

# The state of Apps

## From an eavesdroppers perspective



OWASP

Security

# Agenda

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



# Who we are

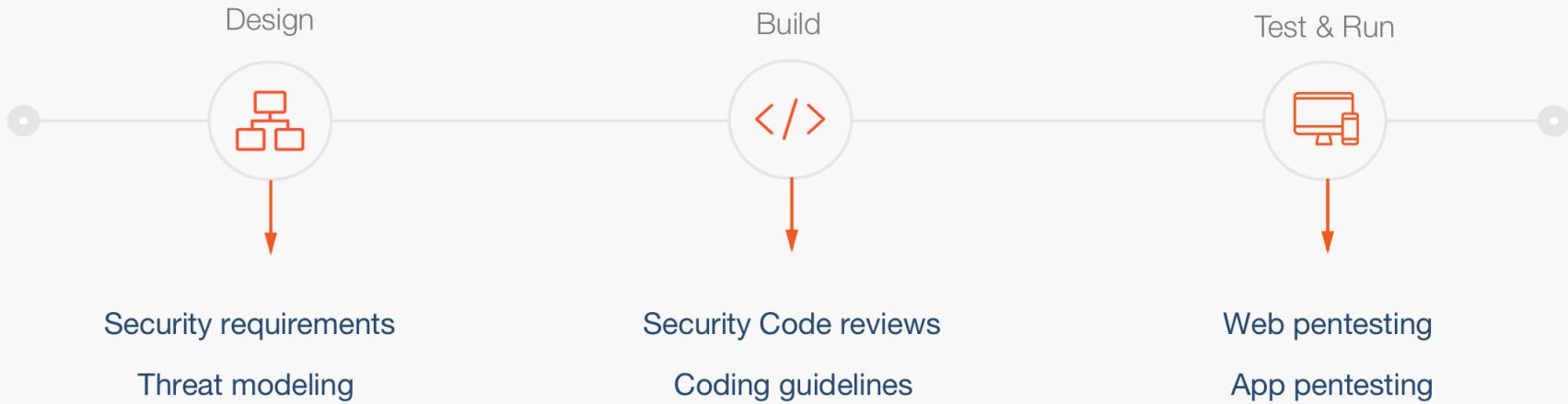
Application Security Testing & Build Security In



Web + Mobile + Desktop + Cloud

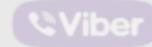


# What we do

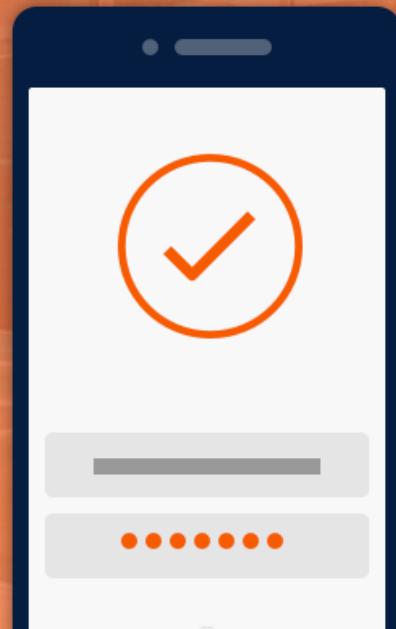


# Research time!

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.akomagazine-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.koekeipad-1001000.apk  
10 air.nl.freelensing.gotopo\_free-3013000.apk  
11 air.nl.freelensing.snapplingsuarez-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.berneboelmobile-1000000.apk  
20 air.nl.playlikeachampion.telesporttourspeel-1000000.apk  
21 air.nl.squila.parentdashboard-1000008.apk  
22 air.nl.topomonkey.hooghoudenhd-2006000.apk  
23 air.nl.vvn.fietsexamen-1000003.apk  
24 air.nl.zpress.meidenquizit-1001000.apk  
25 air.nl.zwijsen.spellinginbeeld4li-1000000.apk  
26 com.abnambro.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.bernillillii.nl-3.apk  
34 com.divineaps.nl.miniclub.lite-17.apk  
35 com.divineaps.nl.miniclub.only\_coloring-12.apk  
36 com.divineaps.nl.miniclub.only\_math-12.apk  
37 com.effects.cordova-4.apk  
38 com.elky.likekids.bnffree-28.apk  
39 com.esds.bnbn.mobile.nl-2.apk  
40 com.frugalflyer.airport.nl-3.apk  
41 com.gau.go.launcherex.language.nl-12.apk  
42 com.guldencoin.androidwallet.nl-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.slechtedekking-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.snshelp-2.apk                      |
| 800 | nl.wk2014.onsonanje-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.apk |
| 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.yipyip.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

