Your Apps and Evolving Network Security Standards

Session 701

Bailey Basile, Secure Transports Engineer
Chris Wood, Secure Transports Engineer
Best practices
Best practices

App Transport Security update
Best practices
App Transport Security update
Transport Layer Security
Best Practices
Best Practices
Best Practices

No “set and forget”
Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices
Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries
Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options
Best Practices

No “set and forget”

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options

ATS enforces best practices
Best Practices

No "set and forget"

Standards bodies, academic research, and industry best practices

Update libraries

OS removes insecure options

ATS enforces best practices

Worth the maintenance cost
Best Practices

BEAST  FREAK  CRIME  POODLE
Sweet32  SLOTH  NOMORE  FLAME
SHAttered  Lucky13  LogJam  Factoring
BREACH  DROWN  Mis-issuance  3HS
## Best Practices

### Encryption

<table>
<thead>
<tr>
<th>BEAST</th>
<th>FREAK</th>
<th>CRIME</th>
<th>POODLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sweet32</td>
<td>SLOTH</td>
<td>NOMORE</td>
<td>FLAME</td>
</tr>
<tr>
<td>SHAtered</td>
<td>Lucky13</td>
<td>LogJam</td>
<td>Factoring</td>
</tr>
<tr>
<td>BREACH</td>
<td>DROWN</td>
<td>Mis-issuance</td>
<td>3HS</td>
</tr>
</tbody>
</table>
## Best Practices

<table>
<thead>
<tr>
<th>Encryption</th>
<th>BEAST</th>
<th>FREAK</th>
<th>CRIME</th>
<th>POODLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic hashes</td>
<td>Sweet32</td>
<td>SLOTH</td>
<td>NOMORE</td>
<td>FLAME</td>
</tr>
<tr>
<td>SHAttered</td>
<td>Lucky13</td>
<td>LogJam</td>
<td>Factoring</td>
<td></td>
</tr>
<tr>
<td>BREACH</td>
<td>DROWN</td>
<td>Mis-issuance</td>
<td>3HS</td>
<td></td>
</tr>
</tbody>
</table>
Best Practices

Encryption

BEAST  FREAK  CRIME  POODLE

Cryptographic hashes

Sweet32  SLOTH  NOMORE  FLAME

Public keys

SHAttered  Lucky13  LogJam  Factoring

BREACH  DROWN  Mis-issuance  3HS

Encryption

Cryptographic hashes

Public keys
## Best Practices

<table>
<thead>
<tr>
<th>Encryption</th>
<th>BEAST</th>
<th>FREAK</th>
<th>CRIME</th>
<th>POODLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic hashes</td>
<td>Sweet32</td>
<td>SLOTH</td>
<td>NOMORE</td>
<td>FLAME</td>
</tr>
<tr>
<td>Public keys</td>
<td>SHAttered</td>
<td>Lucky13</td>
<td>LogJam</td>
<td>Factoring</td>
</tr>
<tr>
<td>Protocols</td>
<td>BREACH</td>
<td>DROWN</td>
<td>Mis-issuance</td>
<td>3HS</td>
</tr>
</tbody>
</table>
## Best Practices

<table>
<thead>
<tr>
<th>Encryption</th>
<th>BEAST</th>
<th>FREAK</th>
<th>CRIME</th>
<th>POODLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cryptographic hashes</td>
<td>Sweet32</td>
<td>SLOTH</td>
<td>NOMORE</td>
<td>FLAME</td>
</tr>
<tr>
<td>Public keys</td>
<td>SHAttered</td>
<td>Lucky13</td>
<td>LogJam</td>
<td>Factoring</td>
</tr>
<tr>
<td>Protocols</td>
<td>BREACH</td>
<td>DROWN</td>
<td>Mis-issuance</td>
<td>3HS</td>
</tr>
</tbody>
</table>
Best Practices

Encryption: BEAST, FREAK, CRIME, POODLE

Cryptographic hashes: Sweet32, SLOTH, NOMORE, FLAME

Public keys: SHAttered, Lucky13, LogJam, Factoring

Protocols: BREACH, DROWN, Mis-issuance, 3HS

Revocation
Encryption
Encryption

RC4
3DES-CBC
AES-CBC
Encryption

RC4
3DES-CBC
AES-CBC

Future removal: RC4 and 3DES
Encryption

- RC4
- 3DES-CBC
- AES-CBC

- AES-GCM
- ChaCha20/Poly1305

Future removal: RC4 and 3DES
Cryptographic Hashes
Cryptographic Hashes

MD5
SHA-1
Cryptographic Hashes

MD5
SHA-1

New removal: SHA-1 signed certificates for TLS
Cryptographic Hashes

- MD5
- SHA-1

- SHA-2 Family

New removal: SHA-1 signed certificates for TLS
Public Keys
Public Keys

<1024-bit RSA
Public Keys

<2048-bit RSA
Public Keys

<2048-bit RSA

New removal: <2048-bit RSA for TLS
Public Keys

- <2048-bit RSA (red x)
- ≥ 2048-bit RSA (green check)

