Mobile Web Apps:

What You Need to Know

Session 4

Tuesday, November 19, 2013

11:15 AM - 12:30 PM

Ming Chow

Tufts University

The Conference On
Mobile & Smart Device Security

MIS TRAINING INSTITUTE

Key Points

- Understand the physical security implications of the mobile web.
- How the user experience on the mobile web browser significantly affects security.
- Common mobile portal development mistakes including executing untrusted JSON data.
- How not to store application data.
- Session handling and authentication for mobile web apps.

What Will Not Be Discussed

- Exploits in mobile web browser a la Pwn2Own
- Mobile malware
- Common vulnerabilities and flaws in mobile applications

Motivation

- "17.4% of Global Web Traffic Comes Through Mobile" (Mashable, August 2013)
- "Mobile Devices Now Make Up About 20 Percent of U.S. Web Traffic" (All Things D, 2012)
- Breakdown by versions and features is deep (noticeably Android)

Physical Security

- Phones are high value
- Phones will be lost
- Most users do not enable device locking features

Roaming: Moving Target

- Different geolocation
- Roaming IP depending on carrier
- Going from secure to insecure wireless network (i.e., the auto Wi-Fi connect)
- Can you depend on the reliability and security of network if you are mobile?

Mobile Web Browsers

- Many similarities to desktop web browsers including support for JavaScript, plugins, dependencies on WebKit
- Still complex
- Safe guards built into mobile Safari, Opera, Firefox (e. g., Safari's XSS Auditor)
- Many sources of inputs:
  - SMS, iMessage
  - Links in emails
  - Twitter / Facebook Messaging / within native mobile apps
  - Camera
  - Push notifications

What We Know: Firefox for Android Permissions

1. Your location (fine GPS)
2. Storage (i.e., read and write to SD card)
3. Hardware controls (i.e., the camera)
4. Network communication (i.e., the Internet)
5. System Tools (e.g., to install shortcuts, wallpaper, waking up the device); you can install Adobe Flash
6. Your accounts (i.e., account syncing)
7. Your personal information (browser history and bookmarks)
8. Near Field Communication (NFC)
9. Record audio (i.e., the microphone)

Source: https://support.mozilla.org/en-US/kb/how-firefox-android-use-permissions-it-requests

Ways to Hide Information

- Notifications
- Malicious QR Codes
- Malicious short URLs
- Malicious Near field communication (NFC) tags
- Bad user interface (UI)
- Results will cause another app to open or will appear on mobile web browser.

User Interface (UI) Constraints

- The causes: hardware limitations include screen size, bandwidth
- The effects: poor keyboards, harder to convey information, phishing made easier
- Look for the lock on mobile web browser

iPhish. Yuan Niu, Francis Hsu, and Hao Chen @ UC Davis

iSEC PARTNERS

Mobile Drive-Bys and What Have Changed

- Still true for the most part:
  - 10-20x less potential targets than desktops
  - Not many mobile browsers
  - Increased costs to exploit relative to desktops
  - Feature disparities, in particular Flash support
- No longer true: "mobile websites commonly won't have ads"
  - Some ads take up the entire screen, hard to close (e.g., ESPN, Boston.com)
  - Small banners
- Results: download app from platform's app store, increase app visibility, potential malware on Android, exhaust bandwidth

Transport Layer Security (TLS)

- The big question: how good are mobile websites compared to their desktop counterpart?
  - Features?
  - Different second level domain for mobile website (or even redirecting)?
  - Using HTTPS all the way?

Data Storage

- Options, all client-side:
  - Cookies
  - Local Storage
  - Web SQL
- Usual gang of issues like that of desktop web browsers
  - Cross-site scripting (XSS)
- Limit the use of client-side storage

Weak Server Side

- The compromised server
- Insecure web services and API have greater impact now
  - Used in desktop, mobile web, and native mobile apps
- Again, is HTTPS used all the way?
- Session handling: hopefully device information is not used for session ID
- Impact: information leakage, weak authentication

Weak Client Side

- The usual gang of vulnerabilities and more
- The usual gang of recommendations: validate inputs, do not execute untrusted JSON
  - One of the few things the W3C has recommended
- Unintended downloads (especially if "Unknown sources" is checked under Application Settings in Android)
- Unintended phone calls via `tel://`
  - http://www.ietf.org/rfc/rfc3966.txt
- Unintended text messages via `sms://`
  - http://www.ietf.org/rfc/rfc5724.txt

In Summary

- Mobile web browsers and mobile web apps are still very ripe for opportunities and vulnerabilities…
- …but no major cases of data loss, alas less attention than native apps. Will change if potential revenue rises dramatically.
- The constant: easy to take advantage of humans (i.e., make them click on stuff)
- "…unsafe enough that even cyber security experts are unable to detect when their smartphone browsers have landed on potentially dangerous websites."
- Scrimping on SSL for mobile is a very bad idea
- Consistency matters

References

- http://www.w3.org/TR/2010/PR-mwabp-20101021/#bp-security
- http://www.slideshare.net/astamos/mobile-web-security-a-moving-target
- http://www.slideshare.net/JackMannino/owasp-top-10-mobile-risks
- http://www.ibm.com/developerworks/xml/tutorials/x-jquerymobilesecuritytut/index.html?ca=drs-
- http://blog.cenzic.com/2012/11/mobile-application-security-flaw-input-validation/
- http://blog.cenzic.com/2012/10/mobile-application-security-flaw-ineffective-session-termination/
- http://www.sans.org/reading-room/whitepapers/pda/website-security-mobile-34190
- http://blog.kaspersky.com/mobile-browser-security/
- http://www.nbcnews.com/technology/mobile-browser-woes-can-fool-even-experts-report-1C7451203
- http://mashable.com/2013/08/20/mobile-web-traffic/
- http://blogs.forrester.com/julie_ask/13-07-02-when_will_mobile_web_traffic_surpass_pc_traffic_for_you
- http://allthingsd.com/20120525/mobile-devices-now-make-up-about-20-percent-of-u-s-web-traffic/
- http://www.trailofbits.com/resources/mobile_eip-04-19-2012.pdf
- http://www.wallofsheep.com/pages/nfc-security-awareness-project