

The state of Apps

From an eavesdroppers perspective



Agenda

- Who is talking?
- Testing 1000 Dutch Android apps
- Down the rabbit hole
- Video



Who we are

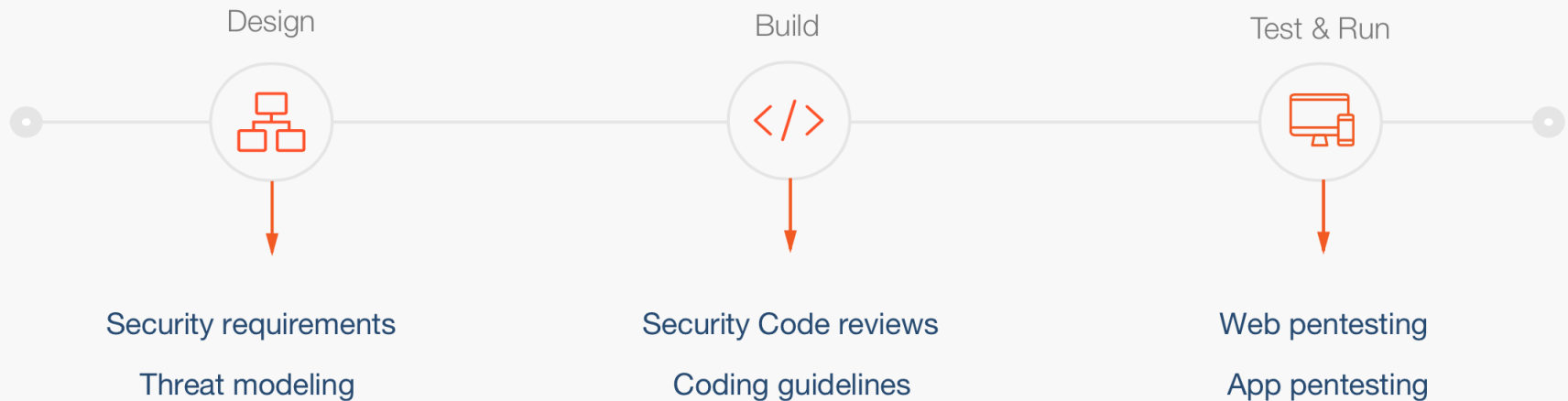
Application Security Testing & Build Security In



