What’s New in Security?
What’s New in Security?

Network Security
What’s New in Security?

Network Security
Cryptography APIs
What’s New in Security?

Network Security
Cryptography APIs
Platform Security on macOS
What’s New in Network Security

Lucia Ballard Secure Transports Engineering Manager
Secure Communications
Secure Communications

HTTPS is the new HTTP

• Confidentiality
• Data integrity
Secure Communications

HTTPS is the new HTTP

• Confidentiality
• Data integrity

Not all HTTPS is created equal
App Transport Security
Current standards
App Transport Security

Current standards

For NSURLSession and NSURLConnection APIs
App Transport Security

Current standards

For NSURLSession and NSURLConnection APIs

• TLS v1.2
App Transport Security

Current standards

For NSURLSession and NSURLConnection APIs

- TLS v1.2
- Strong crypto—AES-128 and SHA-2
App Transport Security
Current standards

For NSURLSession and NSURLConnection APIs

• TLS v1.2
• Strong crypto—AES-128 and SHA-2
• Forward secrecy—ECDHE
App Transport Security
Current standards

For NSURLSession andNSURLConnection APIs
• TLS v1.2
• Strong crypto—AES-128 and SHA-2
• Forward secrecy—ECDHE

Exceptions—global or for particular domains
App Transport Security Enforcement
App Transport Security Enforcement

Enforced at the end of 2016
App Transport Security Enforcement

Enforced at the end of 2016
Reasonable justification required for most exceptions

- NSAllowsArbitraryLoads
- NSExceptionAllowsInsecureHTTPLoads
- NSExceptionMinimumTLSVersion
App Transport Security Enforcement

Enforced at the end of 2016
Reasonable justification required for most exceptions
• NSAllowsArbitraryLoads
• NSExceptionAllowsInsecureHTTPLoads
• NSExceptionMinimumTLSVersion
Example—Communicating with a specific third-party server
App Transport Security Enforcement

Enforced at the end of 2016
Reasonable justification required for most exceptions

- NSAllowsArbitraryLoads
- NSExceptionAllowsInsecureHTTPLoads
- NSExceptionMinimumTLSVersion

Example—Communicating with a specific third-party server
App Transport Security Enforcement
App Transport Security Enforcement

New exceptions to make it easier
App Transport Security Enforcement

New exceptions to make it easier
• Streaming media using AVFoundation
App Transport Security Enforcement

New exceptions to make it easier

• Streaming media using AVFoundation
• Web content using WKWebView
New exceptions to make it easier

- Streaming media using AVFoundation
- Web content using WKWebView

```
NSAppTransportSecurity : Dictionary {
    NSAllowsArbitraryLoads : Boolean
    NSAllowsArbitraryLoadsInWebContent : Boolean
}
```
Evolving Standards
Deprecation of older algorithms
Evolving Standards

Deprecation of older algorithms

RC4 disabled by default
Evolving Standards

Deprecation of older algorithms

RC4 disabled by default
SSLv3 disabled in SecureTransport
Evolving Standards

Deprecation of older algorithms

RC4 disabled by default
SSLv3 disabled in SecureTransport
Other algorithms showing their age
- SHA-1
- 3DES
Evolving Standards

Deprecation of older algorithms

RC4 disabled by default
SSLv3 disabled in SecureTransport
Other algorithms showing their age
• SHA-1
• 3DES

Now is the time to upgrade your servers
Certificates
Certificates

Strong TLS is not enough
Certificates

Strong TLS is not enough

Certificate ensures that you’re talking to the right server
Certificates Today

Certificate Authority

Server

Client
Certificates Today

Certificate Authority

Server

Client
Certificates Today

Certificate Authority

Server

Certificate

Client
Certificates Today
What could go wrong?
Certificates Today
What could go wrong?

Certificate Authority
Server
Client
Certificates Today
What could go wrong?

Certificate Authority

Server

Attacker’s Server

Client
Certificates Today
What could go wrong?
Certificates Today
What could go wrong?

