

Mobile Application Programming

Mobile Security

Areas of Concern



Device-Server



Device Local



Device-Device



Physical

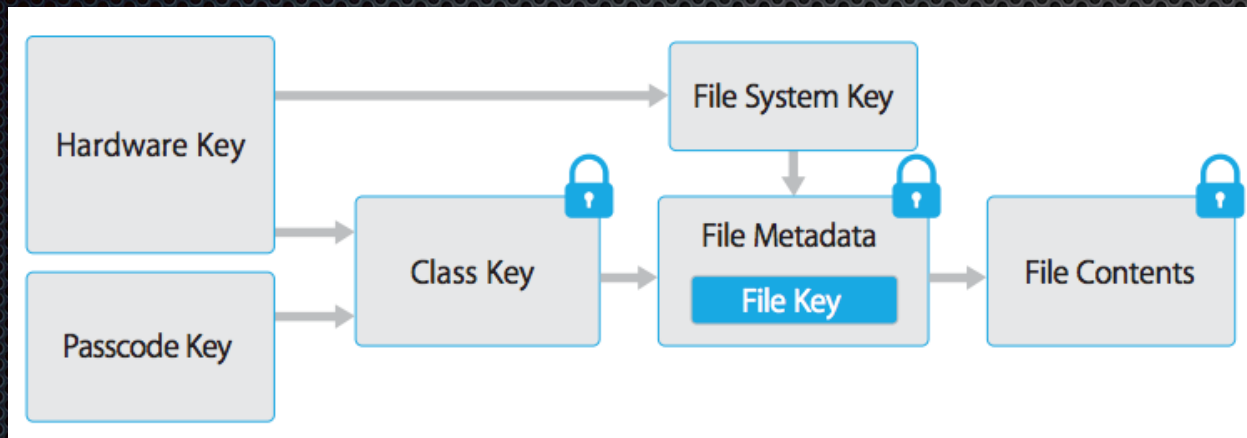


Physical

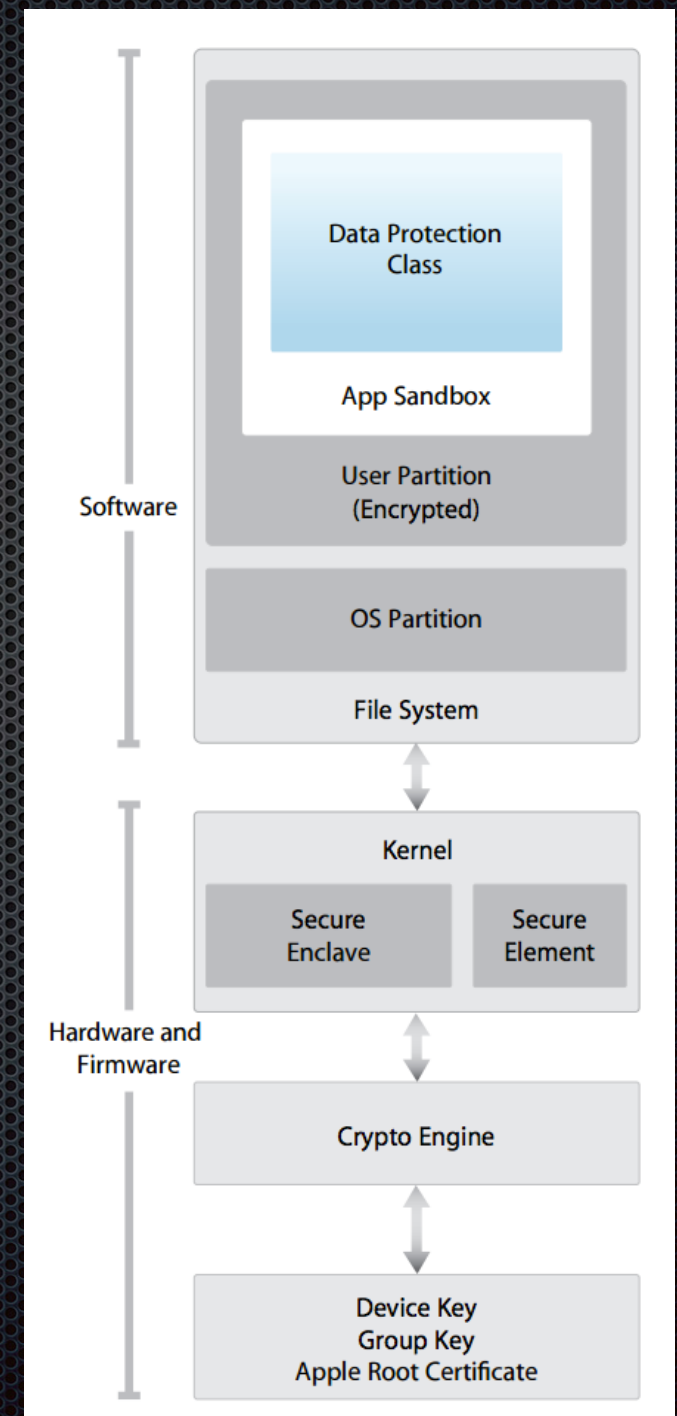


TouchID

Encryption



Availability	File Data Protection	Keychain Data Protection
When unlocked	NSFileProtectionComplete	kSecAttrAccessibleWhenUnlocked
While locked	NSFileProtectionCompleteUnlessOpen	N/A
After first unlock	NSFileProtectionCompleteUntilFirstUserAuthentication	kSecAttrAccessibleAfterFirstUnlock
Always	NSFileProtectionNone	kSecAttrAccessibleAlways
Passcode enabled	N/A	kSecAttrAccessible-WhenPasscodeSetThisDeviceOnly