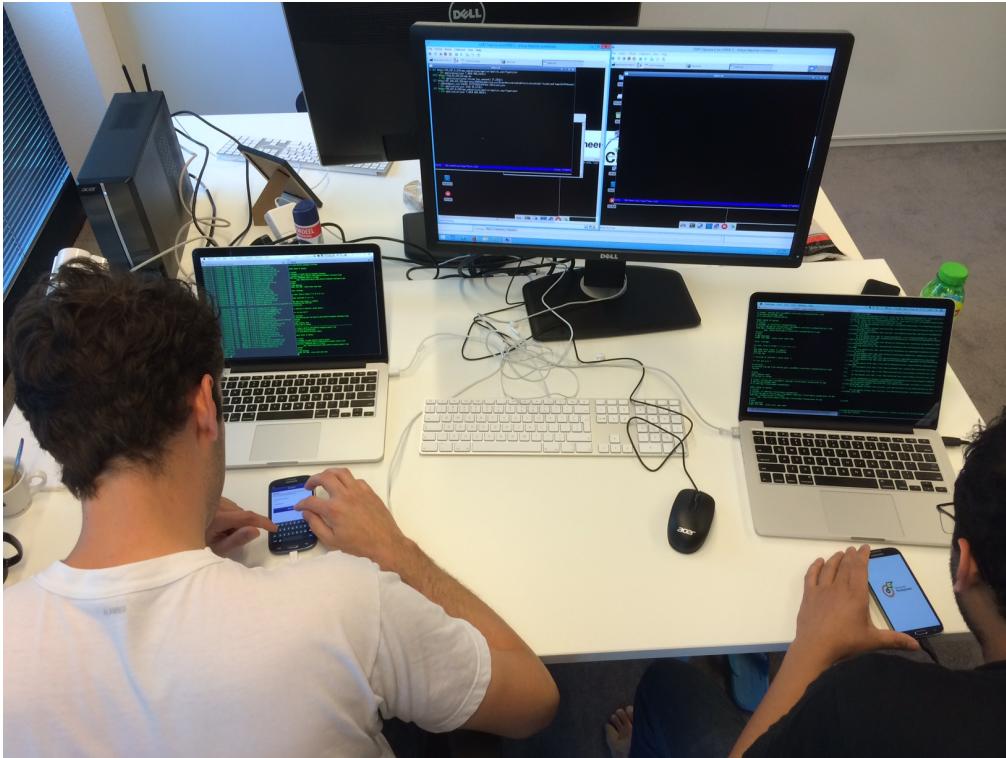
1. Run DHCP server, with gateway set to the IP of the AP;
2. Run intercepting proxy for MiTM; e.g. mitmproxy;
3. Forward TCP connections (80 & 443) through proxy;
4. NAT other connections;
5. Run Wireshark to inspect non-HTTP(s) connections.



951 nl.vispijanner-8.apk  
952 nl.visualnovels.sleeplessnight-100.apk  
953 nl.vlsolutions.buien-14.apk  
954 nl.voa.android.oplaadpunten-2.apk  
955 nl.vodafone.thuistv-3.apk  
956 nl.vodafone.net.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.drievoorwaalf.luisterpaal-27.apk  
965 nl.vrouw-1.apk  
966 nl.vv.fietsknop-26.apk  
967 nl.vvdboogaard.zonsondergang-1.apk  
968 nl.www.vvvapp-13.apk  
969 nl.wadden.terschelling-10.apk  
970 nl.wadden.texel-9.apk  
971 nl.walibi.corporate-7.apk  
972 nl.walibi.corporate-2-7.apk  
973 nl.walibi.corporate-6-8.apk  
974 nl.wandelzoekpagina.wandelzapp-2.apk  
975 nl.wartel.vangsten-27.apk  
976 nl.wasco.wascomobile-4.apk  
977 nl.webiq.wadwaaier-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.weirdbeard.brickswizardacademy-6.apk  
983 nl.wel.welappje-40.apk  
984 nl.west.spoorzoeker-2013061202.apk  
985 nl.westerscheldetunnel.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.wielerrflits-2.apk  
995 nl.wieringssoftware.argus-2.apk  
996 nl.wikit.factuurmakken-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?

