobile communication
Organization

• Quick Overview of Mobile Devices
• Mobile Threats and Attacks
• Countermeasures
Mobile Access Control

• Very easy for attacker to control a mobile device if he/she has physical access
  – Especially if there’s no way to authenticate user
  – Then device can join botnet, send SMS spam, etc.
• Need access controls for mobile devices
  – Authentication, authorization, accountability
  – Authentication workflow:
    • Request access
    • Supplication (user provides identity, e.g., John Smith)
    • Authentication (system determines user is John)
    • Authorization (system determines what John can/cannot do)
Authentication: Categories

- Authentication generally based on:
  - Something supplicant knows
    - Password/passphrase
    - Unlock pattern
  - Something supplicant has
    - Magnetic key card
    - Smart card
    - Token device
  - Something supplicant is
    - Fingerprint
    - Retina scan
Authentication: Passwords

• Cheapest, easiest form of authentication
• Works well with most applications
• Also the weakest form of access control
  – Lazy users’ passwords: 1234, password, letmein, etc.
  – Can be defeated using dictionary, brute force attacks
• Requires administrative controls to be effective
  – Minimum length/complexity
  – Password aging
  – Limit failed attempts
Authentication: Smart Cards/Security Tokens

- More expensive, harder to implement
- Vulnerability: prone to loss or theft
- Very strong when combined with another form of authentication, e.g., a password
- Does not work well in all applications
  - Try carrying a smart card in addition to a mobile device!
Authentication: Biometrics

• More expensive/harder to implement
• Prone to error:
  – False negatives: not authenticate authorized user
  – False positives: authenticate unauthorized user
• Strong authentication when it works
• Does not work well in all applications
  – Fingerprint readers becoming more common on mobile devices (Atrix 4G)
Authentication: Pattern Lock

- Swipe path of length 4–9 on 3 x 3 grid
- Easy to use, suitable for mobile devices
- Problems: [30]
  - 389,112 possible patterns; (456,976 possible patterns for 4-char case-insensitive alphabetic password!)
  - Attacker can see pattern from finger oils on screen
# Authentication: Comparison

<table>
<thead>
<tr>
<th></th>
<th>Passwords</th>
<th>Smart Cards</th>
<th>Biometrics</th>
<th>Pattern Lock</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security</strong></td>
<td>Weak</td>
<td>Strong</td>
<td>Strong</td>
<td>Weak</td>
</tr>
<tr>
<td><strong>Ease of Use</strong></td>
<td>Easy</td>
<td>Medium</td>
<td>Hard</td>
<td>Easy</td>
</tr>
<tr>
<td><strong>Implementation</strong></td>
<td>Easy</td>
<td>Hard</td>
<td>Hard</td>
<td>Easy</td>
</tr>
<tr>
<td><strong>Works for phones</strong></td>
<td>Yes</td>
<td>No</td>
<td>Possible</td>
<td>Yes</td>
</tr>
</tbody>
</table>

– Deeper problem: mobile devices are designed with single-user assumption…
Current smartphone access control focus: 1 user (admin)

Hard to achieve fine-grained mobile device management:
- Control app installation/gaming
- Parental controls
- Lend phone to friend

We design DiffUser, differentiated user access control model [31]
- Different users use smartphone in different contexts
- User classification: admin, “normal,” guest

<table>
<thead>
<tr>
<th>Smartphone Privileges</th>
<th>Admin</th>
<th>Normal</th>
<th>Guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Info</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMS</td>
<td>✓</td>
<td>✓</td>
<td>✘</td>
</tr>
<tr>
<td>Contacts</td>
<td>✓</td>
<td>✓</td>
<td>✘</td>
</tr>
<tr>
<td>Resource Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WiFi</td>
<td>✓</td>
<td>✓</td>
<td>Limit!</td>
</tr>
<tr>
<td>GPS</td>
<td>✓</td>
<td>✓</td>
<td>Limit!</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>✓</td>
<td>✓</td>
<td>Limit!</td>
</tr>
<tr>
<td>Apps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>App Install</td>
<td>✓</td>
<td>Limit</td>
<td>✘</td>
</tr>
<tr>
<td>Sensitive Apps</td>
<td>✓</td>
<td>Limit</td>
<td>✘</td>
</tr>
</tbody>
</table>

