Mobile Devices Vulnerabilities and Attacks (1)

Lecture 6

Security of Mobile Devices

2023

General Concepts

Application Security

Remote Attack Surfaces

Bibliography

Outline

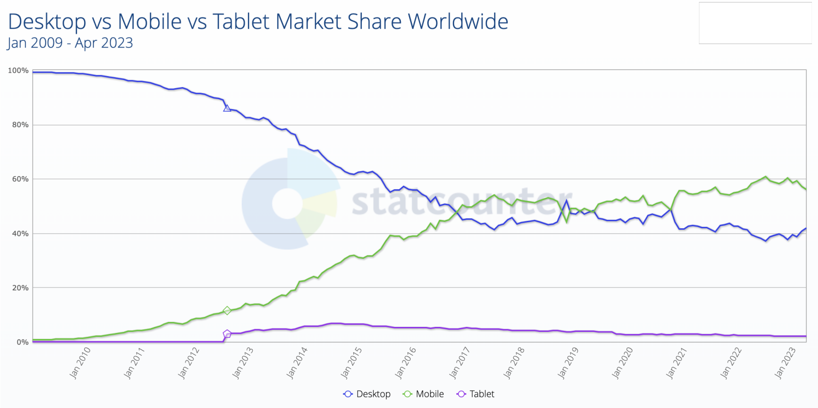
General Concepts

Application Security

Remote Attack Surfaces

Bibliography

Mobile vs Desktop



Source: statcounter.com

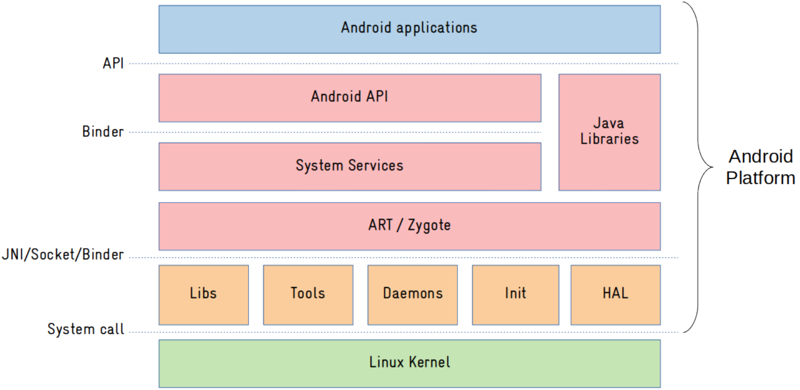
- Vulnerability
  - Weakness that can be exploited
- What can someone gain?
  - Access to confidential information
  - Root access
  - Money
  - Destructive impact

- Causes
  - Software/hardware bug
    - e.g. HeartBleed - missing boundary check in OpenSSL
  - Configuration error
    - e.g. web server accepting HTTPS with TLS v.1.0/1.1

Attack Surface

- Attack surface
  - Entry points into the system
  - Can be used to exploit a vulnerability
  - Network interfaces, USB ports, network packets, web pages, emails, etc.
- Attack vector
  - Mechanism to obtain unauthorized access
  - Break through an entrance from the attack surface

Android System Attack Surface



Source: https://sergioprado.blog/what-differs-android-from-other-linux-based-systems/

Attack Surface Classification

- Remote - anywhere in the world
- Local - vicinity of the target
- Physical - present near the target

Outline

General Concepts

Application Security

Remote Attack Surfaces

Bibliography

Android Application Attack Surface

- Activities
- Services (exposed and bound services)
- Broadcast receivers
- Content providers

Application Security - Permissions

- Permissions for performing actions outside the sandbox
- Undergranting
  - Fewer permissions than needed
  - App may crash
- Overgranting
  - More permissions than needed
  - Permissions should be correlated with app's functionality

Application Security - Data

- Insecure transmission of sensitive data in plaintext
  - Solution: end-to-end encryption
  - TLS 1.3, SHA-256, RSA with 2048 bits keys
- Insecure data storage
  - Plaintext storage, no encryption
  - Solution: encrypt data on the disk
  - Skype - logs accessed by any proces