Web + Mobile + Desktop + Cloud



What we do

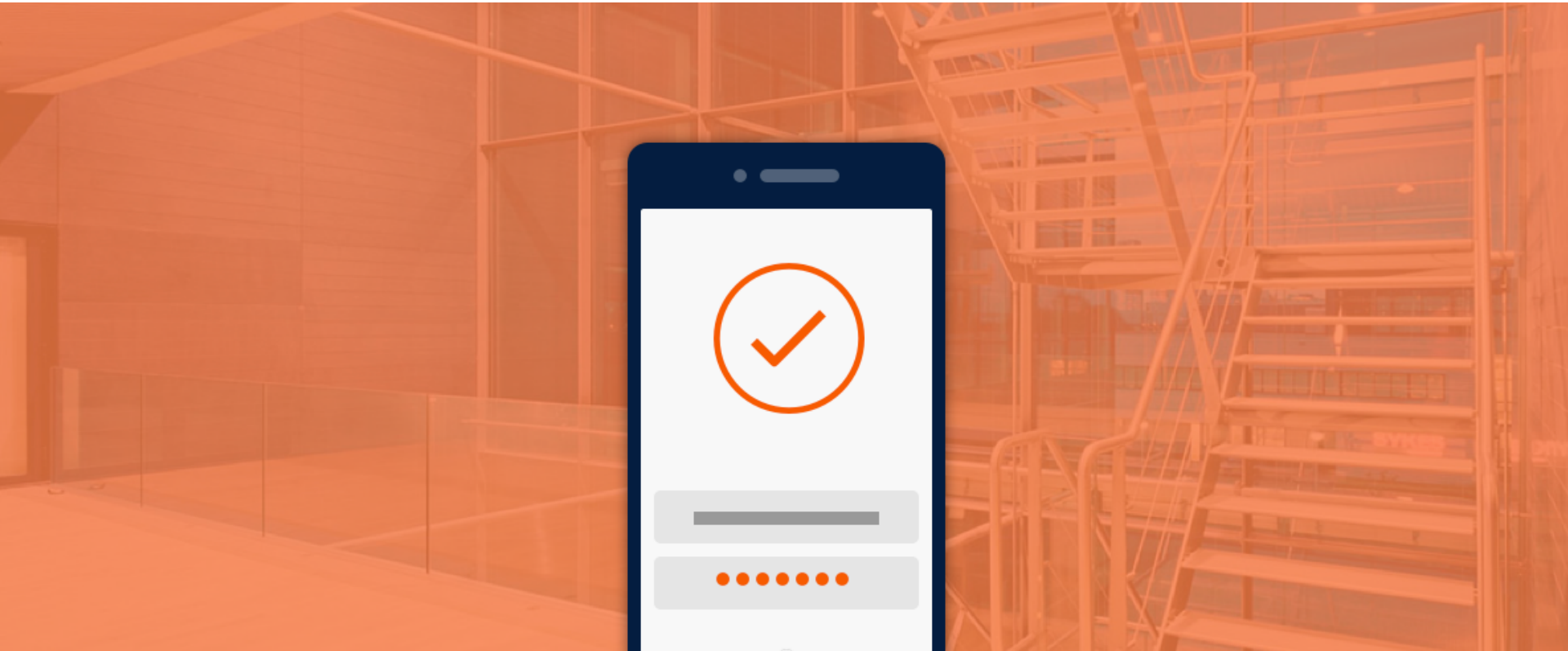


Research time!

Software Ownage.



Testing 1000 Dutch Android Apps on SSL



Research questions

- How to get 1000 apps?
- What is our threat model?
- What is private data?
- How to test so many?



4	air.nl.ako.magazine-2003000.apk
5	air.nl.astfarma.doseringswijzer-2000000.apk
6	air.nl.bison.proefbehang-1000003.apk
7	air.nl.books2download.fgrijk-1000000.apk
8	air.nl.cnv.tools-3004000.apk
9	air.nl.eo.koekelipad-1001000.apk
10	air.nl.freelensing.gotopo_free-3013000.apk
11	air.nl.freelensing.snappingsuarez-1001000.apk
12	air.nl.frontwise.flits-1000005.apk
13	air.nl.genj.questmaster-1005000.apk
14	air.nl.golf4holland.mobile-1002004.apk
15	air.nl.jeew.zelfstandigentarief-1000000.apk
16	air.nl.kennisnet.kennyhd-1001000.apk
17	air.nl.kro.kindertijd.tv-1003008.apk
18	air.nl.kro.rabradio.popduel-1007000.apk
19	air.nl.mediaheads.berneboelmoblie-1000000.apk
20	air.nl.playlikeachampion.telesporttourspe-1000000.apk
21	air.nl.squla.parentdashboard-1000008.apk
22	air.nl.topommonkey.hooghoudenhd-2006000.apk
23	air.nl.vvn.fietsexamen-1000003.apk
24	air.nl.zpress.meidenquizeit-1001000.apk
25	air.nl.zwijzen.spellinginbeeld4li-1000000.apk
26	com.abnamro.nl.markets.turbo-7.apk
27	com.abnamro.nl.mobile.payments-26.apk
28	com.adecco.nl-7.apk
29	com.aitype.android.lang.nl-201.apk
30	com.akzonobel.nl.flexa-6023.apk
31	com.akzonobel.pro.nl.sikkens-5028.apk
32	com.babbel.mobile.android.nl-61.apk
33	com.berniiiiiii.nl-3.apk
34	com.divineaps.nl.miniclub.lite-17.apk
35	com.divineaps.nl.miniclub.only_coloring-17.apk
36	com.divineaps.nl.miniclub.only_math-12.apk
37	com.effacts.cordova-4.apk
38	com.elky.likekids.nlfree-28.apk
39	com.esds.bnb.mobile.nl-2.apk
40	com.frugalflyer.airport.nl-3.apk
41	com.gau.go.launcherex.language.nl-12.apk
42	com.guldencoin.androidwallet.nlg-162.apk

What we did

- Scraping the store.
- Gut feeling approach on private data.
- Scope on public traffic only. (sign-on/in).
- Test with untrusted cert only (self signed).
- Static analysis (has high false-positive rate).
- Generating traffic (trigger events) - work to do.
- Human interaction needed :-)



