SECURING MOBILE APPLICATIONS

Ulf Larson



ulf.larson@owasp.org

Thursday, September 13, 12



ulf.larson@adecco.se

Google ClientLogin Authentication Protocol



Google ClientLogin Authentication Protocol



Google ClientLogin Authentication Protocol



- Authorization header sent over HTTP
- When users connected via wifi, apps automatically sent the token in an attempt to automatically synchronize data from server
- Sniff this value, impersonate the user

ime .	Source	Destination	Protocol	No.	Info							
2.107059	134.60.238.158	289.85.147.136	TCP	23483	51618 > http	[SYN] Sec	q=0 Win=58	48 Len=0 N	(55=1460 T	SV=58257	TSER=8	WS=1
2.108227	134.60.238.158	209.85.147.136	TCP	23484	51610 > http	[SYN] Sec	-0 Win-58	40 Len-0 N	(SS=1460 T	SV=58257	TSER-6	WS=1
2.189754	134.60.238.158	209.85.147.136	TCP	23485	51610 > http	[SYN] Sec	q=0 Win=58	40 Len=0 M	ISS=1460 T	SV=58257	TSER=8	WS=1
2.136078	289.85.147.135	134.60.238.158	TCP	23491	http > 51618	[SYN, ACH	K] Seq=0 A	ck=1 Win=5	672 Len=8	MSS=1430	TSV=7	4566883 TSER=
2.155532	134.60.238.158	209.85.147.136	HTTP	23508	GET /data/fe	ed/api/use	er,	<pre>?imgmax=1</pre>	18246max-r	results=10	005th	unbsize=144u,1
2.175801	269.85.147.136	134.60.238.158	TCP	23505	http > 51610	[ACK] Sec	q=1 Ack=53	7 Win=6784	Len=0 TS	V=7459692	8 TSEF	1=58262
2.418105	 Follow TCP Stream 										- 0.2	38 Len=0 TSV
2.418417	Stream Content											38 Len=0 TSV
2. THE LOCAL	Serverin Concern											
2.503555	GET /data/feed/api/user/	7imgmax=182	46max-resu	ults=100	06thumbsize=1	44u,1024u	6visibilit	y=visible	Skind-alb	um HTTP/1.	1.	
2.503555 2.506605	GET /data/feed/api/user/ GData-Version: 2	?imgmax=182	46max-resu	ults=100	06thumbsize=1	44u,1024u	ővisibilit	y=visible	Skind—alb	um HTTP/1.	1	-74587253
2.503555 2.506605 2.507338	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip	7imgmax=182	46max-resu	ults=100	06thumbsize=1	44u,1024u	6visibilit	y=visible	Skind—alb	um HTTP/1.	1	=74587253 =74587253
2.503555 2.506605 2.507338 2.508620	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog	7imgmax-182	46max-resu	ults=100	06thumbsize=1	44u,1024u	6visibilit	y=visible	Skind−alb	un HTTP/1.	1	=74587253 =74507253 0 Len=0 TSV=
2.501008 2.503555 2.506605 2.507338 2.500520 2.509169	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLoo Vx365_1vCUeYJ3b8P0bZ05g4	71mgnax=182 gin auth=DQAAAKYAAAQ AE6sW5hKQZ9naw7ZSvu	46max-resu	ults=100	065thumbsize=1	44u, 1824u	6visibilit	y-visible	Skind−alb	um HTTP/1.	1	=74587253 =74587253 =74507253 =0 Len=8 TSV= =0 Len=8 TSV=
2.563555 2.566665 2.507338 2.566628 2.568628 2.569169 2.527908	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx365_1vCUeYJ3b8P0b205g/ Bm8m-o050RNjBvn6k5x0L400	7imgmax-102 gin auth=DQAAAKYAAAA AE6sW5hKQ29naw72Svu cwr82q5nUFYiAHfmzg	46nax-resu	ults=100	065thumbsize=1	44u, 1024u	6visibilit	y-visible	Skind—alb	un HTTP/1.	1	=74587253 =74587253 0 Len=8 TSV= 0 Len=8 TSV= 0 Len=8 TSV=
2.503608 2.503555 2.506605 2.507338 2.508628 2.509169 2.527908 2.538535	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx365_1vCUeYJ3b8P0b205g/ Bn8m-o05ORNjBvnGk5x0L400 Host: picasaweb.google.c	7imgmax-102 gin auth=DQAAAKYAAAA AE6sW5hKQ29naw72Svu ewr82q5nUFY1AHfmzg com	46nax-resu	ults=100	06thumbsize-1	44u, 1024u	6visibilit	y=visible	Skind—alb	un HTTP/1.		-74587253 -74507253 0 Len=8 TSV= 8 Len=8 TSV= 9 Len=8 TSV= 9 Len=8 TSV=