In the News



50% DoJ
45% Apple

<http://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone>

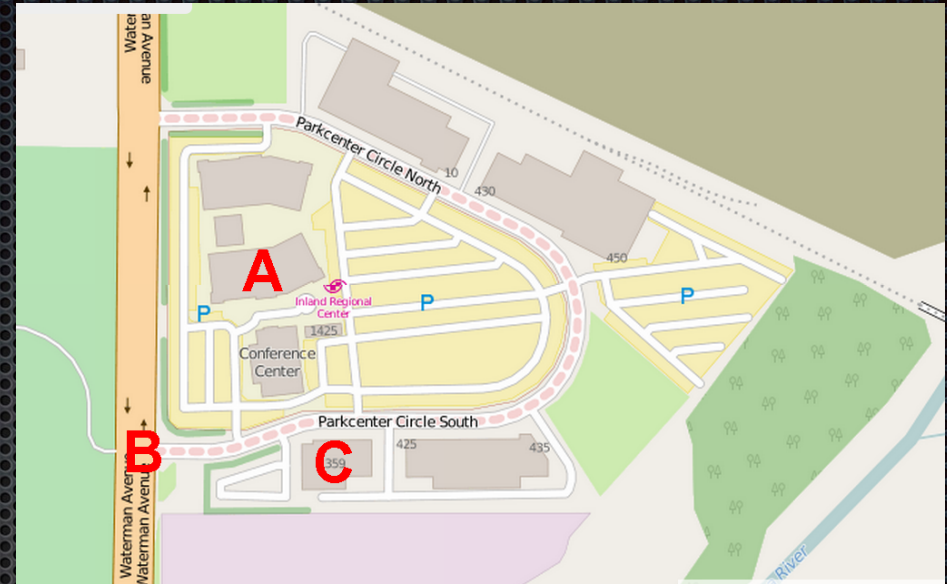
From the beginning, we objected to the FBI's demand that Apple build a backdoor into the iPhone because we believed it was wrong and would set a dangerous precedent. As a result of the government's dismissal, neither of these occurred. This case should never have been brought.

We will continue to help law enforcement with their investigations, as we have done all along, and we will continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated.

Apple believes deeply that people in the United States and around the world deserve data protection, security and privacy. Sacrificing one for the other only puts people and countries at greater risk.

This case raised issues which deserve a national conversation about our civil liberties, and our collective security and privacy. Apple remains committed to participating in that discussion.

<http://techcrunch.com/2016/03/28/justice-department-drops-lawsuit-against-apple-over-iphone-unlocking-case/>



Inland Regional Center

Department of Public Safety

14 killed, 22 injured

https://en.wikipedia.org/wiki/2015_San_Bernardino_attack

February 16, 2016

A Message to Our Customers

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.

<http://www.apple.com/customer-letter/>

Data Files

```

1  <?xml version="1.0" encoding="utf-16"?>
2  <Realm xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
3    <Name>basics</Name>
4    <Description>satellite launching 101</Description>
5    <LevelFileNames>
6      <string>R01_LVL01_Intro</string>
7      <string>R01_LVL02_Spincontrol</string>
8      <string>R01_LVL03_Stars</string>
9      <string>R01_LVL04_Gravity</string>
10     <string>R01_LVL05_Timing</string>
11     <string>R01_LVL06_PinchZoom</string>
12     <string>R01_LVL07_Thruster</string>
13     <string>R01_LVL08_Speed</string>
14     <string>R01_LVL09_SkillTest1</string>
15     <string>R01_LVL10_SkillTest2</string>
16     <string>R01_LVL11_SkillTest3</string>
17   </LevelFileNames>
18 </Realm>
19

```

Key	Value
▼ Information Property List	(13 items)
CFBundleDevelopmentRegion	English
CFBundleDisplayName	\$(PRODUCT_NAME)
CFBundleExecutable	\$(EXECUTABLE_NAME)
CFBundleIconFile	Icon.png
CFBundleIdentifier	com.pixiotech.MobileFinder
CFBundleInfoDictionaryVersion	6.0
CFBundleName	\$(PRODUCT_NAME)
CFBundlePackageType	APPL
CFBundleSignature	????
CFBundleVersion	1.6.0
UIFileSharingEnabled	<input checked="" type="checkbox"/>
▼ UISupportedInterfaceOrientations	(4 items)
Item 0	UIInterfaceOrientationPortrait
Item 1	UIInterfaceOrientationPortraitUpsideDown
Item 2	UIInterfaceOrientationLandscapeLeft
Item 3	UIInterfaceOrientationLandscapeRight
▼ CFBundleURLTypes	(1 item)
Item 0	(2 items)