787	nl.skyradiogroup.skyradio-9.apk
788	nl.skywave.ovinfo-112.apk
789	nl.skywise.kidstimer-12.apk
790	nl.slechedekking-9.apk
791	nl.smartalarm.android-3.apk
792	nl.smartcoupons.knaek-29.apk
793	nl.smeetsis.theoriecursus-16.apk
794	nl.smulweb-8.apk
795	nl.snabor.android.feestdagen-6.apk
796	nl.snabor.android.klaverjas-3.apk
797	nl.sneeuwhoogte.android-31.apk
798	nl.snsbank.snsbankieren-22.apk
799	nl.snsbank.snsheip-2.apk
800	nl.wk2014.onsoranje-3.apk
801	nl.wligtenberg.gvs-1.apk
802	nl.wligtenberg.kkscanner-3.apk
803	nl.wligtenberg.tpw-5.apk
804	nl.wowdeal.android-4.apk
805	nl.wowwww.hallmark.kpp.android-1110199073
806	nl.wpg.mobile.app.hoi-3.apk
807	nl.wtf-109.apk
808	nl.wur.aid-18.apk
809	nl.x_ip.odij-7.apk
810	nl.x_services.kaartsaldo-716.apk
811	nl.xite.messenger-4.apk
812	nl.xmade.slotmachinealieninvasion-1.apk
813	nl.xmade.slotmachinediamondsrubies-1.apk
814	nl.yellowbytes.zwemwaterapp-4.apk
815	nl.yestelecom.app-5.apk
816	nl.yipyp.kkjp.android-20000.apk
817	nl.zeemeijer.fourpicsoneword-5.apk
818	nl.zeemeijer.wordsearch-7.apk
819	nl.zerok.ictu-7.apk
820	nl.ziggo.android.tv-50.apk
821	nl.ziggo.android.usage-1.apk
822	nl.ziggo.muziek-101.apk
823	nl.ziggo.voip-59.apk
824	nl.ziggo.vvm-30.apk
825	nl.zomoto-102.apk
826	nl.zonneveld.pldkal_free-10.apk

MiTM Set-up

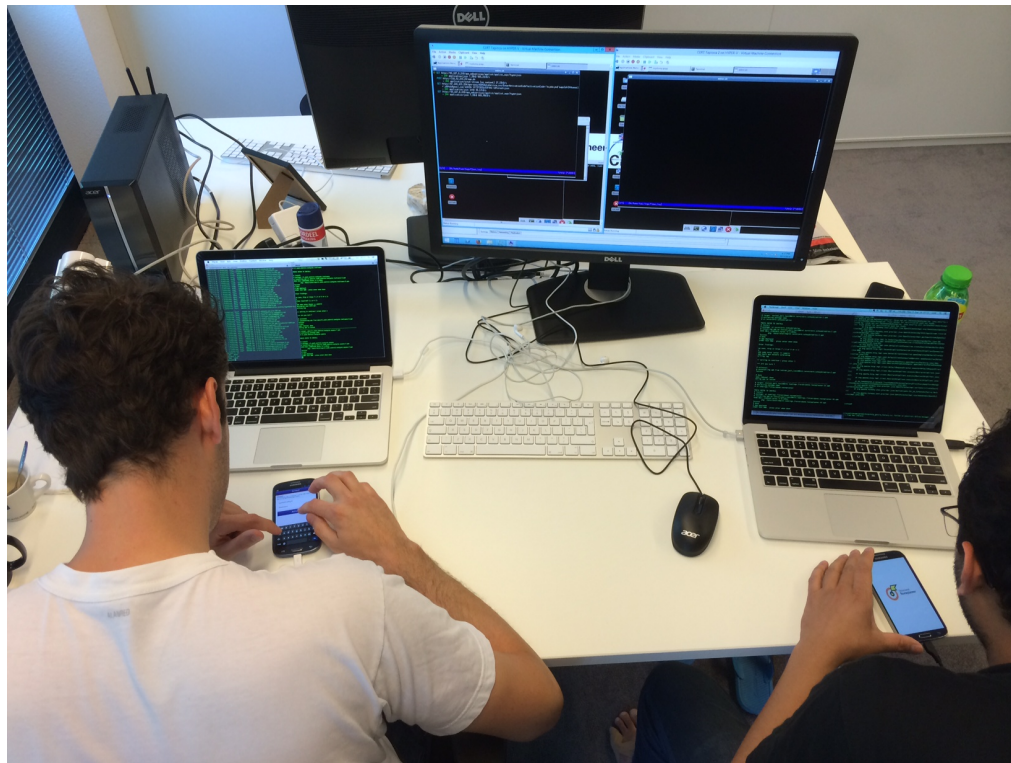
1. Run DHCP server, with gateway set to the IP of the AP;
2. Run intercepting proxy for MiTM; e.g. mitmproxy;
3. Forward TCP connections (80 & 443) through proxy;
4. NAT other connections;
5. Run Wireshark to inspect non-HTTP(s) connections.