2,501000 2,503555 2,506605 2,507338 2,508620 2,509169 2,527908 2,510535 2,539016	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx365 1vCUeYJ3b8P0b205g/ Bm8m-0050RNjBvnGk5x0L40c Host: picasaweb.google.c Connection: Keep-Alive	71mgmax-102 gin auth=DQAAAKYAAAA AE6sW5hK029naw72Svu ewr82q5nUFY1AHfmzg com	46max-resu	ults=100	06thumbsize-1	44u, 1024u	ővisibilit	y-visible	Skind∸alb	um HTTP/1.	1	=74597253 =74597253 0 Len=0 TSV= 9 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= =74597253
2,501000 2,503555 2,506605 2,507338 2,508628 2,509169 2,527908 2,527908 2,527908 2,527908 2,5239015 2,539015	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx3GS lvCUeYJ3b8P0b20Sg/ Bm8m-00SORNjBvnGk5x0L40c Host: picasaweb.google.c Connection: Keep-Alive User-Agent: Cooliris-GDa	7imgmax-102 gin auth=DQAAAKYAAAA AE6sW5hK029naw72SvuV ewr02q5nUFY1AHfmzg com ata/1.0; gzip	46max - resu	ults=100	06thumbsize-1	44u, 1024u	ővisibilit	y=visible	Skind-alb	um HTTP/1.	1	-74507253 -74507253 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= =74507253 6 Len=0 TSV=
2.501000 2.50355 2.506605 2.507338 2.508620 2.509109 2.527908 2.527908 2.527908 2.527908 2.529515 2.539616 2.539626 2.539670	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoggleLog Vx365 lvCUeYJ3b8P0b205g/ Bm8m-0050RNjBvnGk5x0L40c Host: picasaweb.google.4 Connection: Keep-Alive User-Agent: Cooliris-GDa	71mgmax-102 gin auth=DQAAAKYAAAA AE6sW5hK029naw725vu0 ewr02q5nUFY1AHfmzg com ata/1.0; gzip	46max-resu	ults=100	96thumbsize=1	440,10240	6visibilit	y=visible	Skind−alb	un HTTP/1.	.1	-74507253 -74507253 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= 2 Len=0 TSV= =74507253 6 Len=0 TSV= 6 Len=0 TSV=
2,502000 2,503555 2,506605 2,507338 2,508628 2,508628 2,508628 2,509169 2,527908 2,527908 2,527908 2,5235016 2,539616 2,539626 2,539670 2,541038	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx365 lvCUeYJ3b8P0b205g/ BnBm-0050RNjBvnGk5x0L40c Host: picasaweb.google.c Connection: Keep-Alive User-Agent: Cooliris-60a (2122 bytes missing in 4	71mgmax-102 gin auth=DQAAAKYAAAA AE6sW5hK029naw725vul ewr02q5nUFY1AHfmzg com ata/1.0; gzip capture file].SR.1	46max-resu .jb.%≷<	ults=100	96thumbsize=1 SZpl6Vf	44u,1024u	6visibilit F:∀7	y=visible	Skind-alb	un HTTP/1.	1	-74507253 -74507253 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= -74507253 6 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV=
2,502000 2,503555 2,506605 2,507338 2,508620 2,508620 2,508620 2,527908 2,528535 2,539616 2,539626 2,539670 2,541038 2,544082	GET /data/feed/api/user/ GData-Version: 2 Accept-Encoding: gzip Authorization: GoogleLog Vx365 lvCUeYJ3b8P0b205g/ Bn8m-0050RNjBvnGk5x0L40c Host: picasaweb.google.c Connection: Keep-Alive User-Agent: Cooliris-60a (2122 bytes missing in c (168	7imgmax-102 gin auth=DQAAAKYAAAA AE6sW5hKQ29naw725vul ewr02q5nUFYiAHfmzg com ata/1.0; g2ip capture file].SR.1 	46max-resu .jb.%%< qWv. <u< td=""><td>ults=100</td><td>6&thumbsize=1</td><td>44u,1024u .*X.L07g.].%.t XY.Z</td><td>Gvisibilit F:wY7 Y</td><td>y=visible 1.V.oB(. </td><td>Skind-alb</td><td>un HTTP/1.</td><td>1</td><td>-74507253 -74507253 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= 2 Len=0 TSV= 5 Len=0 TSV= 6 Len=0 TSV= 6 Len=0 TSV= 6 Len=0 TSV=</td></u<>	ults=100	6&thumbsize=1	44u,1024u .*X.L07g.].%.t XY.Z	Gvisibilit F:wY7 Y	y=visible 1.V.oB(. 	Skind-alb	un HTTP/1.	1	-74507253 -74507253 0 Len=0 TSV= 0 Len=0 TSV= 0 Len=0 TSV= 2 Len=0 TSV= 5 Len=0 TSV= 6 Len=0 TSV= 6 Len=0 TSV= 6 Len=0 TSV=



