

App Transport Security: what, why, How?

About Me

- Chris Dzombak
- iOS @ NY Times
- @cdzombak on Twitter

Don't take notes.

App Transport Security

→ WWDC 2015

→ iOS 9

→ OS X 10.11

App Transport Security

...is just a few rules about network connections.

App Transport Security

...is just a few rules about network connections.

...for apps built against the iOS 9 or OS X 10.11 SDKs.

The rules

No HTTP

TLS 1.2

**Good TLS cipher suite,
that provides forward
secrecy**

**SSL certificate issued by
a trusted certificate
authority**

Safe lengths for encryption keys

- RSA keys: 2048 bits or longer
- ECC keys: 256 bits or longer

**Server certificate uses
SHA-256 or better**

ATS Rules

- HTTPS
- TLS 1.2
- TLS cipher suite with forward secrecy
- Trusted certificate authority
- Safe encryption key size
- Certificate using SHA-256 or better

HTTPS Best Practices

Certificate pinning?

Almost nobody uses certificate pinning 😢



Frederic Jacobs

@FredericJacobs



Following

It's 2016 & apps like YouTube, Peach, Instagram or Slack don't do certificate pinning. Rogue CAs anyone?

ATS is implemented somewhere in Core Foundation territory

App Transport Security rules apply to NSURLSession,
NSURLConnection, libcurl, ...

ATS: On the server

ATS: On the server

- Use Mozilla's server-side TLS guide and configuration generator
- Get a free certificate from Let's Encrypt
- Or an inexpensive one from Namecheap
 - Test with SSLabs SSL Tester

Adopting ATS

**Build against the iOS 9/
OS X 10.11 SDK**

ATS Exceptions

- Configure exceptions per-domain
- NSAppTransportSecurity key in Info.plist

```
NSAppTransportSecurity : Dictionary {  
    NSEExceptionDomains : Dictionary {  
        <domain-name-string> : Dictionary {  
            NSIncludesSubdomains : Boolean  
            NSEExceptionAllowsInsecureHTTPLoads : Boolean  
            NSEExceptionRequiresForwardSecrecy : Boolean  
            NSEExceptionMinimumTLSVersion : String  
        }  
    }  
    NSAllowsArbitraryLoads : Boolean  
}
```

NSEExceptionDomains

- Optional.
- Dictionary. Keys are domain names; values are dictionaries.

NSIncludesSubdomains

- Optional; defaults to NO.
- Whether this domain's exceptions apply to its subdomains, too.

NSEExceptionMinimumTLSVersion

- Optional; defaults to TLSv1.2.
- The minimum TLS version that will be accepted for connections to this domain.
- Valid values: TLSv1.0, TLSv1.1, TLSv1.2

NSExceptionRequiresForwardSecrecy

- Optional; defaults to YES.
- Setting to NO allows for using TLS cipher suites that don't provide forward secrecy for connections to this domain.

NSEExceptionAllowsInsecureHTTPLoads

- Optional; defaults to NO.
- If YES, your app can connect insecurely to this domain with no certificate, or a self-signed, expired, or hostname-mismatched certificate.

Third-party exceptions

- NSThirdPartyExceptionAllowsInsecureHTTPLoads
- NSThirdPartyExceptionRequiresForwardSecrecy
- NSThirdPartyExceptionMinimumTLSVersion

```
NSAppTransportSecurity : Dictionary {  
    NSEExceptionDomains : Dictionary {  
        <domain-name-string> : Dictionary {  
            NSIncludesSubdomains : Boolean  
            NSEExceptionAllowsInsecureHTTPLoads : Boolean  
            NSEExceptionRequiresForwardSecrecy : Boolean  
            NSEExceptionMinimumTLSVersion : String  
        }  
    }  
}  
  
// let's talk about this...  
NSAllowsArbitraryLoads : Boolean  
}
```

NSAllowsArbitraryLoads

- Optional; defaults to NO.
- When YES, disables ATS for all domains, except those you configure via exceptions.

Exceptions can opt domains out of ATS...

...

