Mobile Device Data Collection and Its Security Attack Surfaces

March 2012

Presentation to the FedCASIC 2012 Conference

Glenn Jones

Mathematica Policy Research

MATHEMATICA
Policy Research

What Will Be Covered

- Definitions
- Data collection and mobile security
- Mobile application architectures
- Mobile attack vector classes
- Mobile security risks
- Differences between mobile and nonmobile applications
- Conclusions

Definitions

Definitions

- **Mobile device – handheld device that can have custom applications (apps) installed, such as smartphones (Android, Blackberry, iPhone, and iPad)**
- **Ordinary computer – nonmobile device such as a server or desktop and laptop computers**
- **Threat – a possible danger that might exploit a vulnerability and cause harm,[1] could be intentional or accidental**
- **Attack – an actual attempt to exploit a vulnerability**

Definitions

- **Vulnerability – Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source[2] [NIST SP 800-30]**
- **Threat model – procedure for optimizing network/application/internet security by identifying objectives and vulnerabilities[3]**
- **Trust boundary – entry point through which anyone could interact with the application[3]**
- **Attack vector – the way an attacker might attempt to exploit a vulnerability[4]**

Data Collection and Mobile Devices

Data Collection and Mobile Devices

- **The data collected are often sensitive.**
  - **Personally identifiable information (PII)**
  - **Personal health information (PHI)**
- **Data are not only the property of the device owners, but could contain sensitive data for many hundreds of people.**
- **In many scenarios the data will be transmitted.**
- **The data collected are probably covered by some form of regulatory compliance requirements (a YouTube video of a dancing cat is not).**

Mobile Application Architectures

Mobile Architectures

- **Stand-Alone**
  - Collected data are stored on the mobile device until transferred off of it.
- **Client/Server**
  - Collected data can be stored on the server but might also be stored on the mobile device.
- **Web Browser-Based**
  - Collected data are stored on the server.

Mobile Architectures – Trust Boundaries

- **All mobile architectures have common trust boundaries.**
  - **User of the mobile device**
  - **Final resting place of the collected data and other nonmobile uses for the data, such as "fill ins" subsequent surveys**
- **Each mobile architecture also has its own unique set of trust boundaries.**

Mobile Architectures – Stand-Alone Details

- All of the data collected will be stored on the mobile device
- Transmission of the data will be performed in a controlled environment, such as a USB cable from the device to a nonmobile device
- Full access to all device features (Short Message Service (SMS), phone, contact lists, Global Positioning System (GPS) data, and so on)
- Trust boundary – local nonmobile device

Mobile Architectures – Client/Server Details

- The data are usually stored on the server.
- Data may also be stored on the mobile device. Authentication information is often stored on the mobile device.
- The data will be transmitted using a wireless network (WiFi, 3G, 4G).
- Encryption may or may not be used during transmission.
- The application has full access to all device features.
- All mobile and web service risk factors apply.
- Trust boundary – internet-based web service.

Mobile Architectures – Web Browser Details

- Data are not stored on the mobile device.
- Web browsers cache data, such as security or session tokens.
- Some mobile devices store images of browser screens to increase device performance.
- Data will be transmitted using a wireless network.
- No or very limited access to other device features.
- All vulnerabilities of web applications apply.
- Trust boundary – internet-based web application.

Mobile Attack Vector Classes

Four Classes of Mobile Attack Vectors

1. Hardware-centric attacks
2. Device-independent attacks
3. Software-centric attacks
4. User layer attacks[5]

Mobile Security Attack Vectors – Hardware-Centric

- **Replacement of the SIM chip**
- **Forensic Analysis**
  - **Stolen device**
  - **Loaned device**
  - **Changed owner**

Mobile Security Attack Vectors – Device-Independent

- Possible man-in-the-middle (MitM) attack
- Rogue base station
- Problems with the encryption protocols
- SMS and MMS protocols are old (2006)
- Possible denial-of-service (DOS) attacks by depleting the mobile device battery
- Requires sophisticated techniques