Evil twin

((Q))

authToken over http

99% of all android phones were vulnerable

Free WiFi-hotspot

Thursday, September 13, 12

MOBILE DEVELOPMENT IS NO DIFFERENT FROM OTHER DEVELOPMENT

- Security (at the application layer) means being aware of how your code uses information and ensuring that it does so safely and responsibly
 - Keep personal data safe from prying eyes
 - Ensure that your software collects only the information that it requires.
 - Prevent unauthorized access to or modification of the data while in transit.

SECURITY IS NOT A BULLET POINT ITEM

- The most important thing to understand about security is that it is not a bullet point item.
- Security cannot be bolted on at the end of the development process.
- You must **consciously design security into your app or service from the very beginning**, and make it a conscious part of the entire process from design through implementation, testing, and release.



SECURITY IS NOT A BULLET POINT ITEM

- The most important thing to understand about security is that it is not a bullet point item.
- Security cannot be bolted on at the end of the development process.
- You must consciously design security into your app or service from the very beginning, and make it a conscious part of the entire process from design through implementation, testing, and release.



HOW CAN OWASP ASSIST MOBILE DEVELOPERS?

						Log in / create account			
	$W/\Delta SP$								
The C	Den Web Application Security Project								
F	Page Discussion	R	ead View	source	View history	Go Search			
avigation ome	OWASP Mobile Security Project								
ews WASP Projects ownloads	Project Overview For Mobile Security Testers Mobile Secure Development Guidelines Top Ten Mobile OWASP MobiSec Project	Risks Top Ten M	obile Controls	OW/	ASP GoatDroid Proje	OWASP Mobile Threat Model Project			
ocal Chapters obal Committees opSec Job Board	The OWASP Mobile Security Project is a centralized resource intended to give developers and security teams the resources they need to build and maintain secure mobile applications. Through the project, our is to classify mobile security risks and provide developmental controls to reduce their impact or likelihood of exploitation.								
pSec Conferences neat Sheets WASP Training	We have a Google Doc up where anyone that wants to be involved with the project can add their thoughts, so /d/1bScrvrLJLOHcSbztjBxYoN-jN3kR8bViy9tF8Nx0c08/edit 🔂. There are various tasks that people have started	uggestions, and tak ad over the past 6 m	e ownership onths with v	of initiativ arying lev	res. https://docs.go rels of quality and c	ogle.com/document completeness.			
esentations	PROJECT INFO				RELEASE(S) INF	0			
deo	What does this OWASP project offer you?			What rel	eases are available fo	r this project?			
ress et OWASP Books	what is this project?	CL	irrent rele	ase					
et OWASP Gear	Name: OWASP Mobile Security Project (home page)	Not Yet Published							
ailing Lists	Purpose: Our primary focus is at the application layer. While we take into consideration the underlying mobile	last i	eviewed r	elease					
oout OWASP	platform and carrier inherent risks when threat modeling and building controls, we are targeting the areas that	Not Yet Reviewed							
embership	the average developer can make a difference. Additionally, we focus not only on the mobile applications deployed to end user devices, but also on the broader server-side infrastructure which the mobile apps		all release	s					
eference	communicate with. We focus heavily on the integration between the mobile application, remote authentication services, and cloud platform-specific features.								
ow To	License: N/A								