951 nl.visplanner-8.apk
952 nl.visualnovels.sleeplessnight-100.apk
953 nl.vlsolutions.buienl-14.apk
954 nl.voa.android.oplaadpunten-2.apk
955 nl.vodafone.thuistv-3.apk
956 nl.vodafone.vinson-1.apk
957 nl.voedingscentrum.balansdag-3.apk
958 nl.voedingscentrum.eetmeter-11.apk
959 nl.voedingscentrum.slimkoken-21.apk
960 nl.vogelbescherming.wadvogels-3.apk
961 nl.volkerinfradesign.check-52.apk
962 nl.volkerinfradesign.wave-56.apk
963 nl.volleyball.competition.app-6.apk
964 nl.vpro.drievoortwaalf.luisterpaal-27.apk
965 nl.vrouw-1.apk
966 nl.vv.fietsknoop-26.apk
967 nl.vvdboogaard.zonsondergang-1.apk
968 nl.vvv.vvvapp-13.apk
969 nl.wadden.terrschelling-10.apk
970 nl.wadden.texel-9.apk
971 nl.walibi.corporate-7.apk
972 nl.walibi.corporate2-7.apk
973 nl.walibi.corporate6-8.apk
974 nl.wandelzoekpagina.wandelzapp-2.apk
975 nl.wartel.vangsten-27.apk
976 nl.wasco.wascomobile-4.apk
977 nl.webiq.wadwaaler-1.apk
978 nl.webs.hemophilia-101.apk
979 nl.weeaboo.android.cce-2.apk
980 nl.weerplaza.app-28.apk
981 nl.weerplaza.cast-1.apk
982 nl.weirdbear.brickswizardacademy-6.apk
983 nl.wel.welappje-40.apk
984 nl.west.spoorzoeker-2013061202.apk
985 nl.westerschedetunnel.wst-11.apk
986 nl.widgets.albertheijn.smartphone-15.apk
987 nl.widgets.hiprepay-3.apk
988 nl.widgets.jt-13.apk
989 nl.widgets.kpnprepaid-3.apk
990 nl.widgets.ondertussen-2.apk
991 nl.widgets.relievemobile-2.apk
992 nl.wiebbe.treintijden-65.apk
993 nl.wiebetaaltwat.webapp-4.apk
994 nl.wielerflits-2.apk
995 nl.wieringsoftware.argus-2.apk
996 nl.wikit.factuurmaken-4.apk
997 nl.windcentrale.android-7.apk

Steps

1. Static analysis (automated)
2. Install app (automated)
3. Launch app
4. Generate traffic
5. Inspect traffic
6. Uninstall (automated)



| It took us 3 months... (spare time)



**KEEP
CALM
AND
CARRY
ON**



What did we see?

