Mobile is Big!

3.8B mobile users worldwide. Users spend more time on mobile than on desktops today (exact numbers iffy)
Mobile Market Share

Global Smartphone Market Share (2018 Q1 - 2021 Q1)

- 10-20% Apple.
- Most Android.
Global Bias in Market Share
What’s Valuable on Phones?

Traditional (Similar to Desktop PCs)
- Steal data (e.g., contact list, email, messages, banking information, photos)
- Phishing
- Malvertising
- Join Bots

Mobile Specific
- Identify location
- Record phone calls
- Log SMS (What about 2FA SMS?)
- Send premium SMS messages
Unique Threat Model (Physical)

Powered-off devices under complete physical control of an adversary (including well-resourced nation states)

Screen locked devices under physical control of adversary (e.g. thieves)

Unlocked devices under control of different user (e.g. intimate partner abuse)

Devices in physical proximity to an adversary (with the assumed capability to control radio channels, including cellular, WiFi, Bluetooth, GPS, NFC)
Threat Model (Untrusted Code)

Android intentionally allows (with explicit consent by end users) installation of application code from arbitrary sources

- Abusing APIs supported by the OS with malicious intent, e.g. spyware
- Exploiting bugs in the OS, e.g. kernel, drivers, or system services
- Mimicking system or other app user interfaces to confuse users
- Reading content from system or other application user interfaces (e.g., screen-scrape)
- Injecting input events into system or other app user interfaces
Unique Threat Model (Network)

The standard assumption of network communication under complete control of an adversary certainly also holds for Android. Assume first hop (e.g., router) is also malicious.

Passive eavesdropping and traffic analysis, including tracking devices within or across networks (e.g. based on MAC address or other device network identifiers)

Active manipulation of network traffic (e.g. MITM on TLS)
Mobile Exploits Very Valuable

**ZERODIUM Payouts for Mobiles**

- FCP: Full Chain with Persistence
- RCE: Remote Code Execution
- LPE: Local Privilege Escalation
- SBX: Sandbox Escape or Bypass

<table>
<thead>
<tr>
<th>Payout</th>
<th>Platform</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $2,500,000</td>
<td>iOS</td>
<td>Full Chain with Persistence</td>
</tr>
<tr>
<td>Up to $2,000,000</td>
<td>Android</td>
<td>Remote Code Execution</td>
</tr>
<tr>
<td>Up to $1,500,000</td>
<td>Any OS</td>
<td>Local Privilege Escalation</td>
</tr>
<tr>
<td>Up to $1,000,000</td>
<td>iOS</td>
<td>Sandbox Escape or Bypass</td>
</tr>
</tbody>
</table>

*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*
Mobile Exploits Very Valuable

ZERODIUM Payouts for Mobiles*
- RCE: Remote Code Execution
- LPE: Local Privilege Escalation
- SBI: Sandbox Bypass or Evasion

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners. 2019 ZD © zerodium.com

ZERODIUM Payouts for Desktops/Servers*
- Windows
- macOS
- Linux
- Chrome RCE+LPE
- Safari RCE+LPE
- Microsoft RCE+LPE
- Any OS
- PWE: Virtual Machine Escape

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners. 2019 ZD © zerodium.com
Physical Security
Unlocking Device

**Typically:** Need PIN, pattern, or alphanumeric password to unlock device

Some applications (e.g., banking apps) also require entering a PIN to access the app
Swipe Code Problems

Smudge attacks [Aviv et al., 2010]
- Entering pattern leaves smudge that can be detected with proper lighting
- Smudge survives incidental contact with clothing

Another problem: entropy
- People choose simple patterns – few strokes
- At most 1,600 patterns with <5 strokes
Passcodes

How do you allow a 4-6 digit PIN and be secure?
Review: Modern Password Hashing

Store Salted Hash (Best)
- Store \((r, H(pw || r))\) and check match against \(H(input || r)\)
- Prevents attackers from pre-computing password hashes

Making sure to choose an \(H\) that’s expensive to compute:
  - **SHA-512**: 3,235 MH/s
  - **SHA-3 (Keccak)**: 2,500 MH/s
  - **BCrypt**: 43,551 H/s

Use one of bcrypt, scrypt, or pbkdf2 when building an application
iPhone Password Hashing

Come up password hashing approach where 4-6 digits takes a very long time to crack, even if the device is physically compromised…

Additional Constraints:
- Lots of computation uses up battery (limited resource)!
- Physical access allows copying secret off and cracking remotely
Secure Enclave

iPhones have a second secure processor known as "secure enclave"
- Memory is inaccessible to normal OS
- Secure boot process that ensures its software is signed
- Each secure enclave has an AES key burned in at manufacture.