https://www.owasp.org/index.php/OWASP_Mobile_Security_Project



OWASP MOBILE THREAT MODEL





OWASP MOBILE TOP 10 RISKS

OWASP Mobile Top 10 Risks

M1- Insecure Data	M6- Improper Session
Storage	Handling
M2- Weak Server Side	M7- Security Decisions
Controls	Via Untrusted Inputs
M3- Insufficient Transport Layer Protection	M8- Side Channel Data Leakage
M4- Client Side Injection	M9- Broken Cryptography
M5- Poor Authorization	M10- Sensitive
and Authentication	Information Disclosure



OWASP MOBILE DESIGN GUIDELINES

- I. Identify and protect sensitive data on the mobile device
- 2. Handle password credentials securely on the device
- 3. Ensure sensitive data is protected in transit
- 4. Implement user authentication/authorization and session management correctly
- 5. Keep the backend APIs (services) and the platform (server) secure
- 6. Perform data integration with third party services/applications securely
- 7. Pay specific attention to the collection and storage of consent for the collection and use of the user's data
- 8. Implement controls to prevent unauthorized access to paid-for resources (wallet, SMS, phone calls etc...)
- 9. Ensure secure distribution/provisioning of mobile applications
- 10. Carefully check any runtime interpretation of code for errors



OWASPTRAINING ENVIRONMENTS





Secure coding training environments for Android and iOS developers

Thursday, September 13, 12



Developed by Kenneth R. van Wyk



Exercises Introduction

Home

Server Communication

This exercise demonstrates the need for protecting sensitive data when it is in transit from the iOS device to the server. In the first step, you are presented with an authentication page. From there, you will log in using the provided account credentials--and see whether they get compromised in transit.

Credits

Start Exercise

Thursday, September 13, 12

SAMPLE IGOAT EXERCISE: PROTECT DATA IN TRANSIT



WHAT DID WE LEARN FROM THIS EXERCISE?



WHAT DID WE LEARN FROM THIS EXERCISE?



Protect data in transit!

- Man-in-the-middle attacks
- Tampering w/ data in transit
- Confidentiality of data lost

COMMON PITFALLS

- Complete lack of encryption for transmitted data
 - Or, only encrypting the login page (cf introductory example)
- Weakly encrypted data in transit
- Strong encryption, but ignoring security warnings
 - Ignoring certificate validation errors
 - Falling back to plain text after failures

MOBILETOPTEN #1 - INSECURE DATA STORAGE

- Sensitive data left unprotected
- Applies to locally stored data + cloud synced
- Generally a result of:
 - Not encrypting data
 - Caching data not intended for long-term storage
 - Weak or global permissions
 - Not leveraging platform best-practices

REAL LIFE EXAMPLE: FACEBOOK DATA LEAKAGE



Works from any computer if PIN is not set, and if USB is inserted to charge phone, the .plist-file can be extracted.

.plist-file used for storing confidential data

- full oAuth key and secret in plain text.
- these are encrypted or salted with the device ID...only not.
- and they expired January 4001!

