



Mobile Devices Vulnerabilities and Attacks (1)

Lecture 6

Security of Mobile Devices

2022



SMD

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

General concepts

Application security

Remote attack surfaces

Local attack surfaces

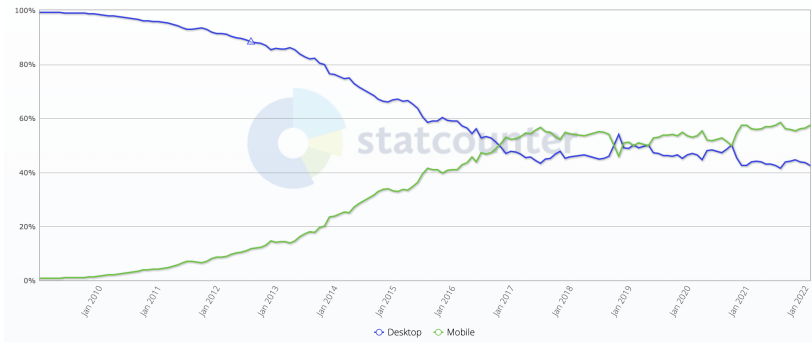
Physical attack surfaces

Bibliography

- ▶ Vulnerabilities
- ▶ What can you gain?
- ▶ Causes

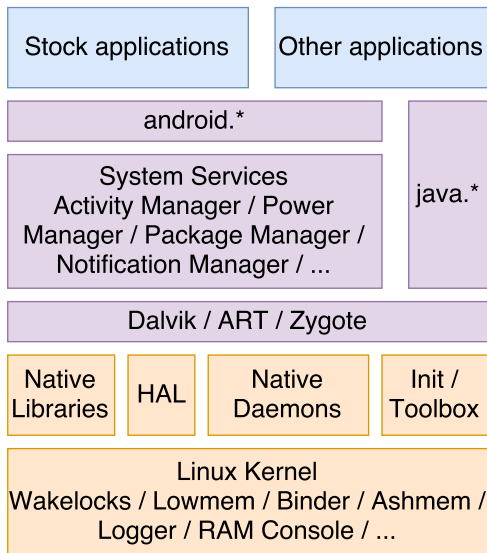
Desktop vs Mobile Market Share Worldwide

Jan 2009 - Feb 2022



Source: [statcounter.com](https://www.statcounter.com)

- ▶ Attack vector
 - ▶ Entry points into the system
 - ▶ Network interfaces, USB ports, network packets, web pages, emails, etc.
- ▶ Attack surface
 - ▶ Mechanism to obtain unauthorized access





- ▶ Remote
- ▶ Local
- ▶ Physical

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

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

- ▶ application permission issues
 - ▶ Android documentation related to permissions does not correspond with what the Android middleware actually requires
 - ▶ undergranting or overgranting permissions
- ▶ insecure transmission of sensitive data
- ▶ insecure data storage
 - ▶ plaintext storage
 - ▶ no encryption
 - ▶ Skype - world-readable, world-writable permissions, no encryption

- ▶ information leakage through logs
 - ▶ excessive, very verbose logging
 - ▶ Firefox - browsing activity, session identifiers
- ▶ insecure transmission of sensitive data
- ▶ Unsecured IPC endpoints
 - ▶ who can access whom?
 - ▶ activities - UI redressing attacks (clickjacking) - Cloak and Dagger
 - ▶ bounded services - expose functionality
 - ▶ content providers - expose data, susceptible to SQLite injection
 - ▶ broadcast receivers - implicit intents

General concepts

Application security

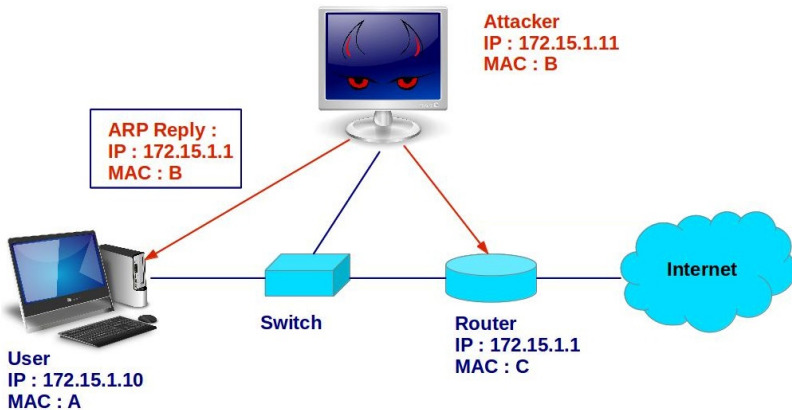
Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