Elliptic Curves

New removal: <2048-bit RSA for TLS
Protocols

http://
SSLv3
TLS 1.0
TLS 1.1
Protocols

- http://
- SSLv3
- TLS 1.0
- TLS 1.1

- https://
- TLS 1.2
Protocols

- http://
- SSLv3
- TLS 1.0
- TLS 1.1

- https://
- TLS 1.2

New addition: TLS 1.3 (draft)
Revocation

No checking
Revocation

No checking

OCSP Stapling
Revocation
Online Certificate Status Protocol
Revocation
Online Certificate Status Protocol

Certificate Authority

Server

Client
Revocation
Online Certificate Status Protocol

Certificate Authority

Server

Client
Revocation
Online Certificate Status Protocol
Revocation
Online Certificate Status Protocol
Revocation
Online Certificate Status Protocol
Revocation
Online Certificate Status Protocol

Additional network connection
Revocation
Online Certificate Status Protocol

Additional network connection

Compromises user privacy
Revocation
Online Certificate Status Protocol

Additional network connection

Compromises user privacy

Requires app opt-in
Revocation

OCSP Stapling

Certificate Authority

Server

Client
Revocation
OCSP Stapling

Certificate Authority

Server

Client
Revocation
OCSP Stapling
Revocation
OCSP Stapling

Certificate Authority

Server

Client
Revocation
OCSP Stapling
Revocation
OCSP Stapling

Slow adoption
Revocation
OCSP Stapling

Slow adoption

Does not protect against malicious servers
Revocation
Enhancement

Apple
Revocation
Enhancement

CT Log

Apple
Revocation
Enhancement

Certificate Authority

Certificate Authority

Certificate Authority

Apple

CT Log
Revocation
Enhancement

Certificate Authority

Certificate Authority

Certificate Authority

Apple

CT Log

Certificate Authority
Revocation Enhancement

Certificate Authority

Client

CT Log

Certificate Authority

Certificate Authority
Revocation
Improvements
Revocation

Improvements

Reduced privacy compromise
Revocation
Improvements

Reduced privacy compromise

Automatic updating
Revocation
Improvements

Reduced privacy compromise

Automatic updating

Faster connections
Evolving Standards
# Evolving Standards

<table>
<thead>
<tr>
<th>Encryption</th>
<th>RC4, CBC modes</th>
<th>AES-GCM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ChaCha20/Poly1305</td>
</tr>
</tbody>
</table>
## Evolving Standards

<table>
<thead>
<tr>
<th>Encryption</th>
<th>RC4, CBC modes</th>
<th>AES-GCM ChaCha20/Poly1305</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hashes</td>
<td>MD5, SHA-1</td>
<td>SHA-2 family</td>
</tr>
</tbody>
</table>

### Encryption
- RC4, CBC modes
- AES-GCM ChaCha20/Poly1305

### Hashes
- MD5, SHA-1
- SHA-2 family
## Evolving Standards

<table>
<thead>
<tr>
<th>Encryption</th>
<th>RC4, CBC modes</th>
<th>AES-GCM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ChaCha20/Poly1305</td>
</tr>
<tr>
<td>Hashes</td>
<td>MD5, SHA-1</td>
<td>SHA-2 family</td>
</tr>
<tr>
<td>Public Keys</td>
<td>&lt;2048-bit RSA</td>
<td>≥ 2048-bit RSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elliptic curves</td>
</tr>
</tbody>
</table>
# Evolving Standards

<table>
<thead>
<tr>
<th>Category</th>
<th>Old Standard</th>
<th>New Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>RC4, CBC modes</td>
<td>AES-GCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ChaCha20/Poly1305</td>
</tr>
<tr>
<td>Hashes</td>
<td>MD5, SHA-1</td>
<td>SHA-2 family</td>
</tr>
<tr>
<td>Public Keys</td>
<td>&lt;2048-bit RSA</td>
<td>≥ 2048-bit RSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elliptic curves</td>
</tr>
<tr>
<td>Protocols</td>
<td>http://, SSLv3, TLS 1.0, TLS 1.1</td>
<td>https://, TLS 1.2+</td>
</tr>
</tbody>
</table>
## Evolving Standards