Certificate Authority

Server

Attacker’s Server

Client
Certificate Transparency
Certificate Transparency

Public verifiable logs of issued certificates
Certificate Transparency

Public verifiable logs of issued certificates
Anyone can submit a certificate to a log
Certificate Transparency

Public verifiable logs of issued certificates
Anyone can submit a certificate to a log
Client checks for proof that certificate has been logged
• In the certificate itself
• In a TLS extension
• Delivered via OCSP stapling
Certificate Transparency
How it works
Certificate Transparency

How it works

Certificate Authority

Server

Client
Certificate Transparency

How it works
Certificate Transparency

How it works

Certificate Authority

Certificate

Server

Log

Client
Certificate Transparency

How it works

Certificate Authority → Certificate → Log → Server → Client
Certificate Transparency

How it works

- Certificate Authority
- Server
- Client
- Log
Certificate Transparency

How it works
Certificate Transparency
Makes attacks more difficult
Certificate Transparency

Makes attacks more difficult
Certificate Transparency

Makes attacks more difficult

Certificate Authority

Server

Certificate rejected by client

Attacker’s Server

Client
Certificate Transparency
Makes attacks more difficult
Certificate Transparency
Makes attacks more difficult

Certificate Authority

Server

Attacker’s Server

Certificate

Publicly visible

Log

Client
Certificate Transparency

How to try it out
Certificate Transparency

How to try it out

You can require Certificate Transparency through App Transport Security
Certificate Transparency
How to try it out

You can require Certificate Transparency through App Transport Security

```
NSAppTransportSecurity {
    NSExceptionDomains {
        example.com : {
            NSRequiresCertificateTransparency : YES
        }
    }
}
```
Certificate Transparency

How to try it out

You can require Certificate Transparency through App Transport Security

```swift
NSAppTransportSecurity {
    NSExceptionDomains {
        example.com: {
            NSRequiresCertificateTransparency : YES
        }
    }
}
```

Proofs required from at least two logs

More information at certificate-transparency.org
Revocation

Best practices
Revocation
Best practices

Certificate Transparency does not replace revocation
Revocation
Best practices

Certificate Transparency does not replace revocation

Recommended practice—OCSP stapling

• Enhancement to the Online Certificate Status Protocol (OCSP)
OCSP

Certificate Authority

Server

Certificate

Client
OCSP

Certificate Authority

Server

Certificate

Client

Certificate
OCSP Stapling
OCSP Stapling
OCSP Stapling
Benefits of OCSP Stapling
Benefits of OCSP Stapling

Reliable, quick revocation information
Benefits of OCSP Stapling

Reliable, quick revocation information

Protects your users’ privacy
Benefits of OCSP Stapling

- Reliable, quick revocation information
- Protects your users’ privacy
- Deliver certificate transparency proofs as well
Benefits of OCSP Stapling

Reliable, quick revocation information

Protects your users’ privacy

Deliver certificate transparency proofs as well

Widely supported and backwards-compatible

• Now fully supported on all Apple platforms
Summary

Network security
Summary

Network security

Move forward to secure algorithms and ciphers—TLS v1.2, forward secrecy, and SHA-2 certificates
Summary

Network security

Move forward to secure algorithms and ciphers—TLS v1.2, forward secrecy, and SHA-2 certificates

Add your certificates to certificate transparency logs
Summary

Network security

Move forward to secure algorithms and ciphers—TLS v1.2, forward secrecy, and SHA-2 certificates

Add your certificates to certificate transparency logs

Enable OCSP stapling
Cryptographic Improvements
SecKey and smart cards
SecKey Improvements
SecKey Improvements

API for asymmetric keys

• Unification of macOS and iOS APIs
• Support for common operations
SecKey Improvements

API for asymmetric keys

- Unification of macOS and iOS APIs
- Support for common operations

Replacement for deprecated CDSA calls
SecKey Improvements

API for asymmetric keys

• Unification of macOS and iOS APIs
• Support for common operations

Replacement for deprecated CDSA calls
Replacement for asymmetric SecTransforms
CryptoTokenKit
CryptoTokenKit

