Studying TLS Usage in Android Apps

Abbas Razaghpanah, Arian Akhavan Niaki, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Johanna Amann, Phillipa Gill





WIRED

Ē

f



WIRED

SHAR

SHARE

E

f







Encryption is Everywhere

It's Time to Encrypt the Entire Internet

KLINT FINLEY BUSINESS 04.17.14 06:30 AM

ENTIRE INTERNET

Encrypted Web Traffic More Than Doubles After NSA Revelations

KLINT FINLEY BUSINESS 05.16.14 05:14 PM

ΗВ TIAN DOUDLLO AFTER NSA REVELATIONS

However...

- TLS is also an important component of mobile applications
 - 88% of Android applications use TLS
- Unlike Web browsers and servers...
 - ...many application developers implementing TLS ...many opportunities to make errors!









Understanding TLS on Android

- Understanding of TLS on Android has been limited ...
- Static analysis: Explores all code paths, but not neccessarily those taken in practice
- Dynamic analysis: May not cover all code paths

- Our Solution: Lumen
- User space traffic monitoring on Android
- Crowd source measurements of application behavior
- Collect anonymized TLS handshake data between apps and servers



- Our study is deemed to be non-human-subject research by UC Berkeley's IRB
- We collect no private information of traffic (encrypted or unencrypted)
- All web browser traffic is excluded
- We are studying software, not people
- We have a comprehensive consent process in place

...Wait a minute

* 💎 📉 🗗 3:33

• Our s Berk

- We c
- All w
- we a
- Weh

Welcome to Lumen

Tutorial. Page 1/3.

Often times, mobile apps leak personal information for advertising and tracking purposes.

Lumen is a tool that helps you to keep your personal data under control and obtain network traffic logs. It analyzes your app's traffic to identify personal information leaks and the organizations collecting such sensitive data.

Lumen may not be supported by all devices due to lack of platform support. This is the case of some Samsung devices. We would love to hear from you if you encounter any problems so that we can improve Lumen!

Lumen is brought to you by academic researchers at the International Computer Science Institute, Berkeley, CA, USA and IMDEA Networks Institute, Madrid, Spain. Lumen is part of an academic research project sponsored by the NSF and Data Transparency Lab.

n-human-subject research by UC

tion of traffic (encrypted or unencrypted)

uded

people

nsent process in place



...Wait a minute

...Wait a minute * 💎 📉 🗗 3:33 Ē 💿 Tutorial. Page 🛛 💿 Tutorial. Page 2/3. subject research by UC • Our s **Data Collection** Welc Berk Our main motivation at the time of developing Lumen is Often times, mobile app providing a tool that promotes mobile transparency and advertising and trackin helps mobile users to understand the fate of their personal Lumen is a tool that he data. fic (encrypted or unencrypted) We c under control and obtai your app's traffic to ide However, Lumen is also a research tool. Analyzing tracking services and privacy leaks is very hard to do in the lab. the organizations collect With Lumen, we can obtain completely anonymous traffic Lumen may not be supp traces in the wild by crowd-sourcing means which help of platform support. Th us enormously to advance the state of the art. The data, devices. We would love • All w will be useful to create research publications and also to any problems so that w help regulators and other stake holders to prevent abusive practices. Lumen is brought to yo International Computer We follow strict ethical research guidelines. Therefore, USA and IMDEA Netwo we collect aggregated and anonymized information about is part of an academic how your mobile apps connect with online services. Lumen we a NSF and Data Transpar exports no private information from your phone: all your personal data remains with you. We do not share this information with commercial third parties. cess in place Weh Previous Next

 \triangleleft

 \triangleleft

0

				Wait
		Tutorial. Page	Tutorial. Page 2,	Tutorial. Page 3/3.
•	Our s Berk	Welc	Data	TLS Interce
•	We c	Often times, mobile app advertising and tracking Lumen is a tool that hel under control and obtain your app's traffic to iden the organizations colled	Our main motivation at the providing a tool that promoted helps mobile users to und data. However, Lumen is also a services and privacy leak	Some apps may use encrypted ch personal information to their online Lumen can exploit apps that do no to perform TLS interception (also middle) locally on your device. This understand what data your apps lo
•	All w	Lumen may not be suppof of platform support. The devices. We would love any problems so that we Lumen is brought to yo	With Lumen, we can obta traces in the wild by crow us enormously to advanc will be useful to create re help regulators and other practices.	channels. The next dialog will allow you to e you can always enable and disable under the TLS settings bar.
•	We a	International Computer USA and IMDEA Netwo is part of an academic NSF and Data Transpar	We follow strict ethical re we collect aggregated an how your mobile apps co exports no private inform personal data remains wi information with commer	
•	We h			
			Previous	Previous
		\triangleleft	\triangleleft	

a minute * * * 3:33

rception

d channels to upload your online servers.

