The state op Apps
From an eavesdroppers perspective

OWASP

Securify

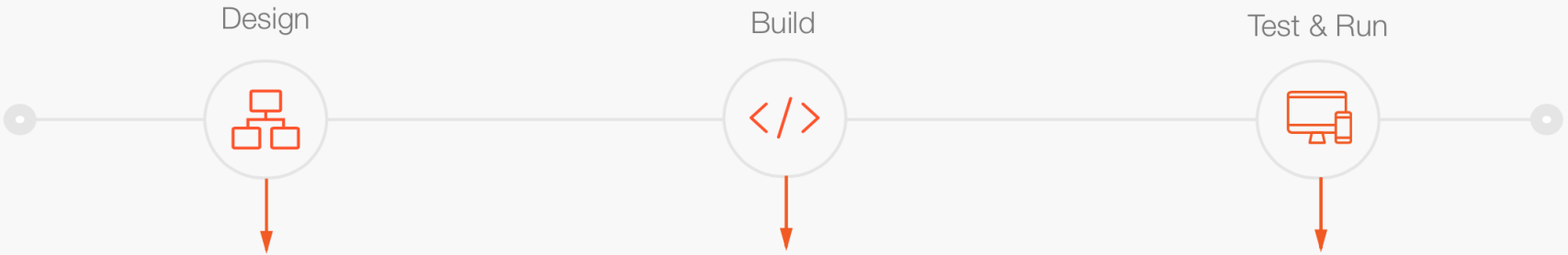
Agenda

- 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

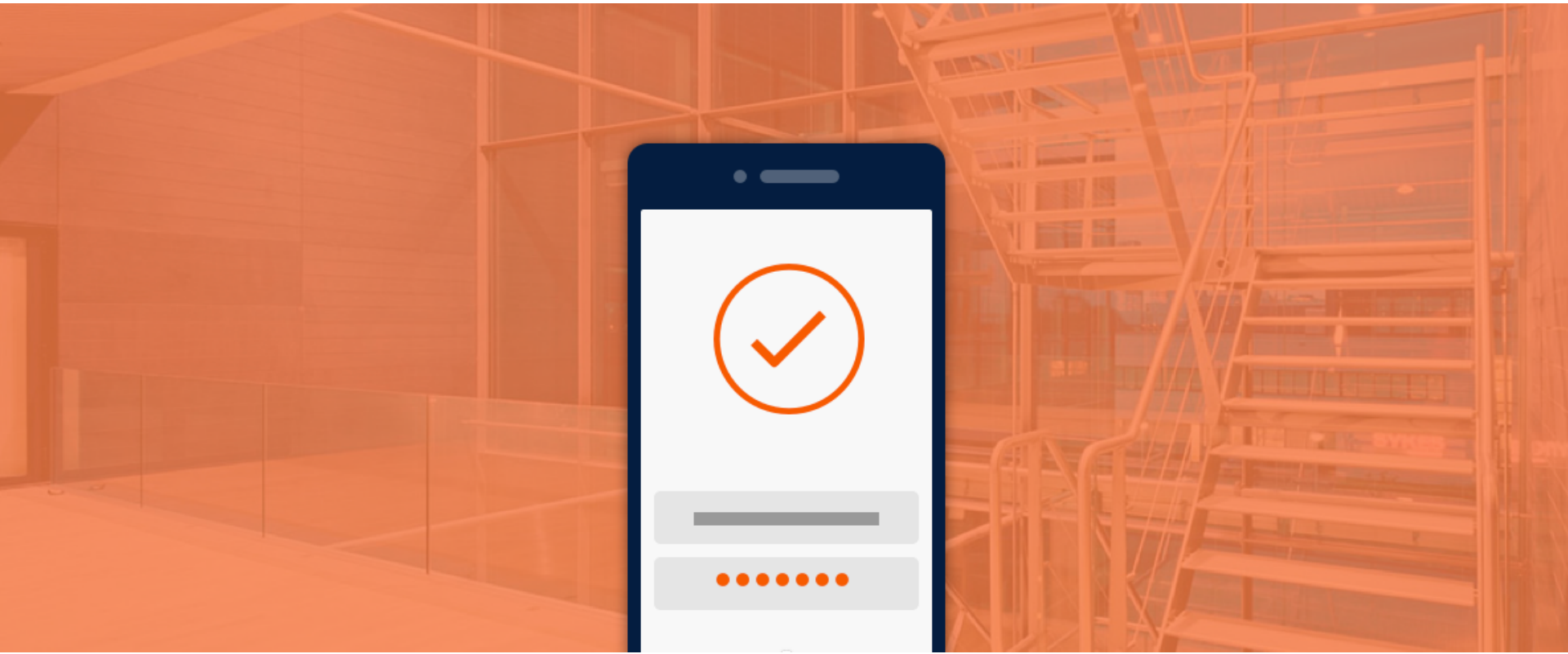