<table>
<thead>
<tr>
<th></th>
<th>RC4, CBC modes</th>
<th>AES-GCM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ChaCha20/Poly1305</td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Hashes</strong></td>
<td>MD5, SHA-1</td>
<td>SHA-2 family</td>
</tr>
<tr>
<td><strong>Public Keys</strong></td>
<td>&lt;2048-bit RSA</td>
<td>≥ 2048-bit RSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elliptic curves</td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
<td>http://, SSLv3, TLS 1.0, TLS 1.1</td>
<td>https://, TLS 1.2+</td>
</tr>
<tr>
<td><strong>Revocation</strong></td>
<td>No checking</td>
<td>Certificate Transparency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OCSP Stapling</td>
</tr>
</tbody>
</table>
TLS Trust Removals
Trust Removals
Trust Removals

SHA-1 signed certificates for TLS
Trust Removals

SHA-1 signed certificates for TLS

Certificates using <2048-bit RSA for TLS
Trust Removals
Trust Removals

Does not affect
Trust Removals

Does not affect

• Root certificates
Trust Removals

Does not affect

• Root certificates
• Enterprise-distributed certificates
Trust Removals

Does not affect
• Root certificates
• Enterprise-distributed certificates
• User-installed certificates
Trust Removals

Does not affect
- Root certificates
- Enterprise-distributed certificates
- User-installed certificates
- Client certificates
This Connection Is Not Private

This website may be impersonating "sha1-intermediate.badssl.com" to steal your personal or financial information. You should go back to the previous page.

Safari warns you when a website has a certificate that is not valid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.
Trust Removals

Safari warns you when a website has a certificate that is not valid. This may happen if the website is misconfigured or an attacker has compromised your connection.

To learn more, you can view the certificate. If you understand the risks involved, you can visit this website.
Trust Removals
Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession
Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession

Servers to upgrade to new certificates
Trust Removals

InvalidCertChain (-9807) SSL errors with URLSession

Servers to upgrade to new certificates

• https://support.apple.com/kb/HT204132
What to Do Now?
What to Do Now?

Check your implementations, libraries, and servers
What to Do Now?

Check your implementations, libraries, and servers

Server Developers
What to Do Now?

Check your implementations, libraries, and servers

Server Developers

• Replace any SHA-1 certificates or weak RSA keys
What to Do Now?

Check your implementations, libraries, and servers

Server Developers
• Replace any SHA-1 certificates or weak RSA keys
• Upgrade servers to TLS 1.2 and authenticated encryption ciphers
What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
What to Do Now?

Check your implementations, libraries, and servers

Server Developers

- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs
What to Do Now?

Check your implementations, libraries, and servers

Server Developers
- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs

App Developers
What to Do Now?

Check your implementations, libraries, and servers

Server Developers
- Replace any SHA-1 certificates or weak RSA keys
- Upgrade servers to TLS 1.2 and authenticated encryption ciphers
- Use OCSP Stapling
- Check that your certificates are in CT logs

App Developers
- Avoid ATS exceptions
App Transport Security Update

Chris Wood, Secure Transports Engineer
App Transport Security
Current standards
App Transport Security

Current standards

From HTTP to HTTPS

• TLS 1.2
• Strong cryptography—AES and SHA-2
• Forward Secrecy—ECDHE
App Transport Security
Current standards

From HTTP to HTTPS
• TLS 1.2
• Strong cryptography—AES and SHA-2
• Forward Secrecy—ECDHE

Exceptions—per-domain, narrow
Exception Updates
Exception Updates

Expansion beyond WebKit
• AVFoundation loads
• WebView requests
• Local network connections
Exception Updates

Expansion beyond WebKit
• AVFoundation loads
• WebView requests
• Local network connections

Certificate Transparency requirement
ATS-Compliant Services
Practice what you preach

APNs
FaceTime
Game Center
Apple Services
iCloud Services (Mail, CloudKit)
iWork
Spotlight
iAd
iTunes
Software Update
ATS on the Rise
ATS on the Rise

ATS adoption is increasing
ATS on the Rise

ATS adoption is increasing

Still more work to be done
ATS on the Rise

ATS adoption is increasing
Still more work to be done
Minimize or reduce exceptions
Transport Layer Security
SSL and TLS Lineage

A long road
SSL and TLS Lineage

A long road

TLS 1.0

1999
SSL and TLS Lineage
A long road

- TLS 1.0
  - 1999

- TLS 1.1
  - 2006
SSL and TLS Lineage

A long road

- TLS 1.0: 1999
- TLS 1.1: 2006
- TLS 1.2: 2008
SSL and TLS Lineage

A long road

- TLS 1.0: 1999
- TLS 1.1: 2006
- TLS 1.2: 2008
- TLS 1.3 (draft): 2017
TLS 1.3
Best practice by design
TLS 1.3
Best practice by design