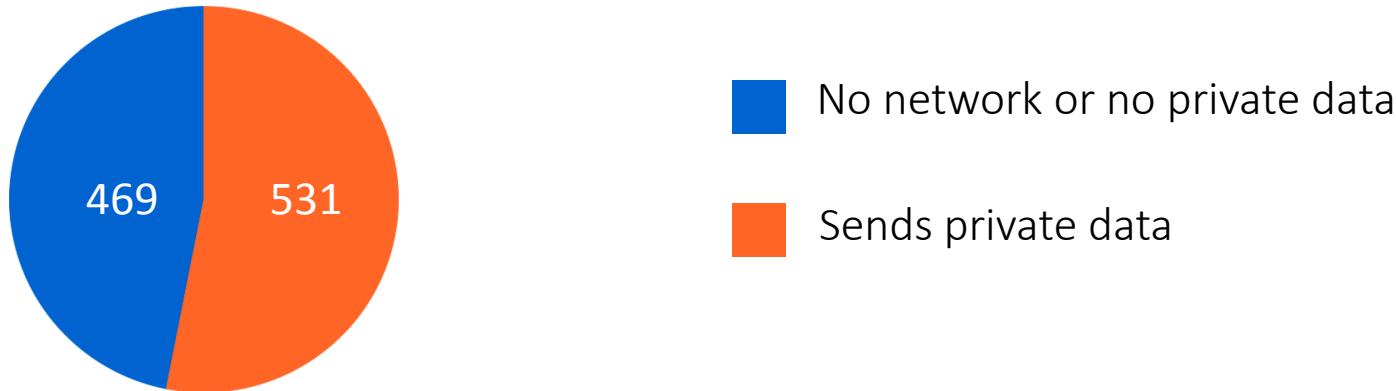
.. name, address, date of birth, e-mail, phone, username, password, secrets, insurance policy number, bank account, creditcard, pictures, medicine prescriptions, diary, BSN, political preference, FB credentials, appointments, tickets ..

%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+kinderen%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



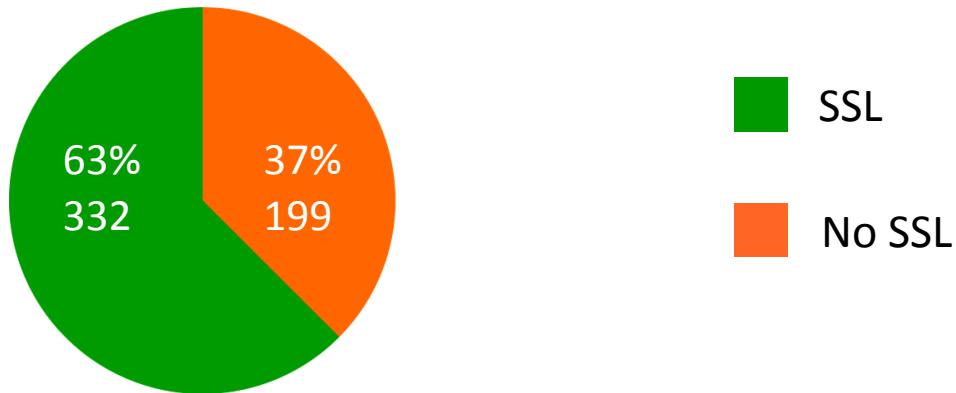
# Results

We started with 1000 apps



# Results

We continue with 531.



# Results

We continue with 531.



# Result

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



# What happened next?



NOS

De Telegraaf



Browser Windows 10 heet Microsoft Edge

Microsoft wil apps overzetten naar...

'Apple benadert meer BBC-mensen'

Omstreden app Secret stopt er mee

Waze deelt verkeersinfo via Twitter

Time Warner-baas verwacht tv-dienst...

'Krakkemikkie' motortje voor horloges...

Salesforce 16% hoger op overnemergerucht

Apple vreest miljardenboete

Chrome-extensie beschermt tegen phishing

Vliegtuigen aan de grond door

Foto: Rechtnvrije

WhatsApp Messenger Facebook Pet Rescue Sack Despicable Me NU.nl Skype - free (S)

Deel op FB 445 Tweet 141 G+ 1

zo 23 nov 2014, 18:40

## 'Honderden Nederlandse apps onveilig'

AMSTERDAM - Honderden Nederlandse apps voor Android zijn niet veilig. Ze versturen persoonlijke informatie van gebruikers zonder beveiling, waardoor data kunnen worden onderschept. Dat blijkt uit een test van beveiligingsbedrijf Security, meldt de NOS zondagavond.

Security bestudeerde 1000 willekeurige gratis Android-apps, die in de Google Play store te vinden zijn. De onderzoekers onderschepten BSN-nummers, e-mailadressen, telefoonnummers, persoonlijke gegevens, wachtwoorden, bankrekeningnummers, foto's en dagboeken.