- ▶ 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

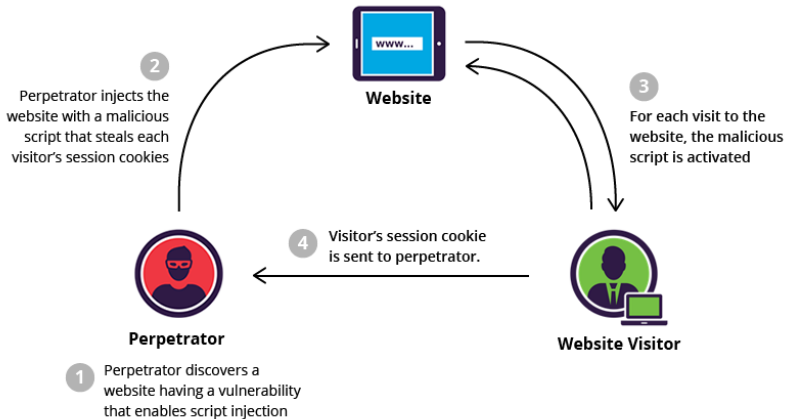


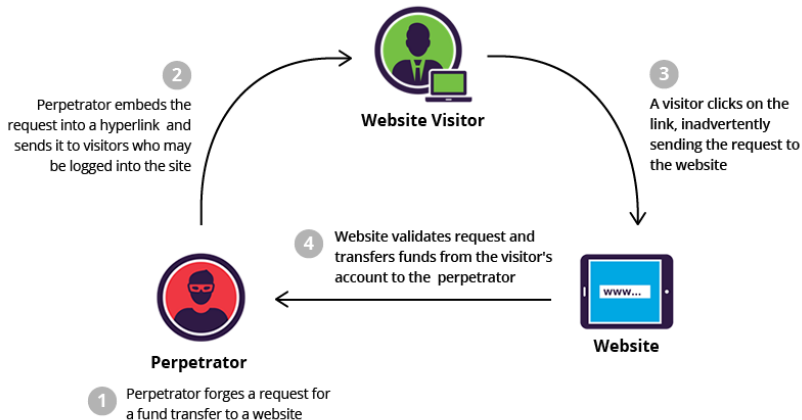
- ▶ Cellular communications - an additional remote surface attack
- ▶ SMS, MMS
- ▶ WAP push (Wireless Application Protocol)

- ▶ Dialer attack
 - ▶ tel://URI received through SMS, Twitter post
 - ▶ USSD code for factory reset
 - ▶ USSD code for resetting PUK - after 10 times, SIM card is destroyed

- ▶ Stagefright attack
 - ▶ Android native multimedia library
 - ▶ exploited through MMS, Hangouts, web browsers
 - ▶ integer overflow leads to heap overflow
 - ▶ shellcode with a reverse TCP connection callback

- ▶ Client applications
- ▶ Browser attacks
 - ▶ Plethora of technologies: HTTP(S)/FTP, HTML, JavaScript
 - ▶ rogue URL
 - ▶ cross-site scripting (XSS)
 - ▶ cross-site request forgery (CSRF)

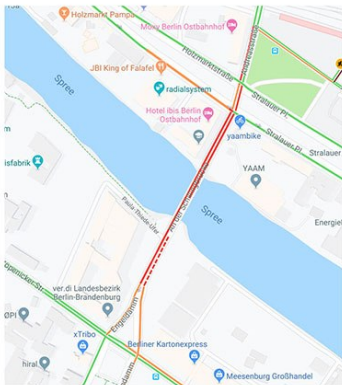




- ▶ Web-Powered mobile applications - Twitter, Dropbox
- ▶ Authentication - SSL/TLS certificates
- ▶ Apps do not adequately validate the certificates
- ▶ 8% of the apps on Google Play Store exposed to MitM attacks

GPS

- ▶ no known attacks to compromise a device
- ▶ GPS spoofing



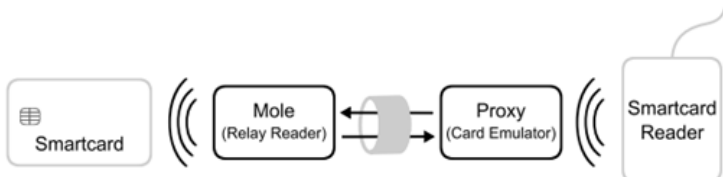
- ▶ Baseband (GSM, HSPA, LTE)
 - ▶ emulate a base station (cell tower) - specialized equipment
 - ▶ RIL (Radio Interface Layer) - AT commands through USB or Bluetooth (attention commands that can read/write messages, downgrade OS, charge the user)

▶ Bluetooth

- ▶ weaknesses related to pairing and encryption in the Android Bluetooth stack (BlueDroid)
- ▶ Bluejacking - send unsolicited messages to the target
- ▶ Bluesnarfing - access unrestricted data from the target
- ▶ BlueBorne - unrestricted access to a remote device. Heap overflow generated by sending multiple Bluetooth discovery packets.
- ▶ BlueFrag - allows remote code execution through a specially crafted Bluetooth packet. Bluetooth address can be deduced from MAC address.

- ▶ WiFi
 - ▶ WEP, WPA, WPA2, WPA3
 - ▶ rogue AP (access point)
 - ▶ Krack - Key Reinstallation Attack

- ▶ NFC
 - ▶ lack of encryption and authentication
 - ▶ browser attack
 - ▶ NFC relay attack



General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

- ▶ file system - files, pipes, character and block devices
 - ▶ F2FS (Flash Friendly File System) vulnerabilities
 - ▶ memory corruption → boundary checks → integer overflows
- ▶ TCP/IP stack
 - ▶ CVE-2014-0100
 - ▶ IPv4 fragmentation
 - ▶ race condition - fragment deleted before being added to a LRU list
 - ▶ use-after-free issue
 - ▶ internal denial of service

- ▶ binder
 - ▶ use-after-free issue caused by race conditions between binder ioctl calls
- ▶ shared memory
 - ▶ KillingInTheNameOf jailbreak
 - ▶ remaps the system properties address space to be writable
 - ▶ ro.secure = 0
 - ▶ root access through ADB

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

- ▶ dismantling the device
- ▶ USB
 - ▶ send AT commands to the RIL - issue calls, alter the pin
 - ▶ vold vulnerability - allows to overwrite filesystems through USB

General concepts

Application security

Remote attack surfaces

Local attack surfaces

Physical attack surfaces

Bibliography

- ▶ Android Hacker's Handbook, Joshua J. Drake, 2014
- ▶ A Survey on Smartphones Security: Software Vulnerabilities, Malware and Attacks

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