...or, if ATS is disabled via
NSAllowsArbitraryLoads, exceptions can opt
domains back *into* ATS.

Domain only accessible via HTTP

```
NSAppTransportSecurity
NSEExceptionDomains
"media-server.example.com"
NSEExceptionAllowsInsecureHTTPLoads = YES
```

Domain running an old TLS configuration

```
NSAppTransportSecurity
NSEceptionDomains
"less-secure.example.com"
NSEceptionRequiresForwardSecrecy = NO
NSEceptionMinimumTLSVersion = "TLSv1.0"
```

Connecting to user-provided URLs, but using ATS for your own domain

```
NSAppTransportSecurity
    NSAllowsArbitraryLoads = YES
NSExceptionDomains
    "api.example.com"
        NSExceptionAllowsInsecureHTTPLoads = NO
        NSExceptionRequiresForwardSecrecy = YES
        NSExceptionMinimumTLSVersion = "TLSv1.2"
```

SFSafariViewController ==
no ATS configuration
needed

NSA-friendly mode

NSAppTransportSecurity
NSAllowsArbitraryLoads = YES

**Best practice: make the
narrowest exceptions you
can**

Connecting to IP addresses over standard HTTP

```
NSAppTransportSecurity
    NSAllowsArbitraryLoads = YES
NSExceptionDomains
    "api.example.com"
        NSExceptionAllowsInsecureHTTPLoads = NO
        NSExceptionRequiresForwardSecrecy = YES
        NSExceptionMinimumTLSVersion = "TLSv1.2"
```

Connecting to domains with SHA-1 certificates or small key sizes

```
NSAppTransportSecurity
NSEExceptionDomains
    "i-need-a-new-certificate.example.com"
NSEExceptionAllowsInsecureHTTPLoads = YES
```

Debugging

-98xx

**Disable ATS
(temporarily)**

Disable ATS (temporarily)...

...

**...then narrow down the issue with
exception domains**

CFNETWORK_DIAGNOSTICS=1

CFNetwork Diagnostic Logging (Technical Q&A 1887)

https://developer.apple.com/library/ios/qa/qa1887/_index.html

nscurl --ats-diagnostics

```
nscurl --ats-diagnostics  
--verbose https://  
www.dzombak.com
```

```
nscurl --ats-diagnostics
```

- Can I connect to this server with ATS?
 - Why not?
- What exceptions do I need to configure?

Working with Charles Proxy: (temporarily) disable ATS

Additional ATS reference/debugging resources

**Remember, these slides will be posted online
shortly.**

[https://gist.github.com/cdzombak/
3d2ff091b9038fde27bb](https://gist.github.com/cdzombak/3d2ff091b9038fde27bb)

Who's actually using ATS?

September 2015

- 1Password (6.0): **✗** opts out
- Dropbox (4.0): **✗** opts out
- Facebook (39.1): **✗** opts out
- Google Maps (4.10.1): **✗** opts out
- ...

September 2015

→ ...

→ Instagram (7.6.0): ?

→ Microsoft OneNote (2.16.1): ✗ opts out

→ Tumblr (4.5):  uses ATS properly

Jan. 2016: 1Password (6.2)

▼ App Transport Security Settings		Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES	
▼ Exception Domains	Dictionary	(7 items)	
▼ agilebits.com	Dictionary	(2 items)	
NSExceptionAllowsInsecureHTTPLoads	Boolean	NO	
NSIncludesSubdomains	Boolean	YES	
▼ 1password.com	Dictionary	(2 items)	
NSExceptionAllowsInsecureHTTPLoads	Boolean	NO	
NSIncludesSubdomains	Boolean	YES	
▼ dropbox.com	Dictionary	(2 items)	
NSExceptionAllowsInsecureHTTPLoads	Boolean	NO	
NSIncludesSubdomains	Boolean	YES	
▼ app-updates.agilebits.com	Dictionary	(1 item)	
NSExceptionRequiresForwardSecrecy	Boolean	NO	
▼ email.onedrive.com	Dictionary	(1 item)	
NSAllowsArbitraryLoads	Boolean	YES	
▼ s3.amazonaws.com	Dictionary	(1 item)	
NSExceptionRequiresForwardSecrecy	Boolean	NO	
▼ onedrive.com	Dictionary	(2 items)	
NSExceptionAllowsInsecureHTTPLoads	Boolean	NO	
NSIncludesSubdomains	Boolean	YES	