IMG_0274.PNG - Data		
Len: \$00011939	Type/Creator: /	Set: \$00000000:00000000 / \$00000000
00000000:	89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52	.PNG.....IHDR
00000010:	00 00 01 40 00 00 01 E0 08 06 00 00 00 D4 8C B4	...@.....
00000020:	44 00 00 20 00 49 44 41 54 78 01 EC 7D 05 7C 1D	D... .IDATx...}
00000030:	55 FA F6 93 E4 C6 DD DD 9A B4 A9 2B 35 DA 42 A1	U.....+5.B.
00000040:	B4 40 A1 B8 B3 88 2C 0B 7F 58 64 B1 0F 5F 16 59	.@.....Xd....Y
00000050:	6C F1 C5 DD A1 C5 48 A1 D4 A8 50 4A DD 3D A9 C5	l.....K...PJ.=..
00000060:	DD 5D EF F7 3E E7 66 6E 26 C9 8D B5 97 36 29 F3	.)...>.fn&....6).
00000070:	E6 77 33 76 F4 9D 99 E7 BC 36 E7 38 FC E3 96 58	.w3v.....6.8...[
00000080:	CD 37 DD 72 1B 22 A3 A3 E1 E0 E0 00 83 0C 0E 18	.7.r.".....l~..
00000090:	1C 30 38 70 BC 73 20 23 2D 0D 6F BC FA 3F 38 EC	.08p.s #-..o..?8.
000000A0:	DC BB DF 1C 16 15 01 B3 D9 6C 00 E0 F1 7E 07 8Dl.....~..
000000B0:	FE 19 1C 30 38 60 E5 40 4E 46 16 1C F2 CB AB CC	...08`.@NF.....
000000C0:	3C 63 00 A0 95 2F C6 8E C1 01 83 03 7F 10 07 E6	<c.../.....
000000D0:	CF FD 1E 33 66 9E 05 93 B3 F3 1F 54 43 CF 8A 35	...3f.....TC..5
000000E0:	35 35 36 A9 1C 06 00 F6 8C 71 46 EA 3F 9E 03 25	556.....qF.?..%
000000F0:	25 25 30 37 59 9E 4F D6 E6 E2 EA 0A 4F 4F CF 56	%%07Y..0.....00.V
00000100:	15 57 56 56 A2 AE B6 56 9D F3 F0 F0 80 AB 9B 98	.WVV...V.....
00000110:	F5 7A 49 71 B1 1A D8 79 C2 D7 CF 0F 8E 8E 8E D6	.z1q...y.....
00000120:	68 C6 CE B1 E1 C0 DE DD 3B 51 90 97 88 F3 2F B9	k.....;Q...../.
00000130:	1C 9E 5E 5E C7 A6 11 BA 5A 4D 4D 4D 8D EA D0 5E	..^^.....ZMMM...^
00000140:	00 18 73 FD 5E A0 51 84 4A 79 70 D3 3E 1C AC AB	..s.^..Q..Jyp>...
00000150:	AA 6F EC EE 4C 2F C2 8A 6D 05 D8 B3 BF 06 59 F9	.o..L/.m.....Y.
00000160:	0E 48 CF B3 B4 3B 3A 04 88 94 5F 52 3F 57 9C 3C	.H.....R?W.<
00000170:	3C 08 43 A2 03 50 DF D8 08 67 27 A7 BE D1 B1 C3	<.C..P...g'.....
00000180:	6C E5 07 EF BE 83 17 9E 7D 06 AF BE F5 0E 4E 9E	l.....}.....N.
00000190:	7A 4A 87 A5 D4 D7 D5 E1 F1 47 1E C6 8A 65 CB 50	zJ.....G...e.P
000001A0:	56 5A 8A 11 A3 46 E1 FE 7F 3D 8C 84 81 83 54 F4	VZ....F...=...T.
000001B0:	03 FB F7 E1 D1 7F 3D 84 6D 5B B6 C0 43 40 EC 94=m[...C@.
000001C0:	33 67 E2 AE 7B EF 68 07 68 FA 0A 4E 99 34 1E 59	3g...{.k.h..N.4.V
000001D0:	99 99 D6 53 04 B0 71 13 26 E2 AC 59 E7 E0 DA BF	...S..q.&..Y....
000001E0:	5F 0F 27 E1 F0 3D 77 DC 86 AF BF 9C A3 D2 DC 70	...'..=w.....p
000001F0:	D3 3F F0 E8 13 4F A9 7D B6 61 50 42 9C 3C 86 16	.?..0..}..aPB.<..
00000200:	00 DD B4 63 37 C2 23 22 AC 65 19 3B C7 86 03 8E	...c7.#".e;....
00000210:	E2 67 C8 CA CC C0 C7 EF BE 85 73 2E BA 58 EE 49	.g.....s..X.l
00000220:	64 A7 0D 79 F4 B1 97 B0 7D 87 60 CA 11 D2 B0 A1	d..y.....\.....
00000230:	49 F8 F7 C3 B7 B7 2B C5 D4 28 2F 31 C9 5E 00 18	l.....+..</l.^..

Raw Binary / Text Data

FILE*

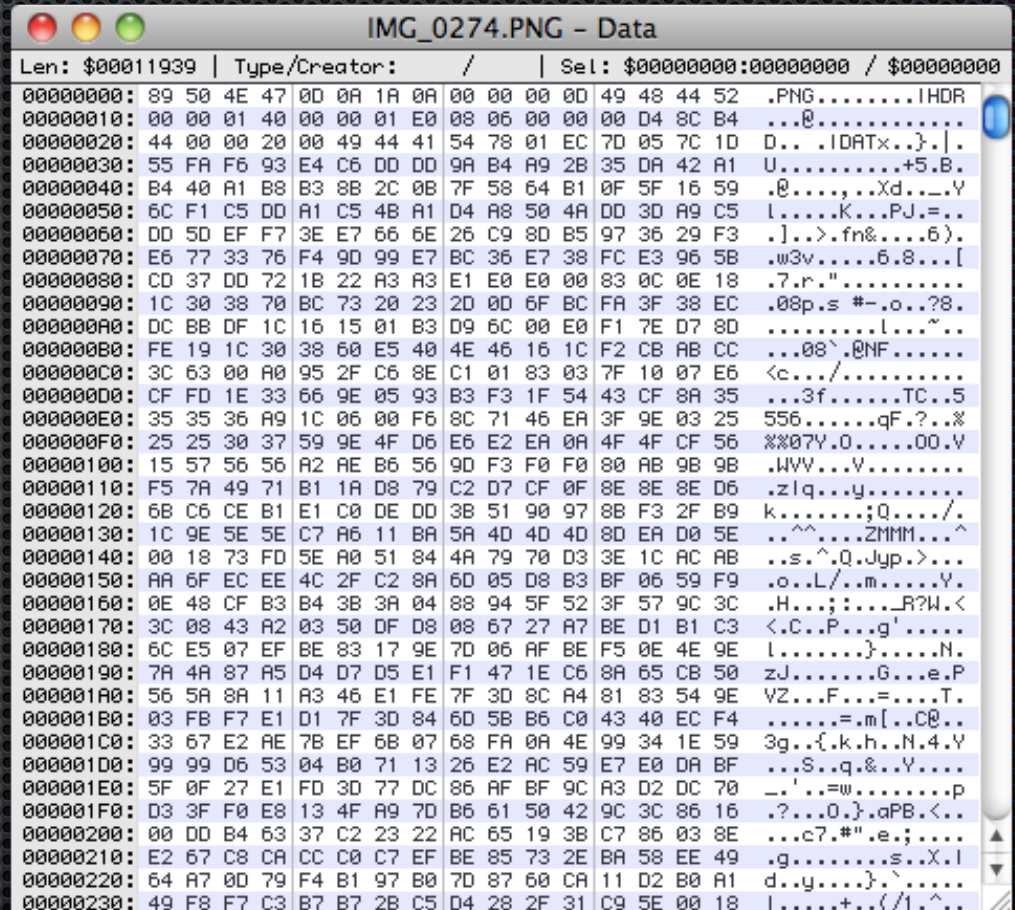
fseek()

fread()

fwrite()

fscanf()

fprintf()