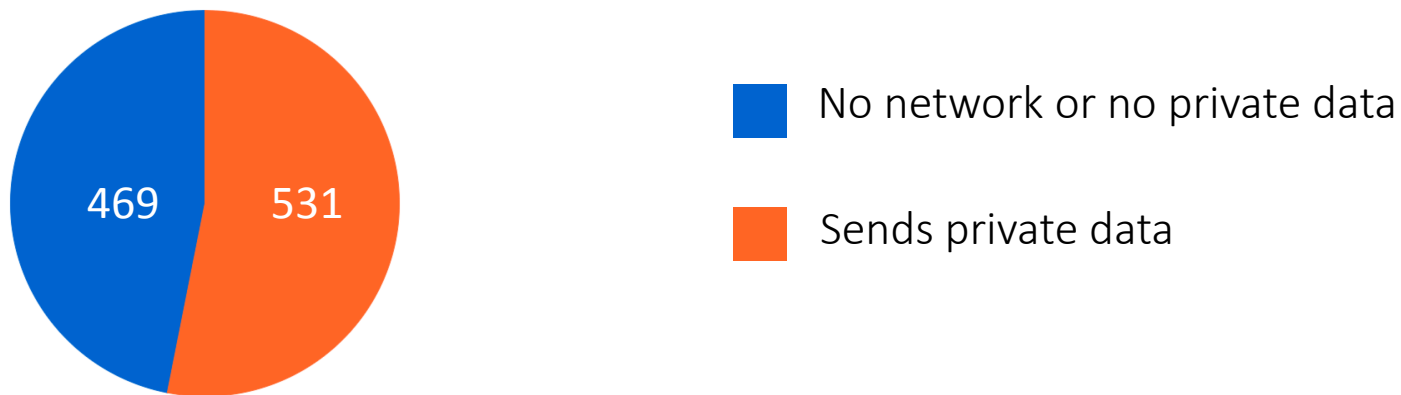
.. name, address, date of birth, e-mail, phone, username, password, secrets, insurance policy number, bank account, creditcard, pictures, medicine prescriptions, diary, BSN, political preference, FB credentials, appointments, tickets ..

```
%3A%3A=bs&Geboortedatum%3A%3A=09-09-2008&Straat+en+huisnummer%3A%3A=jhhd&Postcode%3A%3A=1223jk&Woonplaats%3A%3A=jjhjd&Telefoonnummer+vast%3A%3A=0677888765&Telefoonnummer+mobiel%3A%3A=&E-mail+adres%3A%3A=h%40hj.nl&Zorgverzekeraar%3A%3A=jjjd&Polisnummer%3A%3A=77772&Burgerservicenummer%3A%3A=7777882&%3Alb=%3Alb=&Gegevens+betreffende+de+bevalling%3Alb=%3Alb=&Uitgerekende+datum%3A%3A=2014-21-11&Hoeveelste+zwangerschap%3A%3A=6&Hoeveelste+bevalling%3A%3A=1&Aantal+verwachte+kindern%3A%3A=1&Plaats+bevalling%3A=Thuis&%3Alb=&Gegevens+huidige+gezinssamenstelling%3Alb=%3Alb=&Aantal+volwassenen%3A%3A=5&Aantal+kinderen+van+0+tot+4+jr%3A%3A=5&Aantal+kinderen+van+4+tot+6+jr%3A%3A=5&Aantal+kinderen+van+6+jaar+of+ouder%3A%3A=5&%3Alb=%3Alb=&Gegevens+betreffende+de+kraamtijd%3Alb=%3Alb=&Gewenste+thuiskraamzorg%3A%3A=Basis+zorgpakket+++%2F-+6uu
```



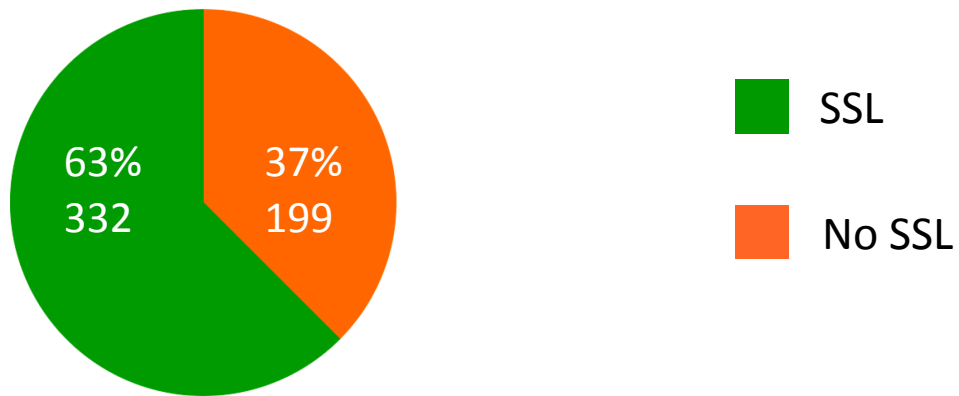
Results

We started with 1000 apps



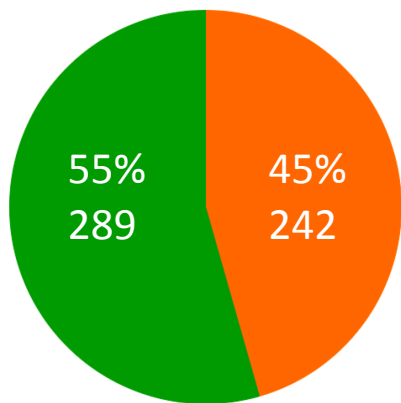
Results

We continue with 531.