What we do


Design
Build
Test & Run
Security requirements
Threat modeling
Security Code reviews
Coding guidelines
Web pentesting
App pentesting

Research time!

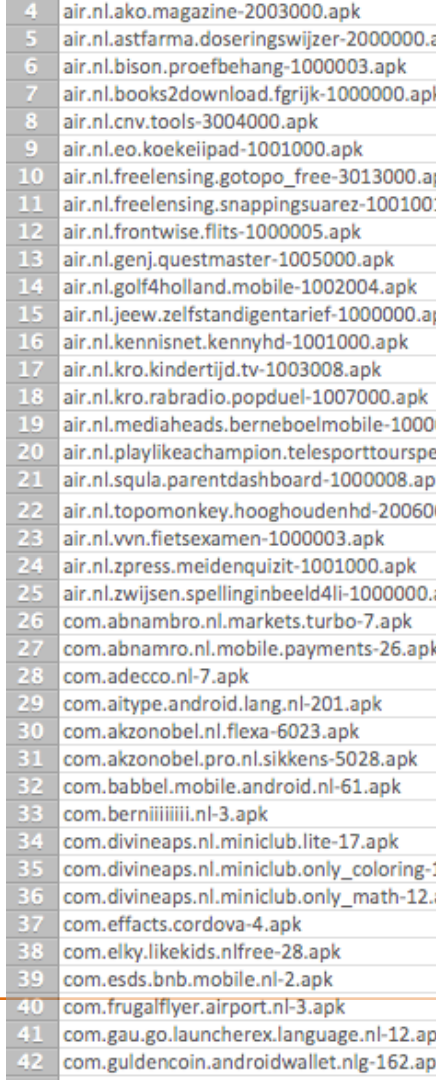
SOftware OwNage.