Len: \$00011939	Type/Creator: /	Set: \$00000000:00000000 / \$00000000
00000000:	89 50 4E 47 0D 0A 1A 0A 00 00 00 00 49 48 44 52	.PNG.....IHDR
00000010:	00 00 01 40 00 00 01 E0 08 06 00 00 00 04 8C B4	...@.....
00000020:	44 00 00 20 00 49 44 41 54 78 01 EC 7D 05 7C 1D	D...!DATx... . .
00000030:	55 FA F6 93 E4 C6 DD DD 9A B4 A9 2B 35 DA 42 A1	U.....+5.B.
00000040:	B4 40 A1 B8 B3 8B 2C 0B 7F 58 64 B1 0F 5F 16 59	.@.....Xd...Y
00000050:	6C F1 C5 DD A1 C5 4B A1 D4 A8 50 4A DD 3D A9 C5	l.....K...PJ.=..
00000060:	DD 5D EF F7 3E E7 66 6E 26 C9 8D B5 97 36 29 F3	.]...>.fn&....6).
00000070:	E6 77 33 76 F4 9D 99 E7 BC 36 E7 38 FC E3 96 5B	.w3v.....6.8...[
00000080:	CD 37 DD 72 1B 22 A3 A3 E1 E0 E0 00 83 0C 0E 18	.7.r".....
00000090:	1C 30 38 70 BC 73 20 23 2D 0D 6F BC FA 3F 38 EC	.08p.s #-..o..?8.
000000A0:	DC BB DF 1C 16 15 01 B3 D9 6C 00 E0 F1 7E D7 8Dl.....~..
000000B0:	FE 19 1C 30 38 60 E5 40 4E 46 16 1C F2 CB AB CC	...08`.@NF.....
000000C0:	3C 63 00 A0 95 2F C6 8E C1 01 83 03 7F 10 07 E6	<c.../.....
000000D0:	CF FD 1E 33 66 9E 05 93 B3 F3 1F 54 43 CF 8A 35	...3f.....TC..5
000000E0:	35 35 36 A9 1C 06 00 F6 8C 71 46 EA 3F 9E 03 25	556.....qF.?..%
000000F0:	25 25 30 37 59 9E 4F D6 E6 E2 EA 0A 4F 4F CF 56	%%07Y.0.....00.Y
00000100:	15 57 56 56 A2 AE B6 56 9D F3 F0 F0 80 AB 9B 9B	.WVY...V.....
00000110:	F5 7A 49 71 B1 1A D8 79 C2 D7 CF 0F 8E 8E 8E D6	.z!q...y.....
00000120:	6B C6 CE B1 E1 C0 DE DD 3B 51 90 97 8B F3 2F B9	k.....;Q..../.
00000130:	1C 9E 5E 5E C7 A6 11 BA 5A 4D 4D 4D 8D EA D0 5E	..^^.....ZMMM...^
00000140:	00 18 73 FD 5E A0 51 84 4A 79 70 D3 3E 1C AC AB	..s.^..Q.Jyp.>...
00000150:	AA 6F EC EE 4C 2F C2 8A 6D 05 D8 B3 BF 06 59 F9	.o..L/..m.....Y.
00000160:	0E 48 CF B3 B4 3B 3A 04 88 94 5F 52 3F 57 9C 3C	.H...;.....R?W.<
00000170:	3C 08 43 A2 03 50 DF D8 08 67 27 A7 BE D1 B1 C3	<.C..P...g'.....
00000180:	6C E5 07 EF BE 83 17 9E 7D 06 AF BE F5 0E 4E 9E	l.....}.....N.
00000190:	7A 4A 87 A5 D4 D7 D5 E1 F1 47 1E C6 8A 65 CB 50	zJ.....G...e.P
000001A0:	56 5A 8A 11 A3 46 E1 FE F7 3D 8C A4 81 83 54 9E	VZ...F....=...T.
000001B0:	03 FB F7 E1 D1 7F 3D 84 6D 5B B6 C0 43 40 EC F4=m[...C@..
000001C0:	33 67 E2 AE 7B EF 68 07 68 FA 0A 4E 99 34 1E 59	3g...{.k.h...N.4.Y
000001D0:	99 99 D6 53 04 B0 71 13 26 E2 AC 59 E7 E0 DA BF	...'..=w.....p
000001E0:	5F 0F 27 E1 FD 3D 77 DC 86 AF BF 9C A3 D2 DC 70	..?..0.}.qPB.<..
000001F0:	D3 3F F0 E8 13 4F A9 7D B6 61 50 42 9C 3C 86 16	...c7,#"..e.;...
00000200:	00 DD B4 63 37 C2 23 22 AC 65 19 3B C7 86 03 8E	.g.....s...X..l
00000210:	E2 67 C8 CA CC C0 C7 EF BE 85 73 2E BA 58 EE 49	d..y.....}.^.....
00000220:	64 A7 0D 79 F4 B1 97 B0 7D 87 60 CA 11 D2 B0 A1	l.....+..</1.^..
00000230:	49 F8 F7 C3 B7 B7 2B C5 D4 28 2F 31 C9 5E 00 18	

Raw Binary / Text Data

FILE*

fseek()