Volgens Security gaat het onder meer om apps voor reizen, financiën, chatten en daten. Het bedrijf wil niet zeggen om welke apps het gaat.

Security heeft niet gekeken naar apps voor iPhones en iPads, maar verwacht daar dezelfde problemen.

Deel op FB 445 Tweet 141 G+ 1

Het PAROOL

nrc.next

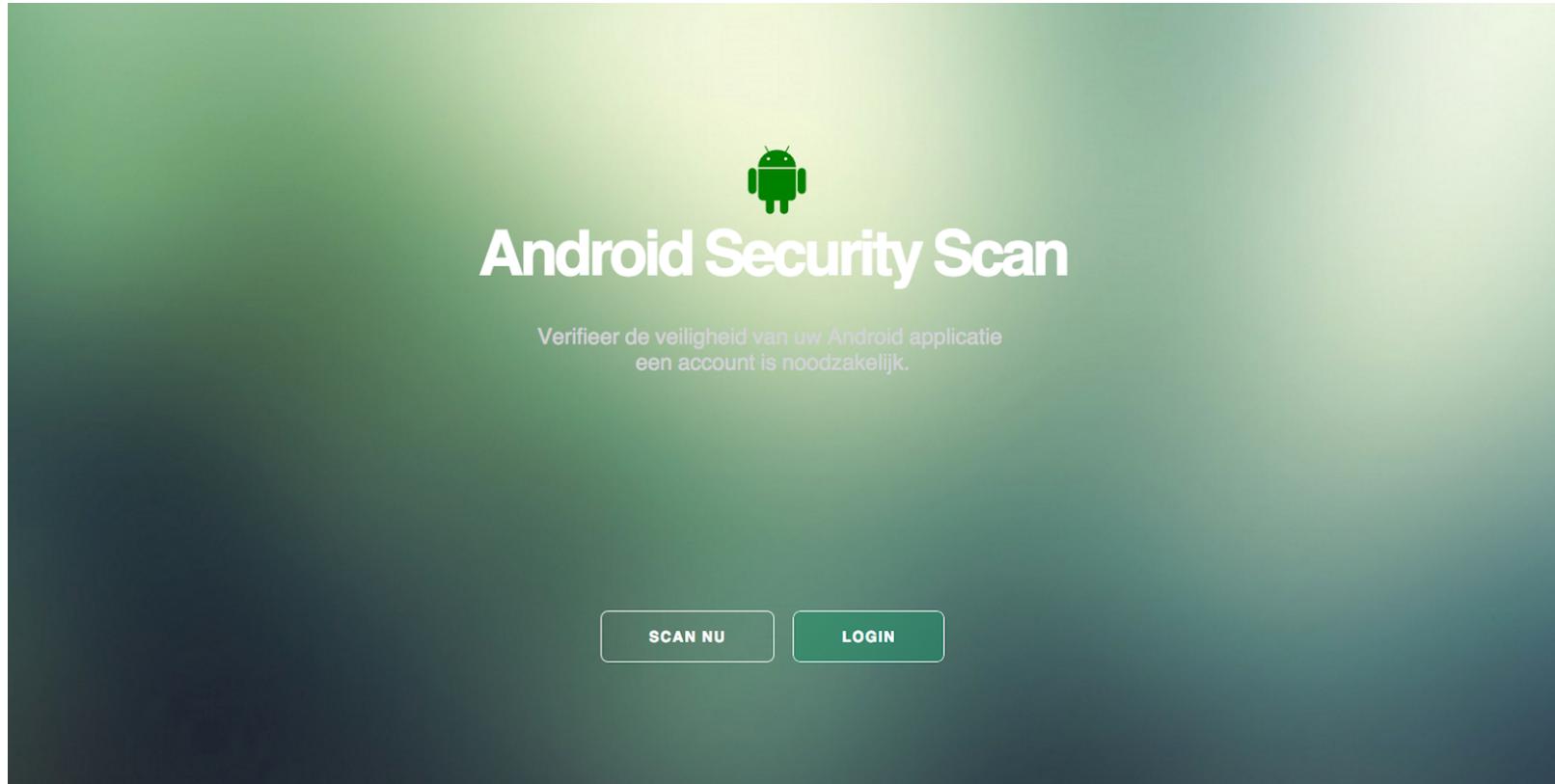
Do we care?

45 organisations contacted us for details....

We stopped chasing...