Application Security - Logs & App Components

- Information leakage through logs
  - Excessive, very verbose logging
  - Firefox - session identifiers & cookies => session hijacking
  - Reduce logging in the release build
- Accessing app components
  - Who can access whom?
  - Activities, services, broadcast receivers, content providers
  - Solution: custom permissions for app components

Application Security - Activities

- Who can access secondary activities?
- Trick the user to perform certain actions
  - Obtain private information
  - Facilitate an exploit
- Cloak and Dagger
  - UI redressing attack
  - Clickjacking to trick the user to overgrant permissions

Cloak and Dagger Attack

- `SYSTEM_ALERT_WINDOW` permission
  - Overlay placed over another app
  - Granted automatically on the older Android versions
- `BIND_ACCESSIBILITY_SERVICE` permission
  - Tracking visual elements displayed on the screen
  - Intercept events (e.g. keyboard)
- Overlay that covers the screen except areas to be clicked
- Tricks the user to grant permission to accessibility service
- Tracks keyboard events and steals passwords

Application security - Bound Services

- Like a server interface that exposes functionality
- App services are public by default
- May provide access to private information - security breach
- Make service private if possible
- Custom permissions for public services

Application security - Content Providers

- Interface to structured data
- May expose private data
- By default, it cannot be accessed from outside the app
  - Private by default, from Android 4.2
- If public -> access control using permissions
- Granular permissions, at URI level
- Protect against SQLite injection

Application security - Broadcast Receivers

- Broadcast message - sender & receiver
- 2 permissions
  - One at the receiver - who can send the broadcast
  - One at the sender - who can receive the broadcast
- Android 8 - restrictions for implicit broadcasts
  - Cannot declare in the Manifest a receiver for an implicit broadcast
  - Some exceptions (e.g. `ACTION_BOOT_COMPLETED`)

Outline

General Concepts

Application Security

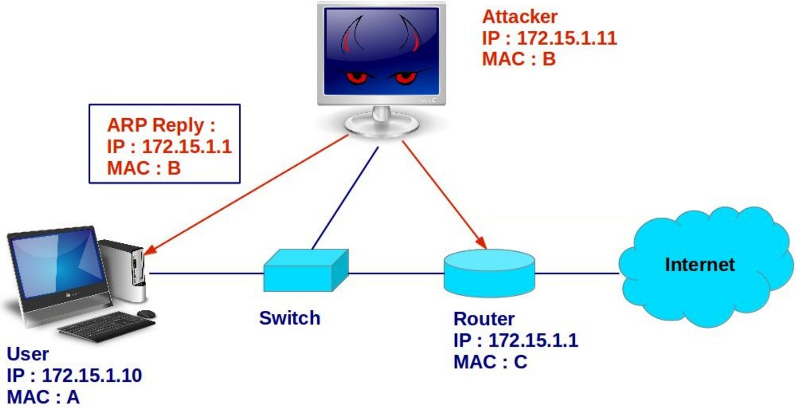
Remote Attack Surfaces

Bibliography

Network Attacks

- No network services available
- Susceptible to common network attacks
  - Spoofing attacks (ARP, DNS, DHCP)
  - Man in the middle attacks
  - TCP attacks (SYN flooding, RST attack, sequence prediction attack)
  - DoS attacks