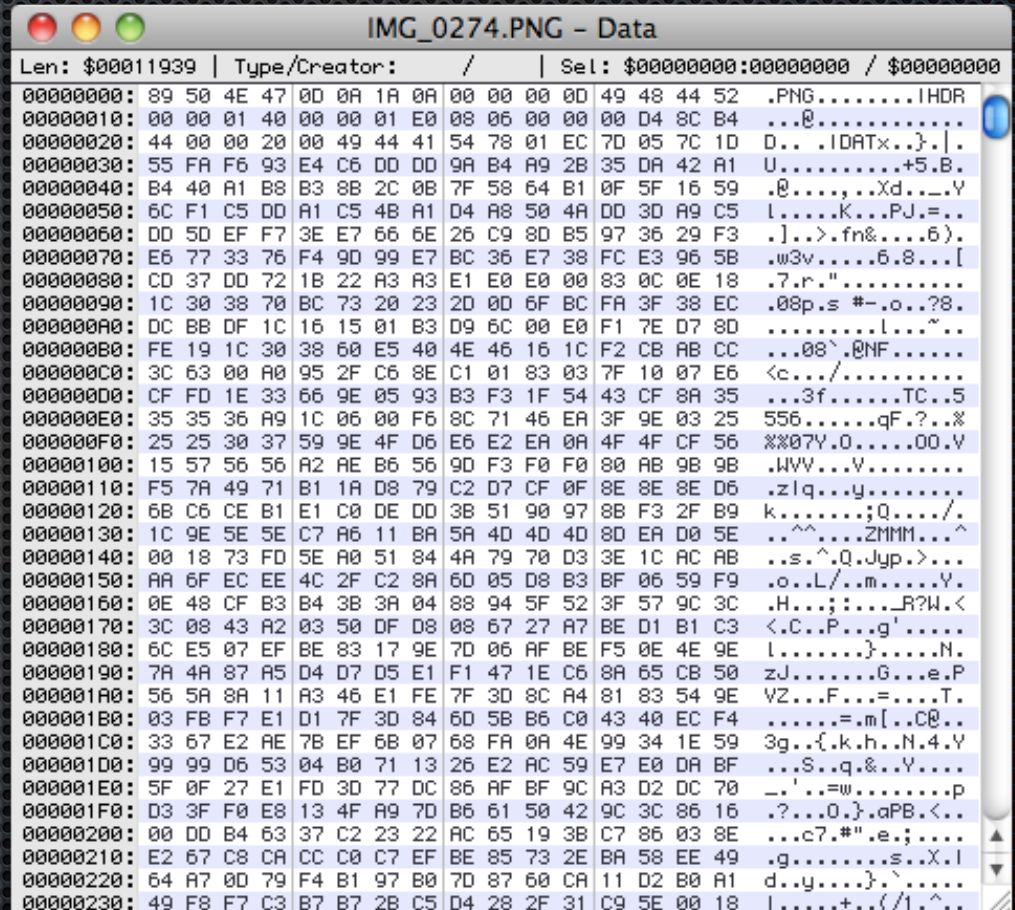
fread()

fwrite()

fscanf()

char*

fprintf()



Buffer Overflow Exploits

HOW THE HEARTBLEED BUG WORKS:

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "POTATO" (6 LETTERS).



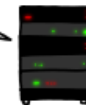
...this page about "books". User Meg wants these 6 letters: **POTATO**. User Ida wants pages about "irl games". Unlocking secure records with master key 513098573343...



HMM...

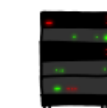


BIRD



...ser Olivia from London wants pages about "snakes in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: **BIRD**. There are currently 346 connections open. User Brendan uploaded the file 634ba962e2c0b9ff89b-d3b-ff8...

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "HAT" (500 LETTERS).



...a connection. Jake requested pictures of deer. User Meg wants these 500 letters: **HAT**. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "Cott0BaSt0r". User...

SERVER, ARE YOU STILL THERE?
IF SO, REPLY "BIRD" (4 LETTERS).



...ser Olivia from London wants pages about "snakes in car why". Note: Files for IP 375.381.283.17 are in /tmp/files-3843. User Meg wants these 4 letters: **BIRD**. There are currently 346 connections open. User Brendan uploaded the file 634ba962e2c0b9ff89b-d3b-ff8...