System support for cryptographic devices
• Smart cards, USB cryptographic tokens
CryptoTokenKit

System support for cryptographic devices

• Smart cards, USB cryptographic tokens

Out-of-the-box integration with system services

• Token content accessible through keychain

• Token cryptographic operations available using SecKey API
CryptoTokenKit

System support for cryptographic devices
• Smart cards, USB cryptographic tokens

Out-of-the-box integration with system services
• Token content accessible through keychain
• Token cryptographic operations available using SecKey API

More information in Security Labs
What’s New in Platform Security

Simon Cooper Trusted Execution Engineering Manager
What’s New in Security
What’s New in Security

How Software is Delivered
What’s New in Security

How Software is Delivered
Developer ID
What’s New in Security

How Software is Delivered
Developer ID
Gatekeeper
What’s New in Security

How Software is Delivered
Developer ID
Gatekeeper
Software Packaging
How Software is Delivered
Software Delivery for iOS
Software Delivery for iOS

App Store
Software Delivery for iOS

App Store
Xcode
Software Delivery for iOS

App Store
Xcode
Enterprise programs
Software Delivery for macOS
Software Delivery for macOS

Mac App Store
Software Delivery for macOS

Mac App Store
Developer ID
What is Developer ID?
What is Developer ID?

Deliver apps outside of the App Store
What is Developer ID?

Deliver apps outside of the App Store
Usually downloaded
What is Developer ID?

Deliver apps outside of the App Store
Usually downloaded
Developer ID Signing Identity
What is Developer ID?

Deliver apps outside of the App Store
Usually downloaded
Developer ID Signing Identity
Developer ID Signed Apps treated specially
iCloud for Developer ID
iCloud for Developer ID

Developer ID can now use iCloud features

• iCloud Drive
• iCloud Keychain
• Push Notifications
• VPN
iCloud for Developer ID

Deliver iCloud-enabled Apps outside of the App Store
iCloud for Developer ID

Deliver iCloud-enabled Apps outside of the App Store

Developer ID apps can now share data with iCloud iOS apps
iCloud for Developer ID

Deliver iCloud-enabled Apps outside of the App Store

Developer ID apps can now share data with iCloud iOS apps

Deploy back to macOS 10.9
iCloud for Developer ID
iCloud for Developer ID

iCloud Development testing today
iCloud for Developer ID

iCloud Development testing today
iCloud Deployment
• Testing in upcoming seeds
• Distribution using GM tools
Gatekeeper
What is Gatekeeper?
What is Gatekeeper?

Controls what software is allowed to run on your Mac

• Mac App Store
• Mac App Store and identified developers
• Anywhere
What is Gatekeeper?

Controls what software is allowed to run on your Mac

- Mac App Store
- Mac App Store and identified developers
- Anywhere

Prompts user before first run
Changes to Gatekeeper
Changes to Gatekeeper

Changing the default options

- Mac App Store
- Mac App Store and identified Developers
- Can still open anyway
Changes to Gatekeeper
Changes to Gatekeeper

Repackaging problem
Gatekeeper enhancement
Repackaging Problem

**Container:** Zip, DMG, ISO

**Correctly Signed App**

**External Resources**

**Code or Code equivalent**

Libraries, plugins, HTML, Lua, Python, etc.
Repackaging Problem

Correctly Signed App

App

Code or Code equivalent Libraries, plugins, HTML, Lua, Python, etc.

External Resources
Repackaging Problem

App

External Resources

Code or Code equivalent Libraries, plugins, HTML, Lua, Python, etc.
Repackaging Problem

App

External Resources
Repackaging Problem

- App
- External Resources
Repackaging Problem

App

External Resources
Repackaging Problem

- **App**
- **External Resources**
Repackaging Problem

App

Malicious Content
Repackaging Problem
Repackaging Problem

Not affected

• From the Mac App Store
• In a signed Apple Installer package
Repackaging Problem
Repackaging Problem

Affected

• ZIP
• Disk Images (DMGs)
• ISO Images
• Other archive formats
Repackaging Problem