Results

We continue with 531.



■ SSL

■ No SSL + broken SSL (unknown CA)



Result

45% of apps dealing with private data
does not protect you against MiTM!



What happened next?



NOS

De Telegraaf



Het PAROOL

nrc.next

Do we care?

45 organisations contacted us for details....

We stopped chasing...



AppVer - Beta - Sneak Preview



Android Security Scan

Verifieer de veiligheid van uw Android applicatie
een account is noodzakelijk.

SCAN NU

LOGIN



Down the rabbit hole



Common flaws Android apps

- Insecure SSL/TLS (or worse no SSL)
- Insecure Javascript interface

These two issues combined allows for remote compromise of your data - for example via a public WiFi hotspot



Insecure SSL/TLS

- SSL/TLS provides integrity, confidentiality & authentication
- Default SSL implementation provides security similar to web browsers
- Various ways to screw this up, including:
 - Insecure Trust Manager
 - Insecure Host Name Verifier
 - Insecure SSL Error Handler (WebView)
 - Mixed content (WebView)

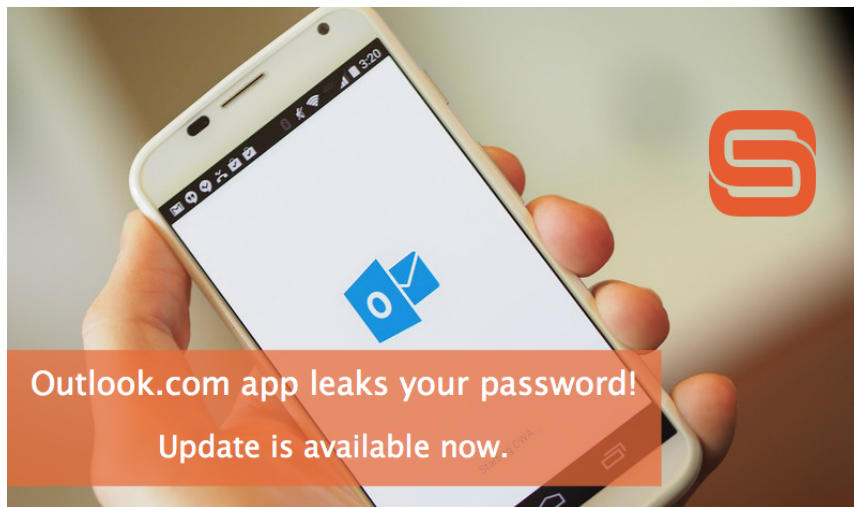


Insecure Trust Manager - example

```
public class InsecureX509TrustManager implements X509TrustManager {  
  
    @Override  
    public void checkClientTrusted(X509Certificate[] x509Certificates, String s)  
        throws CertificateException {  
    }  
  
    @Override  
    public void checkServerTrusted(X509Certificate[] x509Certificates, String s)  
        throws CertificateException {  
    }  
  
    @Override  
    public X509Certificate[] getAcceptedIssuers() {  
        return null;  
    }  
  
}
```



Outlook.com for Android - Insecure SSL



Updated July 28, 2014	Size 9.4M	Installs 10,000,000 - 50,000,000	Current Version 7.8.2.12.49.7564	Requires Android 2.2 and up
Content Rating Everyone	Permissions View details	Report Flag as inappropriate	Offered By Outlook.com	Developer Visit Website



Javascript interface (bridge)

- Used in combination with WebViews
- Allows Javascript to call Java methods
- The interface can be any Object
- The Object's public methods are exposed (with some limitations)

```
public void addJavascriptInterface (Object object, String name)
```



Javascript interface - example

```
class JsObject {  
    public String toString() { return "injectedObject"; }  
}
```

```
webView.addJavascriptInterface(new JsObject(),  
    "injectedObject");  
webView.loadData("", "text/html", null);  
webView.loadUrl(  
    "javascript:alert(injectedObject.toString())");
```



Javascript interface - the flaw

- On Android < API lvl 17 (4.2) ANY public method can be invoked
- Including Reflection API exposed through Object (!)
- *Object.getClass()*

```
var javaObj = interfaceName;
var storagePath = "/data/data/nl.app.name";
var storageFile = "/test.txt";

function execute(cmdArgs) {
    return javaObj.getClass().forName("java.lang.Runtime")
        .getMethod("getRuntime",null).invoke(null,null).exec(cmdArgs);
}

// Copy sdcard filelist to file
execute(["/system/bin/sh","-c","ls -al /mnt/sdcard/ > "+storagePath+storageFile]);
```