Processor has instructions that allow encrypting and decrypting content using the stored key, but the key itself is never accessible (incl. via JTAG)
iPhone Unlocking

User passcode is intertwined with AES key fused into secure enclave (known as UID) when it is entered by the user

Imagine: \( \text{key} = \text{Encrypt}_{\text{UID}}(\text{passcode}) \).

This means that the key to decrypt the device can only be derived on the single secure enclave on a specific phone. Not possible to take offline and brute force.
What prevents asking secure enclave repeatedly to try different passwords?
The passcode is entangled with the device’s UID many times — requires approximately 80ms per password guess.

Imagine: \(\text{Encrypt}_{\text{UID}}(\text{Encrypt}_{\text{UID}}(\text{Encrypt}_{\text{UID}}(\text{passcode})...))\)
iPhone Unlock Time Estimate

At 80ms per password check…

- 5.5 years to try all 6 digits pins
- 5 failed attempts ⇒ 1min delay, 9 failures ⇒ 1 hour delay
  - >10 failed attempts ⇒ erase phone

All of this enforced by firmware on the secure enclave itself — cannot be changed by any malware that controls iOS
After the San Bernardino shooting in 2016, FBI tried to compel Apple to “unlock” iPhone. What were they specifically requesting?

Not possible to make password guessing any faster—innately dependent on performance of burned-in AES key.
FBI–Apple Encryption Dispute

Remember…
- 5 failed attempts ⇒ 1min delay, 9 failures ⇒ 1 hour delay
  - >10 failed attempts ⇒ erase phone

This is managed by code on the secure enclave, which can be updated by Apple, not managed in hardware.
Technical Details

The court order wanted a custom version of a secure enclave firmware that would...

1. "it will bypass or disable the auto-erase function whether or not it has been enabled" (this user-configurable feature of iOS 8 automatically deletes keys needed to read encrypted data after ten consecutive incorrect attempts)

2. "it will enable the FBI to submit passcodes to the SUBJECT DEVICE for testing electronically via the physical device port, Bluetooth, Wi-Fi, or other protocol"

3. "it will ensure that when the FBI submits passcodes to the SUBJECT DEVICE, software running on the device will not purposefully introduce any additional delay between passcode attempts beyond what is incurred by Apple hardware"
What happened?

Apple planned to fight the order, “The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. This moment calls for public discussion, and we want our customers and people around the country to understand what is at stake.”

One day before hearing, FBI dropped the request, saying a third party had demonstrated a possible way to unlock the iPhone in question. No precent set re all writs act.
Secure Boot Chain

Why couldn’t the FBI just upload their own firmware onto the secure enclave?

When an iOS device is turned on, it executes code from read-only memory known as Boot ROM. This immutable code, known as the hardware root of trust, is laid down during chip fabrication, and is implicitly trusted.

The Boot ROM code contains the Apple Root CA public key, which is used to verify that the bootloader is signed by Apple. This is the first step in the chain of trust where each step ensures that the next is signed by Apple.
Software Updates

To prevent devices from being *downgraded* to older versions that lack the security updates, iOS uses *System Software Authorization*.

Device connects to Apple with cryptographic descriptors of each component update (e.g., boot loader, kernel, and OS image), current versions, a random nonce, and device specific Exclusive Chip ID (ECID).

Apple signs device-personalized message allowing update, which boot loader verifies.
Files are encrypted through a hierarchy of encryption keys.

Application files written to Flash are encrypted:

- Per-file key: encrypts all file contents (AES-XTS)
- Class key: encrypts per-file key (ciphertext stored in metadata)
- File-system key: encrypts file metadata
Files are encrypted through a hierarchy of encryption keys.

By default (no FaceID, TouchID), class encryption keys are erased from memory of secure enclave whenever the device is locked or powered off.

When TouchID/FaceID is enabled, class keys are kept and hardware sensor sends fingerprint image to secure enclave. All ML/analysis is performed within the secure enclave.
How Secure is TouchID?

Easy to build a fake finger if you have someone’s fingerprint

- Several demos on YouTube. ~20 min
- Similar work on FaceID

The problem: fingerprints are not secret. Cannot replace.

Convenient, but more secure solutions exist, e.g., unlock phone via bluetooth using a wearable device
More Information

iOS Security

Bring Your Own Device (BYOD)

Many companies are now allowing users to bring/use their own personal devices — company data resides on devices.

In the past, enterprise workstations were centrally managed.

How do you handle when users want to bring their own devices?
Mobile Device Management

Manage mobile devices across organization

Consists of central server and client-side software. Now part of mobile OSes too.

Allows:
- Diagnostics, repair, and update
- Backup and restore
- Policy enforcement (e.g. only allowed apps)
- Remote lock and wipe
- GPS Tracking
Sample MDM Enrollment

User consent

user’s phone

enrollment

server cert

push notification to request check in

HTTPS connection to report status and receive instructions

configure, query, lock, wipe, ...