Strong cryptography and Forward Secrecy by default
• Legacy options, ciphers, and key exchange algorithms removed
TLS 1.3
Best practice by design

Strong cryptography and Forward Secrecy by default
• Legacy options, ciphers, and key exchange algorithms removed

Overall simpler specification
TLS 1.3
Best practice by design

Strong cryptography and Forward Secrecy by default
• Legacy options, ciphers, and key exchange algorithms removed

Overall simpler specification

Improved network efficiency
TLS 1.3 Overview

Improved efficiency
TLS 1.3 Overview
Improved efficiency

TLS 1.2
- Client
- Server
- SYN
- SYN+ACK
- ACK

TLS 1.3
- Client
- Server
- SYN
- SYN+ACK
- ACK
TLS 1.3 Overview

Improved efficiency

TLS 1.2

Client
SYN
SYN+ACK
ACK
CH
SH

Server

Time

TLS 1.3

Client
SYN
SYN+ACK
ACK
CH, KEX
SH, KEX

Server

CH - Client Hello
SH - Server Hello
KEX - Key Share
TLS 1.3 Overview
Improved efficiency

TLS 1.2
Client
SYN
SYN+ACK
ACK
CH
SH
KEX
KEX
Server

TLS 1.3
Client
SYN
SYN+ACK
ACK
CH, KEX
SH, KEX
DATA
Server

CH - Client Hello
SH - Server Hello
KEX - Key Share
TLS 1.3 Overview

Improved efficiency

TLS 1.2

Client
- SYN
- SYN+ACK
- ACK
- CH
- SH
- KEX
- KEX
- DATA

Server

TLS 1.3

Client
- SYN
- SYN+ACK
- ACK
- CH, KEX
- SH, KEX
- DATA

Server

Time

CH - Client Hello
SH - Server Hello
KEX - Key Share
How to Enable TLS 1.3 Beta?
How to Enable TLS 1.3 Beta?

It is not on by default
How to Enable TLS 1.3 Beta?

It is **not on by default**

You can install a profile on iOS
How to Enable TLS 1.3 Beta?

It is not on by default

You can install a profile on iOS

You can enable system-wide TLS 1.3 on macOS

```bash
defaults write /Library/Preferences/com.apple.networkd tcp_connect_enable_tls13 1
```
TLS 1.3 Outlook
TLS 1.3 Outlook

IETF standardization (2017-2018)
TLS 1.3 Outlook

IETF standardization (2017-2018)

Third-party collaboration
TLS 1.3 Outlook

- IETF standardization (2017-2018)
- Third-party collaboration
- Enterprise preparation
Takeaways

Implement best practices
Takeaways

Implement best practices

Avoid new and future algorithm removals
Takeaways

- Implement best practices
- Avoid new and future algorithm removals
- Continue upgrading to modern TLS configurations
Takeaways

Implement best practices

Avoid new and future algorithm removals

Continue upgrading to modern TLS configurations
  • Minimize or remove App Transport Security exceptions
Takeaways

Implement best practices

Avoid new and future algorithm removals

Continue upgrading to modern TLS configurations
  • Minimize or remove App Transport Security exceptions
  • Try out TLS 1.3
More Information

https://developer.apple.com/wwdc17/701
<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy and Your Apps</td>
<td>Executive Ballroom</td>
<td>Tuesday 11:20PM</td>
</tr>
<tr>
<td>Advances in Networking, Part 1</td>
<td>Executive Ballroom</td>
<td>Wednesday 3:10PM</td>
</tr>
<tr>
<td>Advances in Networking, Part 2</td>
<td>Executive Ballroom</td>
<td>Wednesday 4:10PM</td>
</tr>
<tr>
<td>Labs</td>
<td>Technology Lab</td>
<td>Time</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------</td>
<td>------------</td>
</tr>
<tr>
<td>Security &amp; Privacy</td>
<td>Lab D</td>
<td>Tue 1:50PM-3:50PM</td>
</tr>
<tr>
<td>Security &amp; Privacy</td>
<td>Lab J</td>
<td>Wed 1:00PM-3:30PM</td>
</tr>
<tr>
<td>Networking Lab</td>
<td>Lab D</td>
<td>Thu 9:00AM-11:00AM</td>
</tr>
<tr>
<td>Networking Lab</td>
<td>Lab J</td>
<td>Fri 1:50PM-3:50PM</td>
</tr>
</tbody>
</table>