Source: [31], Table 1.
DiffUser (2)

- Implement our system on Android using Java
- Override Android’s “Home” Activity for multi-user authentication, profile configuration

Source: [31], Figure 2. From left to right: “normal” user screen; user login and authentication; user profile configuration.
Mobile Device Information Leakage

- Types of mobile device information sources:
  - Internal to device (e.g., GPS location, IMEI, etc.)
  - External sources (e.g., CNN, Chase Bank, etc.)

- Third-party mobile apps can leak info to external sources [32]
  - Send out device ID (IMEI/EID), contacts, location, etc.
  - Apps ask permission to access such info; users can ignore!
  - Apps can intercept info sent to a source, send to different destination!

- Motives:
  - Monitor employees’ activity using accelerometers (cited in [32])
  - Ads, market research (include user location, behavior, etc.)
  - Malice

- How do we protect against such information leakage?
Information Flow Tracking (IFT)

- IFT tracks each information flow among internal, external sources
  - Each flow is tagged, e.g., “untrusted”
  - Tag propagated as information flows among internal, external sources
  - Sound alarm if data sent to third party

- Challenges
  - Reasonable runtime, space overhead
  - Many information sources
TaintDroid

• Enck et al., OSDI 2010 [32]
• IFT system on Android 2.1
  – System firmware (not app)
  – Modifies Android’s Dalvik VM, tracks info flows across methods, classes, files
  – Tracks the following info:
    • Sensors: GPS, camera, accelerometer, microphone
    • Internal info: contacts, phone #, IMEI, IMSI, Google acct
    • External info: network, SMS
  – Notifies user of info leakage

Source: [33]
D2Taint (1)

• Motivation
  – Mobile device users access many information sources, e.g.
    • Online banks (like Chase)
    • Social networking (like Facebook)
    • News websites (like CNN)
  – Different info sources: different sensitivity levels
  – Applications’ diverse variable access patterns challenge tag propagation
  – Users’ info source access patterns change over time
  – Need to track many information flows with moderate space, runtime overhead
D2Taint (2)

- Differentiated and dynamic tag strategy [34]
  - Information sources partitioned into differentiated classes based on arbitrary criteria
  - Example (criterion=“info sensitivity level”):
    - Classes: “highly sensitive”, “moderately sensitive”, “not sensitive”
    - Sources: Chase → “highly sensitive”; Facebook → “moderately sensitive”; CNN → “not sensitive”
  - Each class’s sources stored in a location info table
    - Source indices (0, 1, …) ↦ source names (chase.com, …)
D2Taint (3)

- D2Taint uses fixed length tag (32 bits)
  - Tag includes segments corresponding to classes
  - Each segment stores *representations* of information sources in its class
  - Representation: info source’s class table index

- Note: source table grows over time
  - Information source representation does *not* uniquely ID source
D2Taint (4)

• D2Taint implemented on Android 2.2, Nexus One smartphones

• Evaluate D2Taint: 84 popular free apps from Google Play
  – 71/84 leak some data to third parties
    • E.g., Android system version, screen resolution
    • Often, third parties are cloud computing services
    • TaintDroid cannot detect external data leakage
      – 1 bit in tag for “network”
      – Cannot track multiple external sources at once
  – 12/84 leak highly sensitive data, e.g., IMEI/EID (detected by both D2Taint, TaintDroid)

• D2Taint has overhead similar to TaintDroid’s
Location Privacy Protection

• Strong regulation
  – Corporate
  – Individual

• Dynamic MAC and Bluetooth addresses?
  – Collision
  – How often to change?

• Proxy-based communications
  – Dummy device as proxy
  – Group communications
Summary

• Mobile devices are increasingly popular
• There are many threats and attacks against mobile devices, e.g., loss/theft, sensitive information leakage, and location privacy compromise
• Mobile access control, information leakage protection, and location privacy protection, etc.
References (1)


References (2)

References (3)

23. libnfc, http://www.libnfc.org