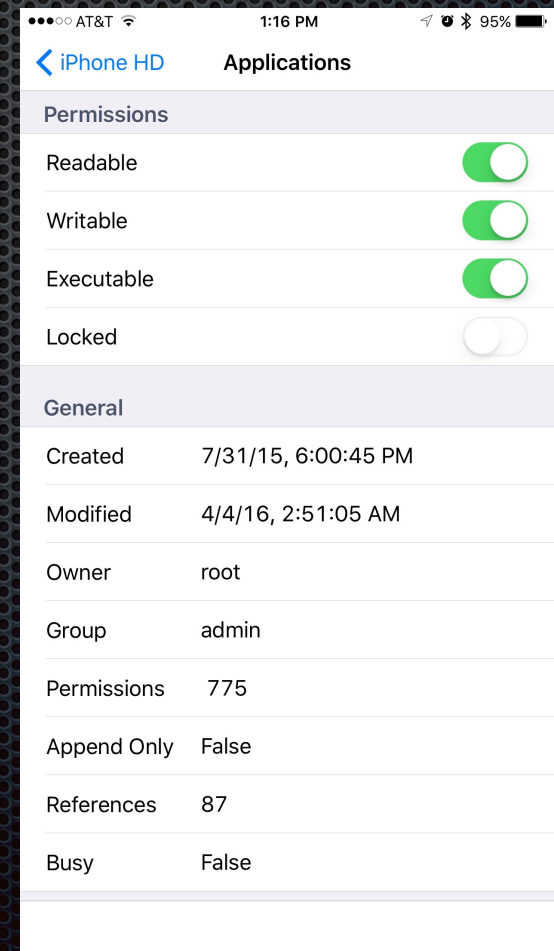
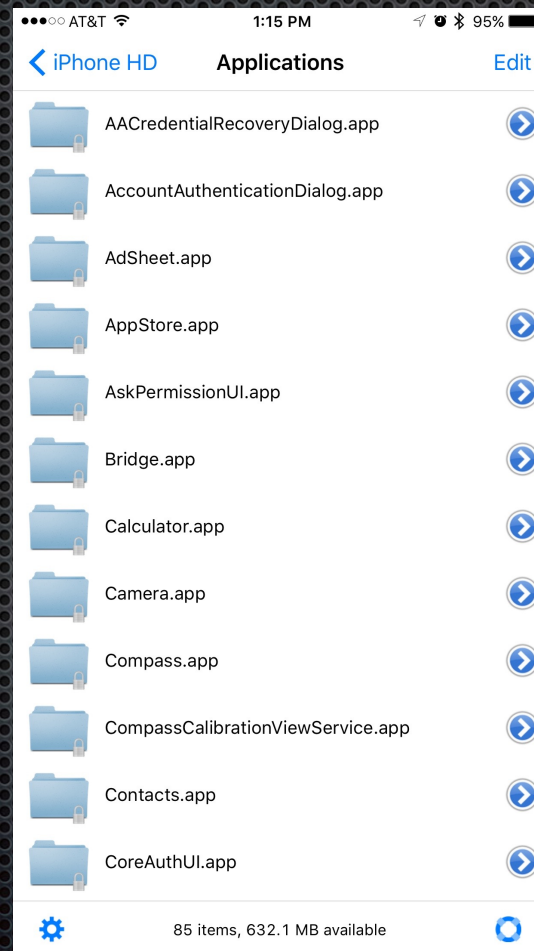
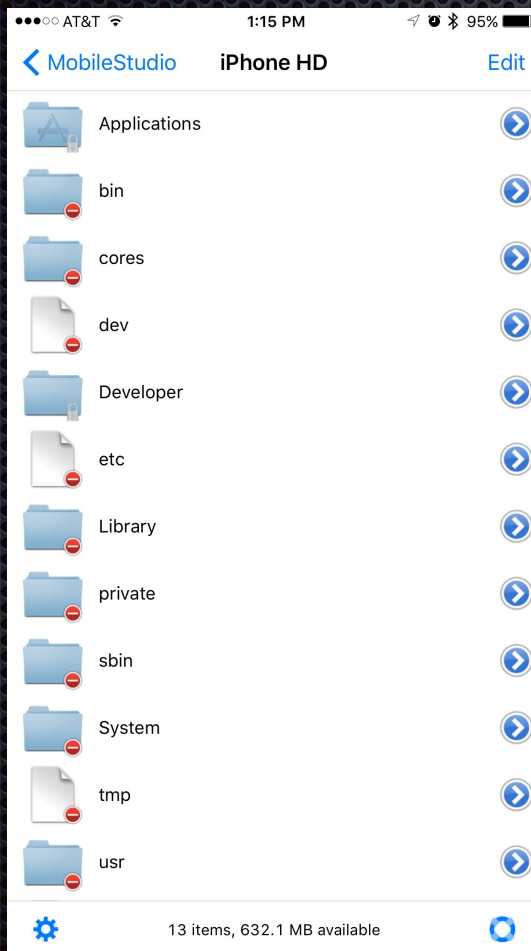
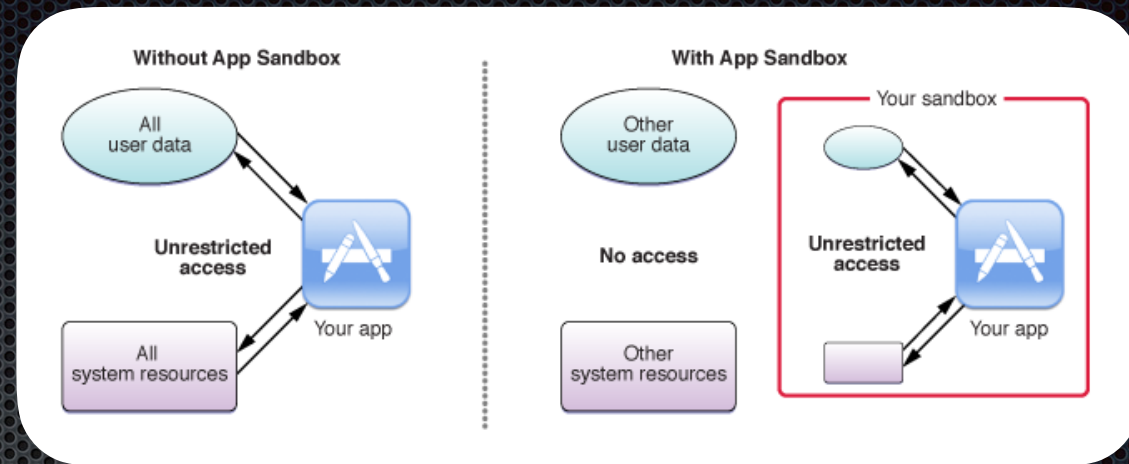
HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "Cott0BaSt0r". User...



...a connection. Jake requested pictures of deer. User Meg wants these 500 letters: **HAT**. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "Cott0BaSt0r". User...