MDM enterprise server

policy file
Mobile Malware
What’s Different?

Applications are isolated
- Each runs in a separate execution context
- No default access to file system, devices, etc.
- Different than traditional OSes where multiple applications run with the same user permissions!

Applications are installed via App Store (and malware spreads)
- Market: Vendor controlled (Apple) / open (Android)
- User approval of permissions
Android Isolation

Based on Linux with sandboxes (SE Linux)

- Apps run as separate UIDs, in separate processes.
- Memory corruption errors only lead to arbitrary code execution in application, not complete system compromise!
- Can still escape sandbox – must compromise Linux kernel
What is Rooting?

Allows user to run applications with root privileges, e.g., modify/delete system files and app, CPU, network management

Done by exploiting vulnerability in firmware to install a custom OS or firmware image

Double-edged sword... lots of malware only affects rooted devices
Examples of Malware

DroidDream (Android)
- Over 58 apps uploaded to Google app market
- Conducts data theft; send credentials to attackers

Zitmo (Symbian, BlackBerry, Windows, Android)
- Poses as mobile banking application
- Captures info from SMS – steal banking 2FA codes
- Works with Zeus botnet

Ikee (iOS)
- Worm capabilities (targeted default ssh password)
- Worked only on jailbroken phones with ssh installed

Attacked vulnerability in Android itself
Malicious application that tricked users
Attacked vulnerability in rooted iPhones
Large Target for Attackers

[Zhou et al.]

The Cumulative Number of New Malware Samples

2010 2011

DroidKungFu (including its variants)

AnserverBot

1260
678
527
403
209
115
66
66
33
23
18
13
13
14
11
12
01
02
03
04
05
06
07
08
09
10
11
Legitimate Apps Too…

Hornyack et al.: 43 of 110 Android applications sent location or phone ID to third-party advertising/analytics servers.

Android flashlight app tracks users via GPS, FTC says hold on
Challenges with Isolated Apps

So mobile platforms isolate applications for security, but....

1) Permissions: How can applications access sensitive resources?

2) Communication: How can applications communicate with each other?
Mobile Permissions
(1) Permission Granting Problem

Smartphones (and other modern OSes) try to prevent such attacks by limiting applications’ default access to:

- System Resources (clipboard, file system)
- Devices (e.g., camera, GPS, phone, …)

How should operating system grant permissions to applications?

Standard approach: Ask the user.
State of the Art

**Prompts (time-of-use)**

![Image of a prompt asking to use location services](image1)

**Manifests (install-time)**

![Image of app permissions](image2)
State of the Art

Prompts (time-of-use)

Disruptive. Leads to user fatigue

Manifests (install-time)
State of the Art

**Prompts** *(time-of-use)*

"WhereIsMyCar" Would Like to Use Your Current Location

*Don't Allow*  *OK*

Disruptive. Leads to user fatigue

**Manifests** *(install-time)*

No context. Users do not understand.
State of the Art

Prompts (time-of-use)

Disruptive. Leads to user fatigue

Manifests (install-time)

No context. Users do not understand.

In practice, both are overly permissive:
Once granted permissions, apps can misuse them.
Are Manifests Usable? (Felt et al)

Do users pay attention to permissions?

- 42% Looked at permissions
- 42% Didn’t look, but aware
- 17% Unaware of permissions

24 observed installations

... but 88% of users looked at reviews.
Do users act on permission information?

“Have you ever not installed an app because of permissions?”

25 interview responses

- Yes: 20%
- No: 72%
- Probably: 8%
Developers Don’t know the Permissions They Need

- Overprivileged: 67.3%
- Possible false positives: 30.4%
- Not overprivileged: 2.3%

Number of extra permissions:
- 1: 20%
- 2: 10%
- 3: 5%
- 4+: 5%
Android Now Asks at Runtime (was not the case historically)
Manifests

In both cases, the Android app needs to request permission in its manifest—it’s just up to the Android OS when it asks the user.

The OS might also just grant the right if it doesn’t seem dangerous.

Manifest also defines what exported endpoints other apps can access. Whole class of malware that takes advantage of this of misconfiguration.
Inter-App Communication
Primary mechanism for IPC between app components in Android: *Intents*

**Explicit:** specify name: e.g., com.example.testApp.MainActivity

**Implicit:** Specify action (e.g., ACTION_VIEW) and/or data (URI & MIME type)

An implicit intent specifies an action that can invoke any app on the device able to perform the action. Using an implicit intent is useful when your app cannot perform the action, but other apps probably can and you'd like the user to pick which app to use.
Intent Eavesdropping

Attack #1: Eavesdropping / Broadcast Theft

com.example.goodapp1

com.example.goodapp2

com.example.badapp
Unauthorized Intent Receipt

Figure 1. How an implicit intent is delivered through the system to start another activity: [1] Activity A creates an Intent with an action description and passes it to startActivity(). [2] The Android System searches all apps for an intent filter that matches the intent. When a match is found, [3] the system starts the matching activity (Activity B) by invoking its onCreate() method and passing it the Intent.