to not use correctly TLS also known as man-in-theto This allows you to also aps leak over encrypted

to enable this feature which sable in Lumen's app settings

search by UC

ted or unencrypted)

ce



				Wait
		Tutorial. Page	Tutorial. Page 2,	Tutorial. Page 3/3.
•	Our s Berk	Welc	Data	TLS Int
•	We c	advertising and trackin Lumen is a tool that hel under control and obtai your app's traffic to idea the organizations collect	providing a tool that prom helps mobile users to und data. However, Lumen is also a services and privacy leak	personal information to their Lumen can exploit apps that to perform TLS interception middle) locally on your devic understand what data your a
•	All w	Lumen may not be supp of platform support. The devices. We would love any problems so that we Lumen is brought to yo	With Lumen, we can obta traces in the wild by crow us enormously to advanc will be useful to create re help regulators and other practices.	channels. The next dialog will allow you you can always enable and d under the TLS settings bar.
•	We a	International Computer USA and IMDEA Netwo is part of an academic NSF and Data Transpar	We follow strict ethical re we collect aggregated an how your mobile apps co exports no private inform personal data remains wi information with commer	
•	We h			
			Previous	Previous
		\triangleleft	\bigtriangledown	\bigtriangledown



				Wait
		Tutorial. Page	Tutorial. Page 2,	Tutorial. Page 3/3.
•	Our s Berk	Welc	Data	TLS Int
•	We c	advertising and trackin Lumen is a tool that hel under control and obtai your app's traffic to idea the organizations collect	providing a tool that prom helps mobile users to und data. However, Lumen is also a services and privacy leak	personal information to their Lumen can exploit apps that to perform TLS interception middle) locally on your devic understand what data your a
•	All w	Lumen may not be supp of platform support. The devices. We would love any problems so that we Lumen is brought to yo	With Lumen, we can obta traces in the wild by crow us enormously to advanc will be useful to create re help regulators and other practices.	channels. The next dialog will allow you you can always enable and d under the TLS settings bar.
•	We a	International Computer USA and IMDEA Netwo is part of an academic NSF and Data Transpar	We follow strict ethical re we collect aggregated an how your mobile apps co exports no private inform personal data remains wi information with commer	
•	We h			
			Previous	Previous
		\triangleleft	\bigtriangledown	\bigtriangledown

a minute

Ó		ŏ		X	8 🔷 📉 🗗 3	3:34
Lumen		Lumen		\$	<	1
номе	LEAKS	номе	LEAKS	APPS	TRAFFI	С
Lu	imen monito	i Name	the certific	cate		
	In stall D	Certifica	te name:			
	Install Ro	lumen-c	a			
lf you want traffic, you Please, sel	t Lumen to be able need to install its r ect Install to proce	to o Credenti eo VPN and	ial use: dapps		•	
Ca	ancel	The packa one CA cer	ge contains: rtificate			
				CANCEL	ОК	

 \triangleleft O \triangleleft O

- Three key items:
 - Client Hello
 - Server Hello (with certificates)
 - Failures of our TLS proxy (reveals pinning)
- Use Con App Don TCF Unic TLS

What do we collect?

rs	>5,000 from >100 count
nections (11/15—6/17)	1,486,082
S	7,258
nains (unique SNIs)	34,176
orts of the second seco	250
que device/OS combos	891
proxy failures	684,209 (4,268 apps and 10,753 domains)

•	TIS RSA WITH AFS 198 GCM SHAPER
	TLS RSA WITH AES 128 CBC SHA256
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV_
	TLS_ECDH_RSA_WITH_RC4_128_SHA]
	TLS ECDH RSA WITH AES 256 GCM SHA384
	TIS ECUM HSA WITH AES 200 UBU ONA
	TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256]
	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA2567
	TLS ECDH RSA WITH AES 128 CBC SHAT
	TLS ECDH ECDSA WITH RC4 128 SHA
	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384]
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384]
	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA_
•	TLS ECDH ECDSA WITH AES 128 GCM SHA2561
•	TIS FODH FODSA WITH AFS 128 OBC SHAPFRT
•	
	TLS_ECDHE_RSA_WITH_RC4_128_SHA_
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256]
	TLS ECDHE RSA WITH AES 256 GCM SHA384
	TIS FORTE RANNIN AFS 356 CRC SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256]
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256]
•	TLS ECDHE RSA WITH AES 128 CBC SHAT
	TIS FCDHE RSA WITH 3DES EDE CBC SHAT
	ILS_ECUME_ECUSA_WITH_CHACHAZU_FULT1305_SHA256 TLS_ECUME_ECDAF_ECDSA_WITH_RCA_128_SHAT
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384]
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 7
	TLS ECDHE ECDSA WITH AES 256 CBC SHAT
•	TIS FOUNE FOUSA WITH AES 128 CBC SHA256
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_
	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHAT
•	TLS_DH_RSA_WITH_CAMELLIA_200_CBC_3HAT
	TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA_
	TLS_DH_RSA_WITH_AES_256_GCM_SHA384_
	TIS DH RSA WITH AES 256 CBC SHAT
	TLS_DH_RSA_WITH_AES_128_GCM_SHA256
	TLS_DH_RSA_WITH_AES_128_CBC_SHA2567
	TLS DH RSA WITH AES 128 CBC SHAT
	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA_
	TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA_
	TLS DH DSS WITH AES 256 GCM SHA384 T
	TIS DH DSS WITH AFS 256 CRC SHA256 T