<https://xkcd.com/1354/>

Sandboxing



App Code Signing



Device-Server



Server Interaction

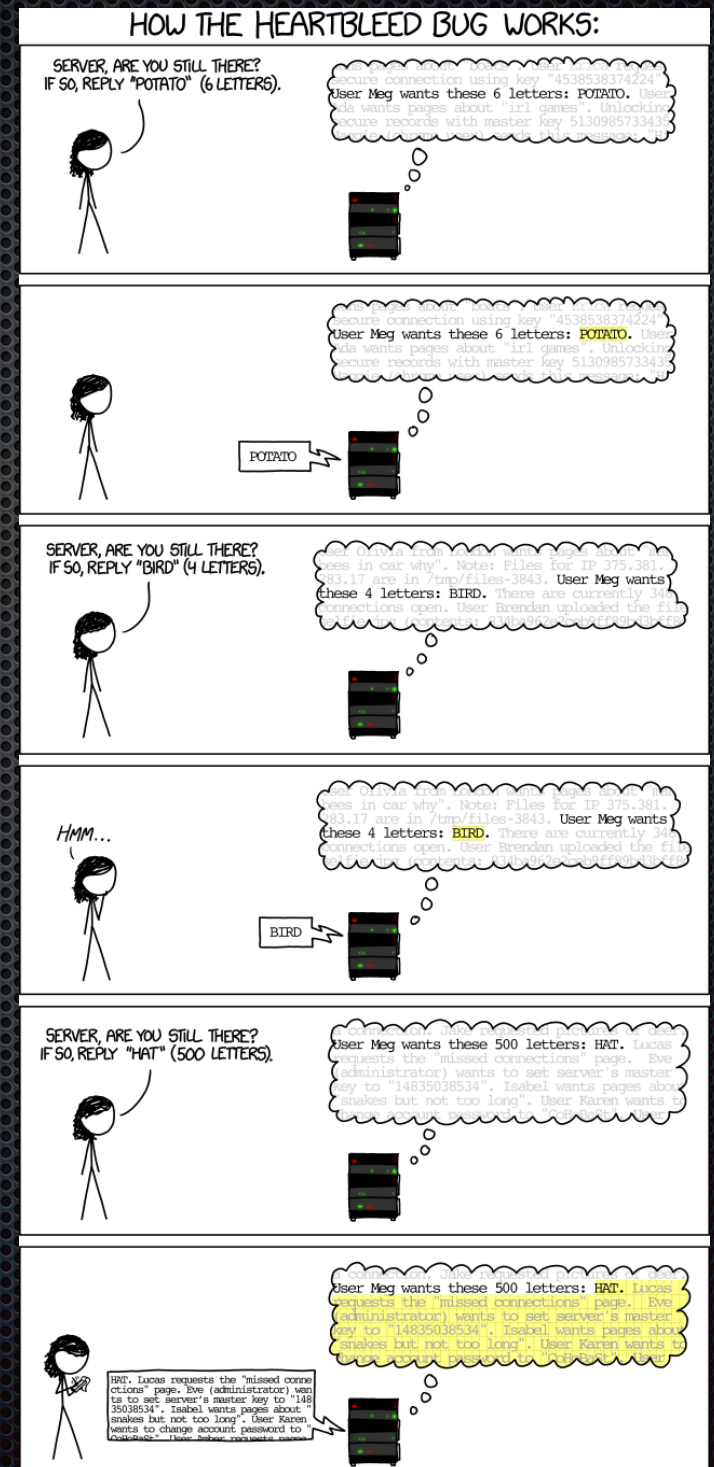
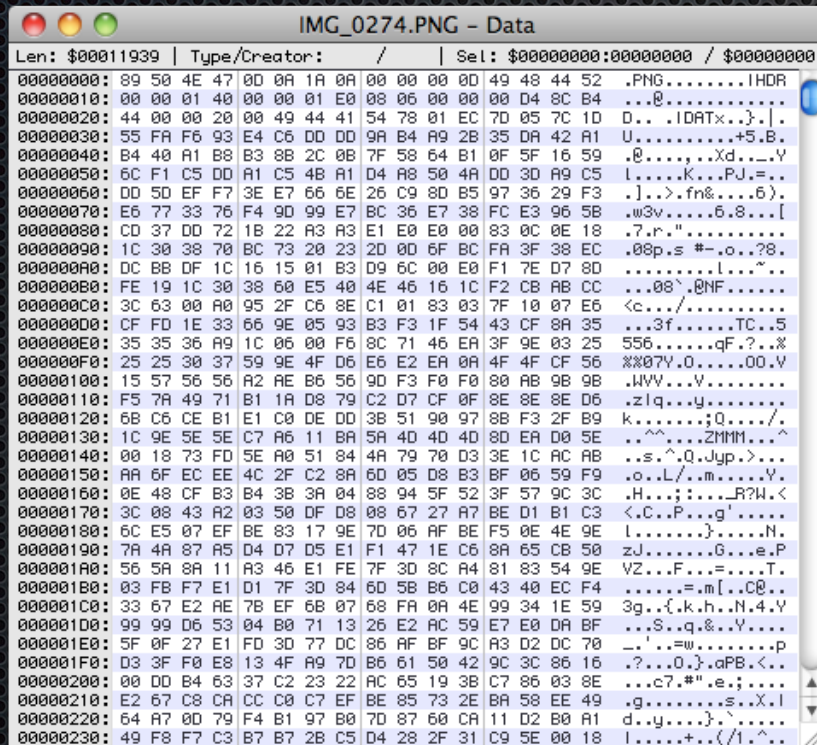


- ✦ **Request** a resource using HTTP and a URL
- ✦ **Wait** for response data to come back from the server
- ✦ **Scrub** the data
 - ✦ Remove superfluous parts
 - ✦ Validate the data
- ✦ **Present** the data to the user



Scrub

Flat Data



Cleaner Way?