ATTACK VECTOR: LOST/STOLEN DEVICE

00	iExplorer					IE	म
		A 🔽		9),	
Back/Forward View Mode Copy Music Ope	n Files on iDevice	Mount Disk New Fo	lder Delete F	Refresh	Book	marks	
Name	File Type	Size			Date	Modified	
▼ Spotify							
▼ Documents				7/	7/11	1:02 PM	N
▼ □ Library				5/	6/12	8:19 AN	4
Application Support				6/1	1/12	2 1:36 PM	N
▼ Caches				6/	2/12	2 1:45 PM	N
com.plausiblelabs.crashreport		DIORE	٦٢	6/	2/12	2 1:45 PM	N
com.spotify.client				6/9	/12	11:29 AN	N
com.testflight.testflightsdk		-		5/	6/12	8:19 AN	N
▶ i crashes				6/	2/12	2 1:45 PM	1
Snapshots				6/1	1/12	2 1:36 PM	N
▶ 🔤 VolatileCache				6/	7/12	2 5:27 PM	N
▼ 🔤 Cookies				1/2	7/12	2 7:57 PM	N
Cookies.binarycookies	BINARYCOOKIES	1 kB		1/2	7/12	2 7:57 PM	N
▶ 🚞 Mail				7/2	9/11	6:26 PM	N
Preferences				6/1	1/12	2 1:56 PM	N
com.apple.dataaccess.launchd	LAUNCHD			7/2	9/11	6:24 PM	4
com.apple.PeoplePicker.plist	PLIST	68 B		6/	2/12	9:51 AM	N
com.spotify.client.plist	PLIST	2 kB		6/1	1/12	2 1:56 PM	N
🕨 🧰 WebKit				4/1	7/12	8:03 AN	N
Spotify.app				5/2	9/12	6:53 AM	N
▶ 🚞 tmp				6/	2/12	2 1:45 PM	N
TunesArtwork		35 kB		6/	2/12	9:51 AM	N
📄 iTunesMetadata.plist	PLIST	1 kB		6/	2/12	9:51 AM	N
▶ 🚞 WhatsMyIP				60			- les
▶ 🚞 Media				60			<k0< td=""></k0<>
Capacity: 5.93 GB used of 13.7 GB				61			<11
			6	62			<ke< td=""></ke<>
				63			<s1< td=""></s1<>
				64			<ke< td=""></ke<>
				65			-+-
				05			20
				66			<k6< td=""></k6<>
				67			<ti< td=""></ti<>
				68			<ke< td=""></ke<>
				69			<s1< td=""></s1<>
				70	-	<td>ict;</td>	ict;
				71	-	<td>list</td>	list

App bundle – Hexdump of binary

– plist file

Explore folders

- ./Documents
- ./Library/Caches/*
- ./Library/Cookies
- ./Library/Preferences

	<pre><key>launchCount</key> <integer>92</integer> <key>password</key> <string>4e6e1e6144431fcde96 <key>proVersion</key> <true></true> <key>ratePopupShowed</key></string></pre>	5a0657729d66b5b1f48df9
V V	<true></true> <key>username</key> <string>drlarson</string> /dict> /plist>	TextWrangler

What's up with vasttrafik's travel planner?

▶ 🔄 Shazam			
🔻 🚞 Reseplanerare			
Documents			
The second secon			
▶ 💼 Caches			
Preferences			
com.apple.PeoplePicker.plist	PLIST	68 B	
com.vaesttrafik.reseplaneraren.plist	PLIST	37 kB	
▶ 💼 WebKit			
▶ 📺 tmp			
▶ 🔤 Vaesttrafik.app			
iTunesArtwork		50 kB	
iTunesMetadata.plist	PLIST	1 kB	
▶ 📺 TrueCaller			
FAIL Blog			
		1	

Let's find out, shall we?

IMPACT

- Confidentiality of data lost
- Credentials disclosed
- Privacy violations
- Non-compliance
- Attack vectors?

PREVENTION TIPS

- Store ONLY what is absolutely required
- Leverage secure containers and platform provided file encryption APIs
- Do not grant files world readable or world writeable permissions

ROUND-UP

- Security cannot be bolted on at the end of the development process.
- OWASP has lots of resources: threat models, top lists, and training environments. Also, everything is FREE
- There may be serious concerns to brand and business if it turns out that your app discloses private information or breaks laws or regulations

 Overall good advise, models, lists, controls and training apps: https://www.owasp.org/index.php/ OWASP_Mobile_Security_Project
 Owasp top ten mobile risks explained in detail with examples: http://www.slideshare.net/JackMannino/owasp-top-10mobile-risks
 Mainly for developers (and testers to some extent): http://www.isecpartners.com/storage/docs/presentations/ secure_development_on_ios.pdf

OS security architecture (by Apple!): http://images.apple.com/ipad/business/docs/iOS_Security_May12.pdf