SHA SHA SHA SHA

S BSA

256 CBC SH 256 GCM SH IA 128 CBC IA 256 CBC

MELL

လလ

R

<

RSA

LS LS

TLS Library Usage

84% of application versions in our dataset use OSdefault libraries with default settings

Why do Apps not use defaults?

- To improve security:
- Some do it wrong:
 - lists that do not have any forward-secret ciphers
- Others use third party libraries instead of the default: Firefox uses NSS, VLC & SoundCloud GnuTLS (some versions)

 Facebook uses OpenSSL and removes weaker cipher suites from the list (e.g. RC4 and 3DES ciphers); it also uses Facebook-specific ALPN • Twitter uses OS-provided libraries with a reordered cipher suite list

Some private messaging and VoIP apps use their own short cipher suite

Weak/outdated primitives

- SSLv3:
- Null and Anonymous ciphers
 - Apps like TuneIn Radio with hundreds of millions of installs
 - Multiple EA games
- Export-grade ciphers:
 - Android 4.0 and below
- Most apps with weak ciphers use poorly-configured OpenSSL

• Supported by any app running on Android 5.0 and below (more than 61% of phones) • EA Games apps (FIFA Mobile, Madden NFL Mobile, etc.) with 100s of millions of installs, even when running on versions of Android that do not support it by default

• Tiffany Alvord Dream World, a children's game that has over one million installs

Solutions?

- De-couple TLS updates from OS updates!
 - TLS should be able to updated independent of the rest of the firmware, making it easier to update without manufacturer/vendor cooperation
 - Google is already doing this with Google Play Services (which bundle their own TLS library and certificate stores), so why not do the same with the **OS-provided TLS library?**
- Give more configuration options to developers
 - This way apps that need extra configuration options (e.g. setting ALPNs) are not forced to use something else

Certificates and Trust

- Android root stores often have "impurities" [Vallina-Rodriguez et al.]
- Some apps do not trust these trust stores and bundle their own CA certificates, pin server certificates, or use self-signed certificates
 - E.g. Firefox (bundles CA cert. store), Uber, Google, Paypal, Facebook (certificate pinning), Yandex (bundles unofficial Yandex) root CA), Samsung apps (self-signed certs.) etc.
 - Implemented poorly, these can open up apps to MITM attacks

- Most apps (98%) trust OS-provided CA stores, and are vulnerable to MITM attacks when those are polluted
- Some apps pin certificates to mitigate the problem of polluted CA stores • It is not very prevalent (less than 2% of apps) • This can be problematic when done poorly: major system recovery app (with root

 - access and ability to flash system firmware, bootloader, recovery, etc.) downloads CA bundle from the cloud in the clear

Outbound connection contents for 47824->52.84.245.50-80(dns:d2to8 GET /truststores/20041/truststore.zip HTTP/1.1 If-Modified-Since: Tue, 21 Mar 2017 15:32:28 GMT+00:00 Connection: close User-Agent: Dalvik/2.1.0 (Linux; U; Android 6.0.1; Nexus 5 Build/M4B30Z) Host: d2to8 .cloudfront.net Accept-Encoding: gzip

What does this all mean?

How do we fix it?

- What do we do with all the polluted CA certificate stores?
 - Google needs to ensure (e.g. through Android's licensing terms) that vendors can not surreptitiously inject their own CA certificates in trust stores
 - CA certificates also need to be able to be updated independently
- But some will still use their own libraries and pin certificates...
 - Make sure developers are properly educated about TLS
 - Detect and prevent poor implementations
 - Google has done something similar in the past: they implemented a tool that prevented developers from uploading apps that used a vulnerable version of GnuTLS and informed them about the issue

How to fix apps with the GnuTLS vulnerability

This information is intended for developers who received a message because they have app(s) utilizing a version of GnuTLS (a communications library implementing SSL, TLS, and DTLS protocols) containing a security vulnerability. These apps violate the Dangerous products provision of the Content Policy and section 4.4 of the Developer Distribution Agreement.

Summary

- First study of TLS usage in Android apps at scale
- Majority of apps (84%) use OS-provided libraries with default settings
- Apps using OS-defaults are vulnerable when the OS is outdated
- Apps using 3rd-party libraries and configurations are prone to misconfiguration and are therefore vulnerable
- Found low use of certificate pinning and CA bundling (less than 2%)
- Provided insights and potential solutions to the problems we found