Mobile Security Attack Vectors – Software-Centric

- **Web browser attack vectors from "bad" websites.**
  - Cross Site Scripting (XSS)
  - Injection (SQL, Command)
  - Cross Site Request Forgery (CSRF)
- **Malware attack vectors from "bad" apps.**
  - Information or identity theft
  - Eavsdropping
  - Financial attacks
  - Mobile botnets
  - DoS Attack against the mobile device
- **Operating system bug vulnerabilities**

Mobile Security Attack Vectors – User Layer

- **Users don't use security mechanisms correctly.**
- **Accepting non-authoritative TLS/SSL certificates.**
- **Shoulder surfing**
- **Social engineering attacks**
  - **Phishing**
  - **Device borrowing**

Mobile Security Risks

Common Security Risk Lists

- **Open Web Application Security Project (OWASP) Top 10 Mobile Risks[3]**
- **European Network and Information Security Agency (ENISA) Top 10 Smartphone Risks[6]**
  - **Based on the OWASP Top 10 Mobile Risks**
  - **Currently include more details of programming best practices**

OWASP Top 10 Mobile Risks

1. **Insecure Data Storage – Stand-alone, client/server, possibly web browser-based**
2. **Weak Server-Side Controls – client/server, web browser-based**
3. **Insufficient Transport-Layer Protection – client/server, web browser-based**
4. **Client-Side Injection – Stand-alone, client/server, possibly web browser-based**
5. **Poor Authentication and Authorization – Stand-alone, client/server, possibly web browser-based**

OWASP Top 10 Mobile Risks *(continued)*

6. **Improper Session Handling – client/server, possibly web browser-based**
7. **Security Decisions via Untrusted Inputs – Stand-alone, client/server, possibly web browser-based**
8. **Side-Channel Data Leakage – Stand-alone, client/server, possibly web browser-based**
9. **Broken Cryptography – Stand-alone, client/server**
10. **Sensitive Information Disclosure – Stand-alone, client/server, possibly web browser-based**

Other Risks

- **Device Can Be Lost or Stolen**
  - **Device can be rooted or jail broken and data can be extracted**
  - **All data on the device can be extracted even if encrypted**
- **Temporarily Loaned**
  - **All data on the device can be obtained quickly without the knowledge of the device owner**
- **Insecure Backup**
  - **Unencrypted backup could be made**
    - To a user's personal machine
    - To the cloud

Other Risks *(continued)*

- **App Installation**
  - **The installed apps could be malware**
    - Key loggers
    - Transmit PII data to an attacker's server
    - SMS text data to the attacker's phone
- **Connections to Many Untrusted Networks**
  - **All transmitted data could be sniffed**
  - **Not always safe if 3G/4G is used, can switch to unencrypted WiFi without the owner's knowledge**

Differences Between Mobile and Nonmobile Applications

Mobile versus Nonmobile

- Mobile more likely to be lost or stolen than a desktop machine
- Mobile devices might not be controlled by the IT department
  - Can IT wipe an employee's personal device?
  - What happens to sensitive data stored on an employee's personal device when the employee leaves?
- Mobile devices can join many networks, not just the one controlled by IT
- App development environments could be significantly different
  - Managed code (Java/.Net) versus unmanaged (Objective C)

Conclusions

- **The mobile security landscape is still in its infancy and constantly changing.**
- **Mobile devices are vulnerable to all of the same attack vectors as nonmobile devices.**
- **They are also vulnerable to many new, mobile-only attack vectors.**
- **Mobile security issues are now at least being discussed.**

References

- [1] Wikipedia. “Threat (computer).” (2012, February). Available at http://en.wikipedia.org/wiki/Threat_(computer). Accessed February 26, 2012.
- [2] “NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments.” (2011, September). Available at http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf. Accessed February 27, 2012.
- [3] “OWASP TOP Ten Mobile Risks.” (2012, February). Available at https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Risks. Accessed February 27, 2012.
- [4] “Definition Attack Vector.” (2004, September). Available at http://searchsecurity.techtarget.com/definition/attack-vector. Accessed February 28, 2012.
- [5] Becher, M., F.C. Fretling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. “Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices.” IEEE Security and Privacy, Oakland, May 2011.
- [6] “ENISA Top Ten Smartphone Risks.” Available at http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks. Accessed February 28, 2012.

For More Information

- **Please contact:**
  - **Glenn Jones**
    - gjones@mathematica-mpr.com