ARP Spoofing

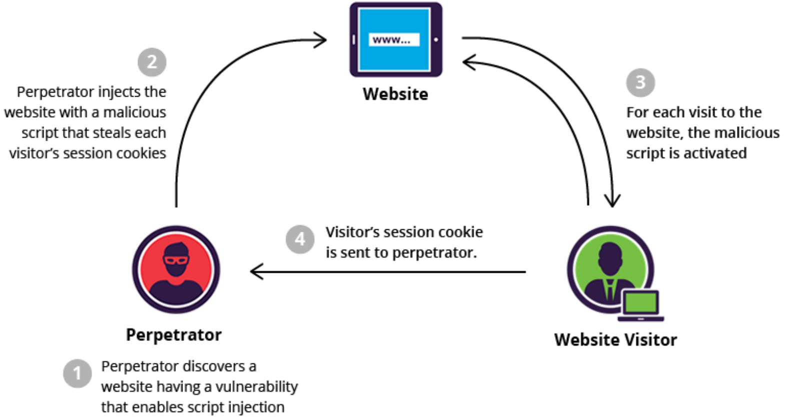


- Android Stagefright
  - Native multimedia library
  - Encoding/decoding .mpeg & .mp4
  - Unpack MMS messages
- Stagefright attack
  - Receive forged .mp4 files via MMS
  - Integer overflow leads to heap overflow
  - Execute shellcode with a reverse TCP connection callback
  - Notifies attacker that it can initiate a TCP connection

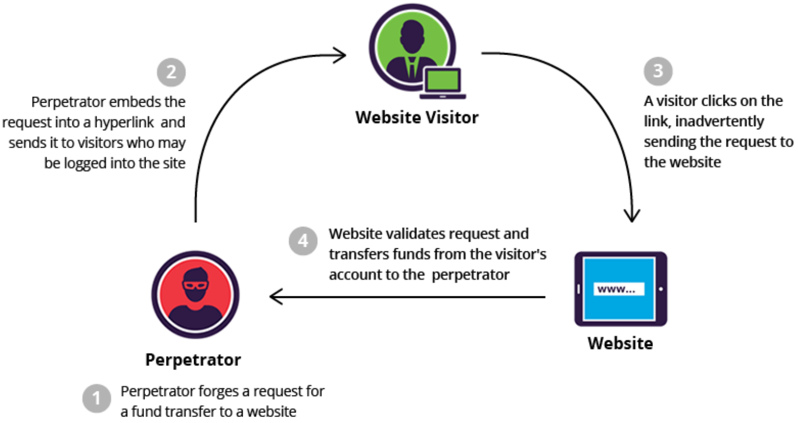
Client-side Attack Surface

- Web clients
- HTTP(S), FTP(S), HTML, JavaScript
- Browser attacks
  - Rogue URL
    - URL similar to a legitimate URL
    - Website very similar to the legitimate one
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)

Cross-Site Scripting (XSS)


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

Cross-Site Request Forgery (XSRF)



Perpetrator embeds the request into a hyperlink and sends it to visitors who may be logged into the site

A visitor clicks on the link, inadvertently sending the request to the website

Website validates request and transfers funds from the visitor's account to the perpetrator

Perpetrator forges a request for a fund transfer to a website

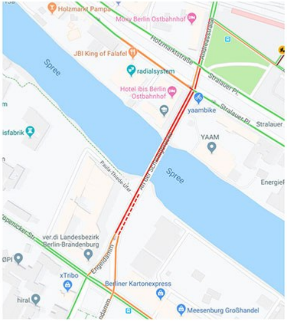
- Web-Powered mobile applications (Twitter)
- Vulnerable to MitM attacks (8% of apps on Play Store)
    - Certificates are not validated
- Authentication - validate SSL/TLS certificates

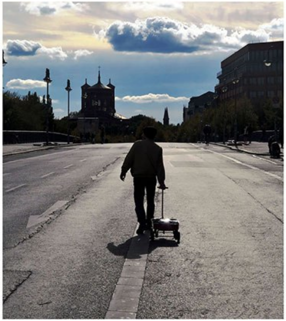
Wireless Communication Attacks - GPS

- No known attacks to fully compromise a device
  - Latitude, longitude, altitude
- GPS spoofing
  - Strongest GPS signal
  - Fake GPS signal stronger than others
  - Obtain fake location

Wireless Communication Attacks - GPS

- Google Maps Hack
  - 99 phones with Google Maps
  - Moving at low speed => traffic congestion
  - Cars were redirected to other streets