Viber - Insecure SSL + Javascript interface



Updated November 20, 2014	Size 32M	Installs 100,000,000 - 500,000,000	Current Version 5.1.1.42	Requires Android 2.3 and up
Content Rating Medium Maturity	In-app Products \$0.99 - \$35.17 per item	Permissions View details	Report Flag as inappropriate	Offered By Viber Media S.à r.l.



How about iOS?

Critical SSL Vulnerability Leaves 25,000 iOS Apps

Vulnerable to Hackers

Saturday, April 25, 2015 Mohit Kumar

8+1 119 Like 743 Share 190 Tweet 156 in Share 21 ShareThis 443



A critical vulnerability resides in **AFNetworking** could allow an attacker to cripple the HTTPS protection of 25,000 iOS apps available in Apple's App Store via *man-in-the-middle (MITM)* attacks.

Thousands of iOS apps left open to snooping thanks to SSL bug

Summary: iOS developers are being urged to update their apps to use the latest version of a library that fixes a security flaw that leaves their apps exposed to man-in-the-middle attacks.



By Liam Tung | April 27, 2015 -- 09:17 GMT (10:17 BST)

Follow @LiamT 2,765 followers

Get the ZDNet Announce UK newsletter now

Comments 22

Share on Facebook 248

Tweet 190

in Share 71

more +

Researchers have uncovered around 25,000 iOS apps that use old versions of a popular networking library, leaving them open to attackers on the same network viewing encrypted traffic.

The bug affects Secure Sockets Layer (SSL) code in AFNetworking, a networking library developers can use to build components of iOS apps. The framework has been updated three times in the past six weeks, addressing numerous SSL flaws that leave apps vulnerable to man-in-the-middle attacks.

The latest version of AFNetworking, 2.5.3, fixes a weakness in the library's domain name validation process. SourceDNA, the security firm that discovered the recurrent flaw, [said on Friday](#) that at least 25,000 apps are still running an outdated version.

"If you are using AFNetworking (any version), you must upgrade to 2.5.3," SourceDNA said. "Also, you should enable public key or certificate-based pinning as an extra defense. Neither of these game-over SSL bugs affected apps using pinning."

Explaining the bug, SourceDNA added: "Domain name validation could be enabled by the `validatesDomainName` flag, but it was off by default. It was only enabled when certificate pinning was turned on, something too few developers are using."

The net result for end users is that an attacker on the same wi-fi network could fairly easily view data in transit, which should otherwise have been encrypted. "Because the domain name wasn't checked, all they needed was a valid SSL certificate for any web server, something you can buy for \$50," Source DNA said.

Read this



iOS vs Android: Which is more of a security threat for the enterprise?

→ Read More



We find these bugs in iOS as well!

Burp Suite Professional v1.6.14 - iOS

Target Proxy Spider Scanner Intruder Repeater Sequencer

Intercept HTTP history WebSockets history Options

Filter: Showing all items

Host	Method	URL
https://public-api.wordpress.com	POST	/oauth2/token
https://public-api.wordpress.com	POST	/oauth2/token

Request Response

Raw Params Headers Hex

POST /oauth2/token HTTP/1.1
Host: public-api.wordpress.com
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Proxy-Connection: keep-alive
Accept: application/json
User-Agent: WordPress/4.9 (iPhone iOS 8.3 Scale/2.00)
Accept-Language: nl q=1, en q=0.9, tr q=0.8
Accept-Encoding: gzip, deflate
Content-Length: 159

client_id=11&client_secret=zf66wMF1z05NohvOLsFYGVm2YbxwVFEVv1XXODcVvzK73JDOPPhrvCuoln0U19o&grant_type=password&password=Welkom12321&username=ssl40ishard.com

ssl@ishard.com

.....

Inloggen

Wachtwoord vergeten?