“Caution: To ensure that your app is secure, always use an explicit intent when starting a Servier. Using an implicit intent to start a service is a security hazard because you can't be certain what service will respond to the intent, and the user can't see which service starts.”
Intent Spoofing

- **Attack #1**: General intent spoofing
  - Receiving implicit intents makes component public.
  - Allows data injection.
- **Attack #2**: System intent spoofing
  - Can’t directly spoof, but victim apps often don’t check specific “action” in intent.
Security Dialogues
We inundate users with security alerts.
Example: IE 6 Mixed Context

"Yes", the possibly less safe option, is the default

How should the user make this decision? No clear steps for user to follow.
Example: IE 8 and 9 Improvement

IE8:

Security Warning

Do you want to view only the webpage content that was delivered securely?
This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

More Info  Yes  No

IE9:

Even better: load the safe content, and use the address bar to enable the rest.
Interaction Guidelines

Philosophy:
– Does the user have unique knowledge the system doesn’t?
– Don’t involve user if you don’t need to — leads to alert fatigue
– If you involve the user, enable them to make the right decision

Make sure your security dialogs are NEAT:
– Necessary: Can the system take action w/o the user? Does user have more information?
– Explained: Does the dialogue include enough information to be understandable?
– Actionable: Can user make correct decision in malicious and benign situation?
– Tested: Test with users who haven’t used system in both malicious/benign situations.
Internet Explorer Bad Certificate Example

Source

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Risk

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Choices

- Click here to close this webpage.
- Continue to this website (not recommended).

Process

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

For more information, see "Certificate Errors" in Internet Explorer Help.
Chrome 2019 Bad Certificate Example

Risk

Explanation

Your connection is not private

Attackers might be trying to steal your information from expired.badssl.com (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

- Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Choices

Advanced

Back to safety
Chrome 2019 Bad Certificate Example

This server could not prove that it is expired.badssl.com; its security certificate expired 1,483 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Saturday, May 4, 2019. Does that look right? If not, you should correct your system's clock and then refresh this page.

Proceed to expired.badssl.com (unsafe)
Secure Messaging
Email Protection

Your email provider may be required to turn over your (securely stored) email

- Warrant (for content)

Metadata

- National Security Letter (NSL), Court Order

What if you want to protect email content?
Modern implementations: GnuPG, Keybase

Each user has:
- A public encryption key, paired with a private decryption key
- A private signature key, paired with a public verification key

How does sending/receiving work?
How do you find out someone's public key?
To send a message:
   Sign with your signature key
   Encrypt message and signature with recipient's public encryption key

To receive a message:
   Decrypt with your private key to get message and signature
   Use sender's public verification key to check sig
How do you obtain Bob's public key?
Get it from Bob's website? 😞
Get it from Bob's website, verify using out-of-band communication
  Keys are unwieldy fingerprints
  A fingerprint is a cryptographic hash of a key

What if you don't personally know Bob?
Web of Trust (WoT)
Social Network (Keybase)
What if Bob's machine compromised?

His key material becomes known

Past messages can be decrypted and read

You also have sender's signature on messages sent, so you can prove identity of sender

Sender must trust recipient's ability/desire to keep her statements private
1. Use authenticated Diffie-Hellman to establish a (short-lived) session key $EK$

$$SS = (g^y)^x$$
$$EK = H(SS)$$

$Sign_{alice}(g^x)$

$Sign_{bob}(g^y)$

$$SS = (g^x)^y$$
$$EK = H(SS)$$
OTR: Off the Record Chat

2. Then use symmetric encryption on message \( M \) ...

and authenticate using a MAC

\[
SS = (g^y)^x \\
EK = H(SS) \\
MK = H(EK)
\]

\[
SS = (g^x)^y \\
EK = H(SS) \\
MK = H(EK)
\]
OTR: Off the Record Chat

3. Re-key using Diffie-Hellman

\[ SS' = (g^{y'})^{x'} \]
\[ EK' = H(SS') \]
\[ MK' = H(EK') \]
\[ MK = H(EK) \]
OTR: Off the Record Chat

4. Publish old MK

Alice

\[ SS' = (g^{y'})^{x'} \]
\[ EK' = H(SS') \]
\[ MK' = H(EK') \]

MK →

Bob

\[ SS' = (g^{x'})^{y'} \]
\[ EK' = H(SS') \]
\[ MK' = H(EK') \]

“Deniability”
Note this is suited to interactive communication, not so much email.

But, OTR provides
- message confidentiality
- authentication
- perfect forward secrecy
- deniability

OTR has since lost popularity. Signal Protocol now de facto standard.