Source: `https://www.simonweckert.com/googlemapshacks.html`

Wireless Communication Attacks - Cellular

- Cellular technologies - 3G, 4G, 5G
- Cellular communications - an additional remote surface attack
- New attack vectors:
  - SMS, MMS
  - WAP push (Wireless Application Protocol)

Wireless Communication Attacks - Cellular

- Baseband modem driver
- Emulation of a rogue base station
  - Phones connected to an antenna (base station)
  - Proprietary hardware & software that is vendor specific
  - Very expensive
  - Open-source initiatives

Wireless Communication Attacks - Cellular

- RIL (Radio Interface Layer) attacks
  - AT (attention) commands sent by the mobile operator
  - Charge the user, read/write messages, downgrade OS
  - Still supported for backwards compatibility
  - Send AT commands via USB/Bluetooth

Wireless Communication Attacks - Cellular

- USSD codes
  - Request information from mobile operator
  - Instruct operator to perform actions on the phone
  - Factory reset
  - PUK reset - after 10 times, SIM card is destroyed
- Dialer attack
  - tel://URI received through SMS, Twitter post
  - URI includes an USSD code

Wireless Communication Attacks - Bluetooth

- Android Bluetooth stack (BlueDroid)
  - Weaknesses related to pairing and encryption
- Bluejacking
  - Send unsolicited messages to the target (DoS)
- Bluesnarfing
  - Gain remote access to a BT device
  - Access unrestricted data from the target

Wireless Communication Attacks - Bluetooth

- BlueBorne
  - Example of Bluesnarfing
  - Obtain unrestricted access to a remote device
  - Heap overflow by sending multiple BT discovery packets
- BlueFrag
  - Allows remote code execution
  - Using a specially crafted BT packet
  - No pairing
  - Deduce BT address from MAC address

Wireless Communication Attacks - WiFi

- Cryptographic standards: WEP, WPA, WPA2, WPA3
- Rogue AP
  - Illegitimate AP in a network
  - Software AP usually
  - Hardware AP - hard to install

Wireless Communication Attacks - WiFi

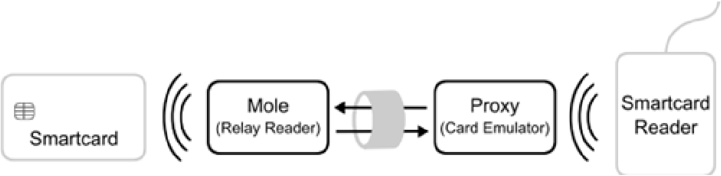
- Krack - Key Reinstallation Attack
  - Replay attack
  - 4-way handshake for the secret key in WPA2
  - 3rd message retransmitted continuously
  - Reset WPA2 encryption key
  - Multiple resets - obtain encryption key
  - Vulnerability at protocol level

Wireless Communication Attacks - NFC

- Lack of encryption and authentication
- Browser attack
  - NFC reader opens URL by default
  - Rogue URL - Javascript-injected code
  - Executes and extracts information for the attacker

Wireless Communication Attacks - NFC

- NFC relay attack
- Card reader (mole) in proximity to the card
- Card emulator device (proxy) to communicate with an actual card reader
- Fast communication channel between mole & proxy
- Command from reader -> proxy -> mole -> card (and back)



Outline

General Concepts

Application Security

Remote Attack Surfaces

Bibliography

- Android Hacker's Handbook, Joshua J. Drake, 2014
- A Survery on Smartphones Security: Software Vulnerabilities, Malware and Attacks https://thesai.org/Downloads/Volume8No10/Paper_5-A_Survey_on_Smartphones_Security.pdf
- https://joncooperworks.medium.com/cloak-and-dagger-malware-techniques-demystified-c4d8a0
- https://www.simonweckert.com/googlemapshacks.html
- https://resources.infosecinstitute.com/topic/near-field-communication-nfc-technology-vulnerabilitie

- Attack vector
- Attack surface
- Application security
- Cellular communications
- WiFi
- Bluetooth
- NFC