Burp Suite Professional v1.6.14 - iOS

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender

Intercept HTTP history WebSockets history Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited
44	https://awunderlist.com	POST	/api/v1/authenticate		

Request Response

Raw Params Headers Hex

POST /api/v1/authenticate HTTP/1.1
Host: a.wunderlist.com
Connection: keep-alive
Accept: application/json
x-client-product-version: 3.2.0
Proxy-Connection: keep-alive
x-client-system-version: 10.10.2
x-client-device-id: 18B56995-CE97-4A91-8364-20E3A65F96D6
Accept-Language: en-us
x-client-platform: Mac
Accept-Encoding: gzip, deflate
Content-Type: application/json
x-client-system: MacBookPro10,2
x-client-product-git-hash: 355bc7b6c1db9d5634799ef056ce708dfa787b9
x-client-id: 5541b1d86e925e2dd7e5
x-client-request-id: 58C74C1C-D824-4235-BF8C-98188B702620
Content-Length: 51
x-client-instance-id: D672C3D0-6FAF-4ACC-9DD2-7B6781D01FBA
User-Agent: Wunderlist/17 CFNetwork/720.2.4 Darwin/14.1.0 (x86_64)
x-client-product: Wunderlist

{'email': 'asdfsad@asdlkj.com', 'password': 'asdfsad'}

asdfsad@asdlkj.com

.....

Sign In

Forgot your password?

Facebook Google

Back



We find these bugs in iOS as well!

Intercept HTTP history WebSockets history Options

Filter: Showing all items

#	Host	Method	URL
11	https://yamalytics-receiver....	POST	/api/ioslogger/prod
12	https://www.yammer.com	POST	/oauth2/access_token

Request Response

Raw Params Headers Hex

POST /oauth2/access_token HTTP/1.1
Host: www.yammer.com
yammer-capabilities: external-messaging
Proxy-Connection: keep-alive
Content-Type: application/json
Accept: application/json
Content-Length: 194
Accept-Language: nl;q=1, en;q=0.9, tr;q=0.8
Accept-Encoding: gzip, deflate
Connection: keep-alive
User-Agent: Yammer/6.4.25.850 iPhone4,1; iPhone OS 8

{ "password": "hahajsj", "username": "hsshsh@siksks.com", "nts": 1, "client_secret": "lm3il4pIKiCe5Ye8ReQV8mkeQis tIXDMTej7MsA" }

hsshsh@siksks.com

password

Intercept HTTP history WebSockets history Options

Filter: Showing all items

Host	Method	URL	Params	Edited	Status	Len
http://portal.afrogaleap.com	GET	/api/get.versionsupport?token=Ezf...			200	510
https://api.pinterest.com	POST	/v3/login?client_id=1431594&time...			401	599

Request Response

Raw Params Headers Hex

POST /v3/login?client_id=1431594×tamp=1428260294&oauth_signature=5323e92357E76d7a3411ae089e63e24a37 HTTP/1.1
Host: api.pinterest.com
User-Agent: Pinterest for iOS/4.5 (iPhone; 8.1.2)
Accept-Language: nl
X-Pinterest-InstalId: 8bee58e3329347589375ae3fe33314bc
Cache-Control: no-cache, no-store
X-Pinterest-AppState: active
X-Pixel-attribution: 2
Accept: application/json
Content-Type: application/x-www-form-urlencoded
X-Pinterest-Device: iPhone4,1
Connection: keep-alive
Proxy-Connection: keep-alive
Content-Length: 107
Accept-Encoding: gzip, deflate

client_id=1431594&first_login=&password=nananan×tamp=1428260294&username_or_email=snnanana40snsjs.com

Sim vengrendeld 20:58 100%

Log in

Log in met Facebook

Twitter Google

OR

snnanana@snsjs.com

Log in

Pinterest

Security Summary for Yammer by Microsoft

Want full details on these apps?

[Get Free Report!](#)

2

Vulnerable Apps

2

Apps Use AFNetworking

High Priority Affected Apps

1. [Yammer](#)

- **Version:** 6.4.24
- **Version:** 6.4.27

Libraries: AFNetworking v2.5.1

Libraries: AFNetworking v2.5.2

SSL Vulnerable

SSL Vulnerable

2. [Yammer Now](#)

- **Version:** 1.0.45

Libraries: AFNetworking v2.x

SSL Vulnerable

Concluding

- Lots of apps not protected against eavesdropping
- All platforms affected
- Root cause varies
 - Debugging/testing
 - Vulnerabilities in libraries
 - Implementation errors
- Basic check is not hard to do!
 - Include in automated tests
 - Test release builds



Thank you!

Questions?

info@securify.nl

@securifybv