Affected
• ZIP
• Disk Images (DMGs)
• ISO Images
• Other archive formats

Maybe affected
• 3rd-party installers
Repackaging Problem
Repackaging Problem

Need your help
Repackaging Problem

Need your help
We need to protect customers
Containers
ZIP, DMG, ISO

Diagram:
- App
- External Resources
Signing Disk Images

![Diagram showing an app and external resources]

- App
- External Resources
Signing Disk Images

Using macOS 10.11.5 or later

App

External Resources
Signing Disk Images

Using macOS 10.11.5 or later
Use the “codesign” tool
Signing Disk Images

Using macOS 10.11.5 or later
Use the “codesign” tool
Signatures are embedded
Signing Disk Images

Using macOS 10.11.5 or later
Use the “codesign” tool
Signatures are embedded
Backwards-compatible with older OS releases
Signing Disk Images

Using macOS 10.11.5 or later
Use the “codesign” tool
Signatures are embedded
Backwards-compatible with older OS releases
For assistance, come to the Security Labs
Packaging Advice

Do these

Avoid the problem

• Put resources inside App Bundle
Packaging Advice
Do these

Avoid the problem
• Put resources inside App Bundle
Packaging Advice

Do these
Packaging Advice

Do these

Distributing an App Bundle?

- Deliver via the Mac App Store
- Sign the App
  - Package in a Zip Archive
  - Verify signature before release
- Signed Apple Installer package
Packaging Advice
Do these
Packaging Advice
Do these

For a container with Apps and resources
• Signed Disk Image
• Sign any content in the container
• Sign the disk image
• Verify signatures before release
Packaging Advice
Packaging Advice

Do These

Adding personalization or licensing information

• Use extended attribute on bundle root—see TN2206

• Sign a personalized Disk Image
Packaging Advice

Do These

Adding personalization or licensing information
- Use extended attribute on bundle root—see TN2206
- Sign a personalized Disk Image

Do Not Do This

Modify your app after signing
Deliver an app with a broken signature
Use an ISO image
Gatekeeper Enhancement

Protecting customers
Gatekeeper Path Randomization
Gatekeeper Path Randomization

Supplements existing Gatekeeper protections
Gatekeeper Path Randomization

Supplements existing Gatekeeper protections

No change for Mac App Store apps
Gatekeeper Path Randomization

Supplements existing Gatekeeper protections

No change for Mac App Store apps
No change for previously run apps
Gatekeeper Path Randomization

Supplements existing Gatekeeper protections

No change for Mac App Store apps

No change for previously run apps

Applies to newly downloaded apps
Gatekeeper Path Randomization

Supplements existing Gatekeeper protections

No change for Mac App Store apps
No change for previously run apps

Applies to newly downloaded apps
Applies to apps on unsigned Disk Images
Gatekeeper Path Randomization
In a folder or Disk Image

Your App
Extra Resources
Gatekeeper Path Randomization

When app is running

Your App
Gatekeeper Path Randomization

When app is running

Your App
Gatekeeper Path Randomization

When app is running

Your App
Gatekeeper Path Randomization

Does not apply
Gatekeeper Path Randomization

Does not apply

User moves just the app bundle

- Must only move a single app bundle
Gatekeeper Path Randomization

Does not apply

User moves just the app bundle
- Must only move a single app bundle

Signed Disk Images
Gatekeeper Path Randomization
Does not apply

User moves just the app bundle
  • Must only move a single app bundle

Signed Disk Images
Signed Apple installer package
Gatekeeper Path Randomization

Does not apply

User moves just the app bundle
- Must only move a single app bundle

Signed Disk Images

Signed Apple installer package

Apps from the Mac App Store
Summary

Sign what you deliver
Check the signatures are valid
More Information

<table>
<thead>
<tr>
<th>Labs</th>
<th>Frameworks Lab</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security &amp; Privacy Lab 1</td>
<td>C</td>
<td>Wednesday</td>
</tr>
<tr>
<td>Security &amp; Privacy Lab 2</td>
<td>B</td>
<td>Thursday</td>
</tr>
</tbody>
</table>