January 2016

- Dropbox (4.2.2): ✗ opts out
- Facebook (46.0): ✗ opts out
- Facebook Messenger (53.0): ✗ opts out
 - Flickr (4.0.7): ✓
 - Gmail (4.3): ✗ old SDK

Jan. 2016: Evernote (7.9.2) X

▼ App Transport Security Settings	Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES
▼ Exception Domains	Dictionary	(5 items)
▼ evernote.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ akamaihd.net	Dictionary	(2 items)
NSIncludesSubdomains	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
▼ fbcdn.net	Dictionary	(2 items)
NSIncludesSubdomains	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
▼ facebook.com	Dictionary	(2 items)
NSIncludesSubdomains	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
▼ yinxiang.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES

Jan. 2016: ForeFlight (7.5.1)

▼ App Transport Security Settings	▲ Dictionary	(2 items)
Allow Arbitrary Loads	▲ Boolean	YES
▼ Exception Domains	▲ Dictionary	(5 items)
▼ api.simperium.com	Dictionary	(1 item)
NSExceptionAllowInsecureHTTPLoads	Boolean	NO
▼ splex.foreflight.com	Dictionary	(1 item)
NSExceptionAllowInsecureHTTPLoads	Boolean	NO
▼ charts.foreflight.com	Dictionary	(1 item)
NSExceptionAllowInsecureHTTPLoads	Boolean	NO
▼ api.foreflight.com	Dictionary	(1 item)
NSExceptionAllowInsecureHTTPLoads	Boolean	NO
▼ cloudfront.foreflight.com	Dictionary	(1 item)
NSExceptionAllowInsecureHTTPLoads	Boolean	NO

January 2016

- Google (11.1.0): ✗ opts out
- Google Maps (4.14.0): ✗ opts out
- Microsoft OneNote (2.18.1): ✗ opts out
 - Pages (2.6.1): ✓
 - Peach (1.0.9): ✗ opts out

Jan. 2016: Instagram (7.13.1) ?

App Transport Security Settings	Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES
Exception Domains	Dictionary	(6 items)
akamaihd.net	Dictionary	(3 items)
NSIncludesSubdomains	Boolean	YES
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
instagram.com	Dictionary	(5 items)
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSExceptionRequiresForwardSecrecy	Boolean	YES
NSRequiresCertificateTransparency	Boolean	NO
NSIncludesSubdomains	Boolean	YES
NSExceptionMinimumTLSVersion	String	TLSV1.2
cdninstagram.com	Dictionary	(5 items)
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSExceptionRequiresForwardSecrecy	Boolean	YES
NSRequiresCertificateTransparency	Boolean	NO
NSIncludesSubdomains	Boolean	YES
NSExceptionMinimumTLSVersion	String	TLSV1.2
fbcdn.net	Dictionary	(3 items)
NSIncludesSubdomains	Boolean	YES
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
facebook.com	Dictionary	(3 items)
NSIncludesSubdomains	Boolean	YES
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSThirdPartyExceptionRequiresForwardSecrecy	Boolean	NO
help.instagram.com	Dictionary	(5 items)
NSExceptionAllowsInsecureHTTPLoads	Boolean	YES
NSExceptionRequiresForwardSecrecy	Boolean	NO
NSRequiresCertificateTransparency	Boolean	NO
NSIncludesSubdomains	Boolean	YES
NSExceptionMinimumTLSVersion	String	TLSV1.2

Jan. 2016: Pinterest (5.7.2) ?