# AppVer - Beta - Sneak Preview

A large, dark green placeholder image representing the Android Security Scan application's user interface. It features a central white area containing the app's logo and text.



## 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)

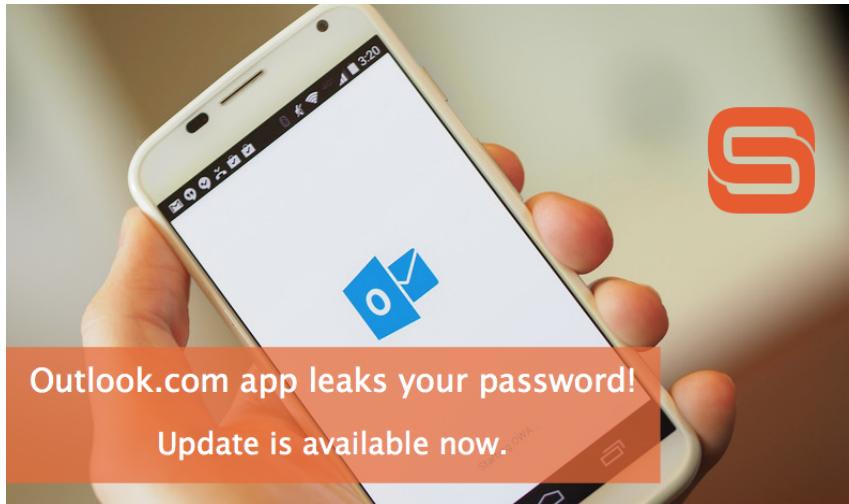


# Insecure Trust Manager - example

```
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<br>July 28, 2014   | Size<br>9.4M                                | Installs<br>10,000,000 - 50,000,000                             | Current Version<br>7.8.2.12.49.7564 | Requires Android<br>2.2 and up             |
| Content Rating<br>Everyone | Permissions<br><a href="#">View details</a> | <a href="#">Report</a><br><a href="#">Flag as inappropriate</a> | Offered By<br>Outlook.com           | Developer<br><a href="#">Visit Website</a> |



# 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



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



# How about iOS?

## Critical SSL Vulnerability Leaves 25,000 iOS Apps

### Vulnerable to Hackers

Saturday, April 25, 2015 by Mohit Kumar

[g+1](#) 119 [Like](#) 743 [Share](#) 190 [Tweet](#) 156 [in Share](#) 21 [ShareThis](#) 443



## AFNetworking SSL Bug

### 25,000 iOS Apps Vulnerable to Hackers

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 validateDomainName 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!

The screenshot shows the Burp Suite interface. On the left, the Network tab displays two POST requests to `/oauth2/token`. The first request is from `https://public-api.wordpress.com` and the second is from `https://public-api.wordpress.com`. The Request tab shows the raw POST data for the second request:

```
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=zf66wMPizUBNohv0LsfYGvM2YbxwgVEVviXXODcVwzK73JDOPPUhrvCuoln0U19o&
grant_type=password&password=Welkom123%21&username=ssl%40ishard.com
```

The screenshot shows the Burp Suite interface. On the left, the Network tab displays a POST request to `/api/v1/authenticate` from `https://a.wunderlist.com`. The Request tab shows the raw POST data:

```
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-C997-4A91-8364-20E3A65F96D6
Accept-Language: en-us
x-client-locale: en-us
Accept-Encoding: gzip, deflate
Content-Type: application/json
x-client-system: MacBookPro10,2
x-client-product-git-hash: 355bc7b6c1db9d5634799ef056ce7087dfa787b9
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": "asdfasd@asdlkj.com", "password": "asdfads"}
```



# We find these bugs in iOS as well!

Charles Proxy screenshot showing a POST request to `https://www.yammer.com/oauth2/access_token`. The request body is a JSON object:

```
{"password": "hahajsj", "username": "hsshns@sikksks.com", "nts": "1", "client secret": "Lm3il4pJKicCe5Ye8PcQfV6cmhQf8tIXDMTej7MSA"}
```



hsshan@sikksks.com  
•••••  
Aanmelden

Heb je geen account?  
Registreren

Charles Proxy screenshot showing a POST request to `https://api.pinterest.com/v3/login/?client_id=1431594&timestamp=1428260294&username_or_email=snnana@snsjs.com`. The request body is a JSON object:

```
{ "client_id": "1431594", "first_login": "1", "password": "nanana", "timestamp": "1428260294", "username_or_email": "snnana@snsjs.com" }
```



# 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](mailto:info@securify.nl)

[@securifybv](https://twitter.com/securifybv)