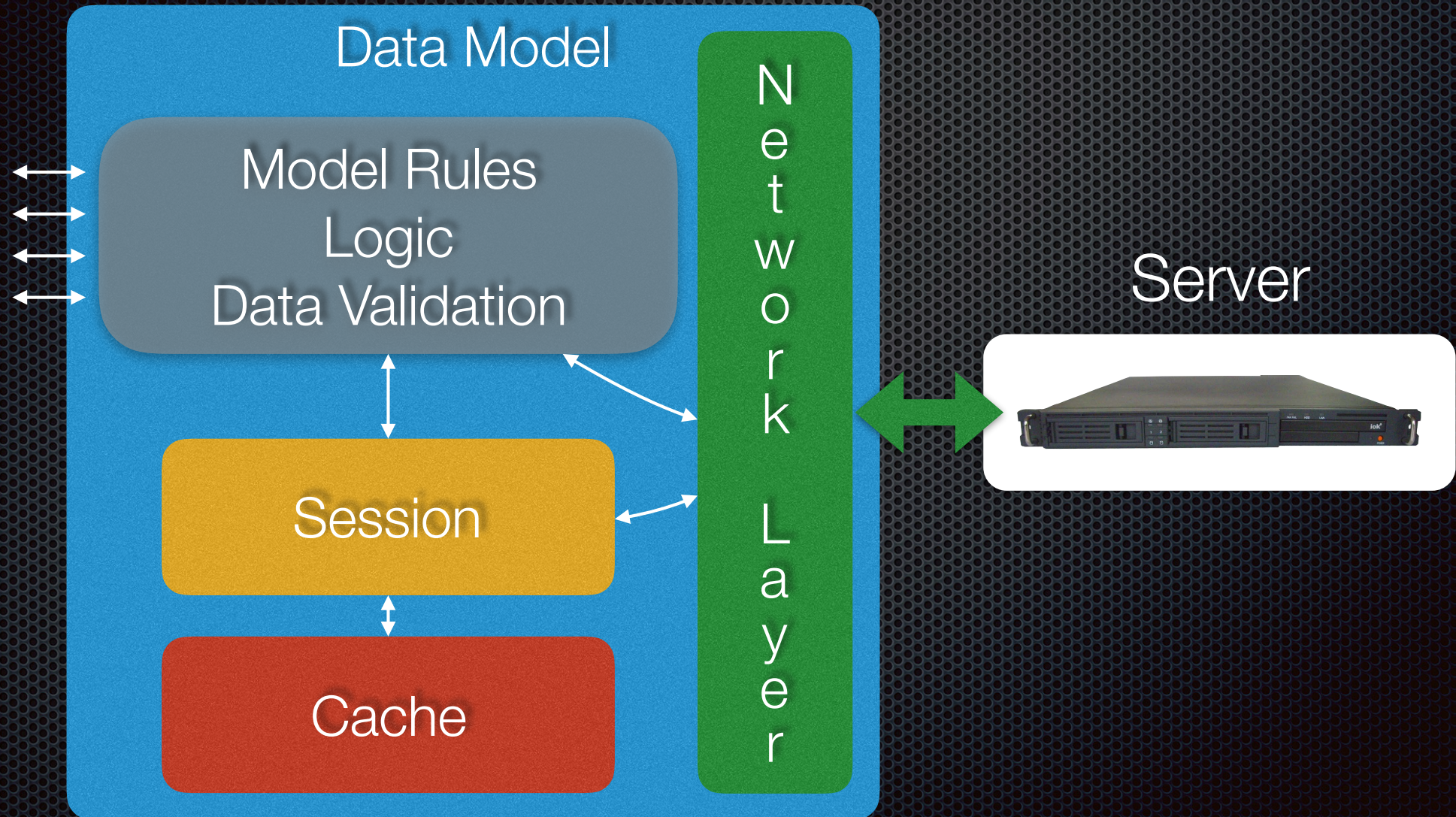
<?xml?>



JSON



Network Architecture



REST



- ✦ Representational State Transfer (REST)
- ✦ Software **architectural style** used in protocols like HTTP

Resource	GET	PUT	POST	DELETE
Collection URI, such as <code>http://example.com/resources/</code>	List the members of the collection, complete with their member URIs for further navigation. For example, list all the cars for sale.	Meaning defined as "replace the entire collection with another collection".	Create a new entry in the collection where the ID is assigned automatically by the collection. The ID created is usually included as part of the data returned by this operation.	Meaning defined as "delete the entire collection".
Element URI, such as <code>http://example.com/resources/7H0U57Y</code>	Retrieve a representation of the addressed member of the collection expressed in an appropriate MIME type	Update the addressed member of the collection or create it with the specified ID.	Treats the addressed member as a collection in its own right and creates a new subordinate of it.	Delete the addressed member of the collection.

See chapter 5 of Roy T. Fielding's doctoral dissertation and REST article on Wikipedia

REST Architectural Constraints



- Client-Server
 - Stateless
 - Cacheable
 - Layered System
 - Uniform Interface
 - Resources and Representations Separate
 - Resources Manipulated by Representation
 - Representation Processing Part of the Message
 - Hypermedia as the Engine of Application State (HATEOAS)
- A server configured to accept **HTTP requests**, return **HTTP responses** with **JSON data payloads**, having **clean hierarchical URLs** fits these constraints.

App Transport Security (HTTPS)

App Transport Security

App Transport Security (ATS) enforces best practices in the secure connections between an app and its back end. ATS prevents accidental disclosure, provides secure default behavior, and is easy to adopt; it is also on by default in iOS 9 and OS X v10.11. You should adopt ATS as soon as possible, regardless of whether you're creating a new app or updating an existing one.

If you're developing a new app, you should use HTTPS exclusively. If you have an existing app, you should use HTTPS as much as you can right now, and create a plan for migrating the rest of your app as soon as possible. In addition, your communication through higher-level APIs needs to be encrypted using TLS version 1.2 with forward secrecy. If you try to make a connection that doesn't follow this requirement, an error is thrown. If your app needs to make a request to an insecure domain, you have to specify this domain in your app's `Info.plist` file.

Supporting App Transport Security

December 21, 2016

App Transport Security (ATS), introduced in iOS 9 and OS X v10.11, improves user security and privacy by requiring apps to use secure network connections over HTTPS. At WWDC 2016 we announced that apps submitted to the App Store will be required to support ATS at the end of the year. To give you additional time to prepare, this deadline has been extended and we will provide another update when a new deadline is confirmed.

[Learn more about ATS.](#)

Device-Device



Bluetooth / NFC

- Hands-Free Profile (HFP 1.5)
- Phone Book Access Profile (PBAP)
- Advanced Audio Distribution Profile (A2DP)
- Audio/Video Remote Control Profile (AVRCP)
- Personal Area Network Profile (PAN)
- Human Interface Device Profile (HID)





iOS Security

iOS 9.3 or later

May 2016

https://www.apple.com/business/docs/iOS_Security_Guide.pdf