▼ App Transport Security Settings	▲ Dictionary	(2 items)
Allow Arbitrary Loads	▲ Boolean	YES
▼ Exception Domains	▲ Dictionary	(5 items)
▼ akamaihd.net	Dictionary	(2 items)
NSEExceptionRequiresForwardSecrecy	Boolean	NO
NSIncludesSubdomains	Boolean	YES
▼ api.twitter.com	Dictionary	(1 item)
NSEExceptionRequiresForwardSecrecy	Boolean	NO
▼ api.braintreegateway.com	Dictionary	(2 items)
NSEExceptionRequiresForwardSecrecy	Boolean	NO
NSEExceptionsAllowsInsecureHTTPLoads	Boolean	NO
▼ fcdn.net	Dictionary	(2 items)
NSEExceptionRequiresForwardSecrecy	Boolean	NO
NSIncludesSubdomains	Boolean	YES
▼ graph.facebook.com	Dictionary	(1 item)
NSEExceptionRequiresForwardSecrecy	Boolean	NO

Jan. 2016: Tumblr (5.1): X

▼ App Transport Security Settings	Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES
▼ Exception Domains	Dictionary	(0 items)

Yahoo Weather (1.9.0) X

▼ App Transport Security Settings	Dictionary	(2 items)
Allow Arbitrary Loads	Boolean	YES
▼ Exception Domains	Dictionary	(13 items)
▼ flurry.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yahoo.net	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ zenfs.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yahoofs.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ www.tumblr.com	Dictionary	(0 items)
▼ flickr.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yahoo.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yhoo.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yimg.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ ahoo.it	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ api.tumblr.com	Dictionary	(0 items)
▼ staticflickr.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES
▼ yahoo-inc.com	Dictionary	(1 item)
NSIncludesSubdomains	Boolean	YES

January 2016

- Slack (2.66): ❌ opts out
- Snapchat (9.21.1): 
- YouTube (10.50.18): ❌ opts out

**5 of those 20 apps use
ATS reasonably well.**

**It's hard?
(debugging is hard?)**

Ad networks



The official blog for information about the AdWords, AdSense, DoubleClick and AdMob APIs and SDKs.

Handling App Transport Security in iOS 9

Posted: Wednesday, August 26, 2015

“To ensure ads continue to serve on iOS9 devices for developers transitioning to HTTPS, the recommended short term fix is to add an exception that allows HTTP requests to succeed and non-secure content to load successfully.

Publishers can add an exception to their Info.plist to allow any insecure connection.”

```
<key>NSEExceptionDomains</key>
<dict>
    <key>facebook.com</key>
    <dict>
        <key>NSIncludesSubdomains</key>
        <true/>
        <key>NSThirdPartyExceptionRequiresForwardSecrecy</key>
        <false/>
    </dict>
    <key>fbcdn.net</key>
    <dict>
        <key>NSIncludesSubdomains</key>
        <true/>
        <key>NSThirdPartyExceptionRequiresForwardSecrecy</key>
        <false/>
    </dict>
    <key>akamaihd.net</key>
    <dict>
        <key>NSIncludesSubdomains</key>
        <true/>
        <key>NSThirdPartyExceptionRequiresForwardSecrecy</key>
        <false/>
    </dict>
</dict>
```

Lack of awareness/unwillingness to learn?

samfriend commented on Jun 9, 2015

Adding the following to your Info.plist will disable ATS

```
<key>NSAppTransportSecurity</key>
```

```
<dict>
```

```
<key>NSAllowsArbitraryLoads</key><true/>
```

```
</dict>
```

Lack of caring?



**Lack of clear
documentation from
Apple?**

What's next?





Available on the
App Store

Start now.

Conclusions (1/2)

- ATS enforces current security best practices
 - Don't disable it
 - Configure your servers to support the TLS configuration ATS requires
- Configure the most narrow exceptions possible to allow your app to talk to domains your company doesn't control

Conclusions (2/2)

- Three-quarters of popular apps aren't using ATS properly 
- You can be one of the few to follow best practices!
- ...and Apple will probably start enforcing this at some point.

Questions/Discussion

TODO

- review flow to ensure talk makes sense and I have the right balance of info on slides
- check for aportrophes, quotes, etc in notes and slides