Testing 1000 Dutch Android Apps on SSL



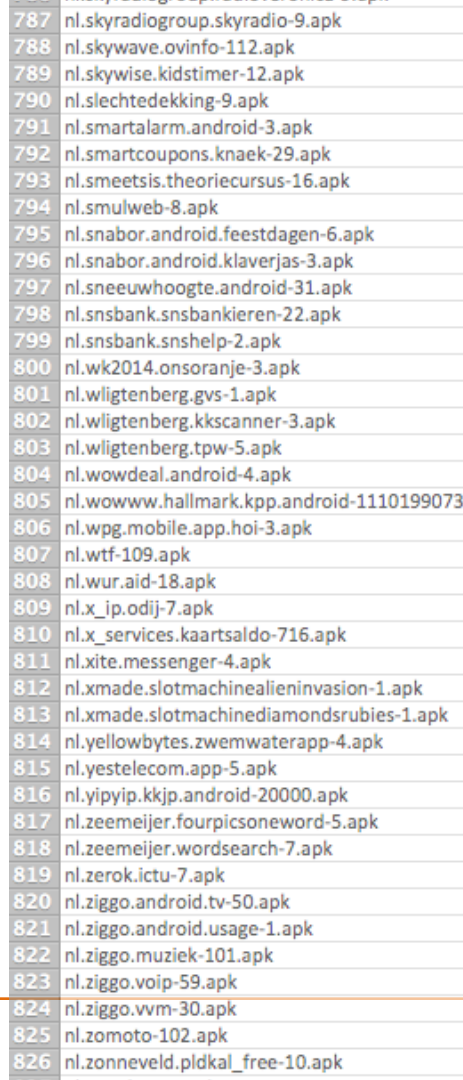
Research questions

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



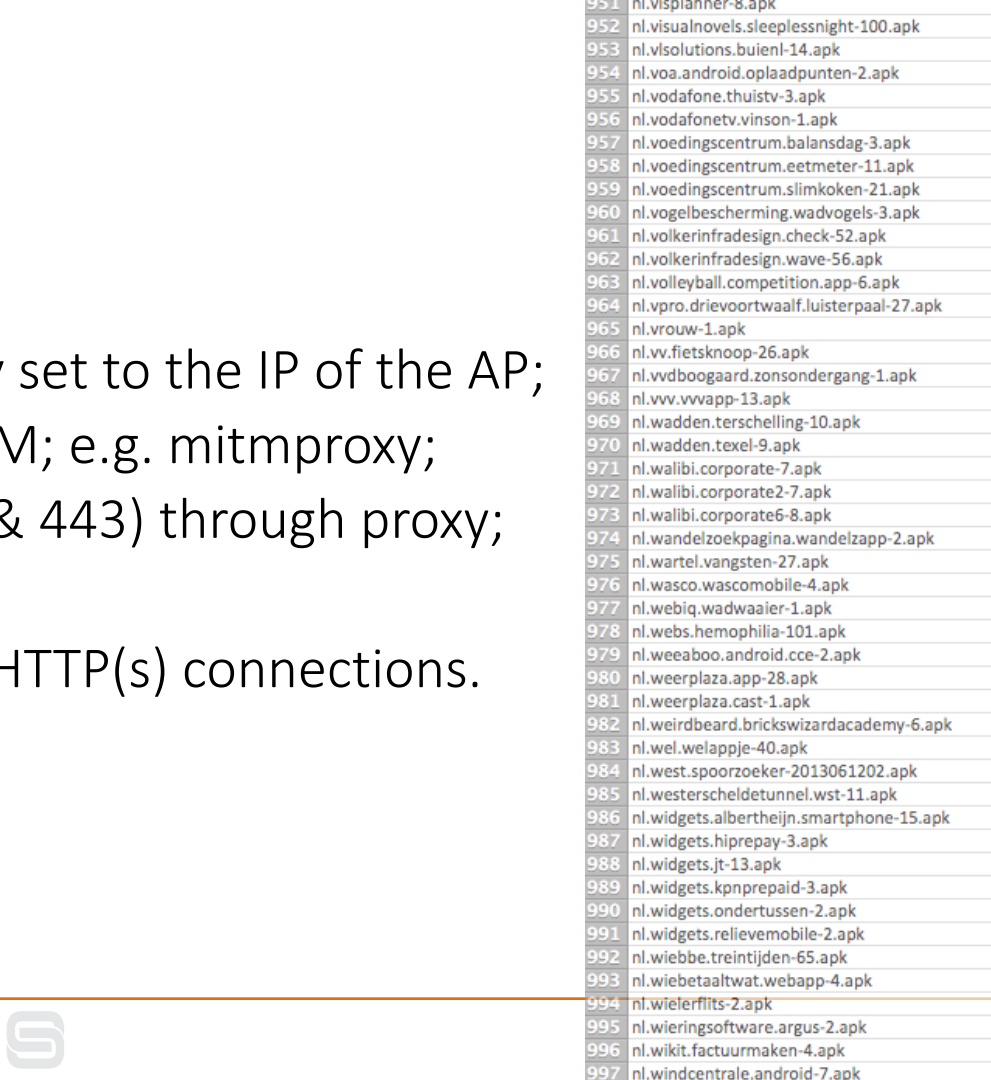
What we did

- 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 :-(



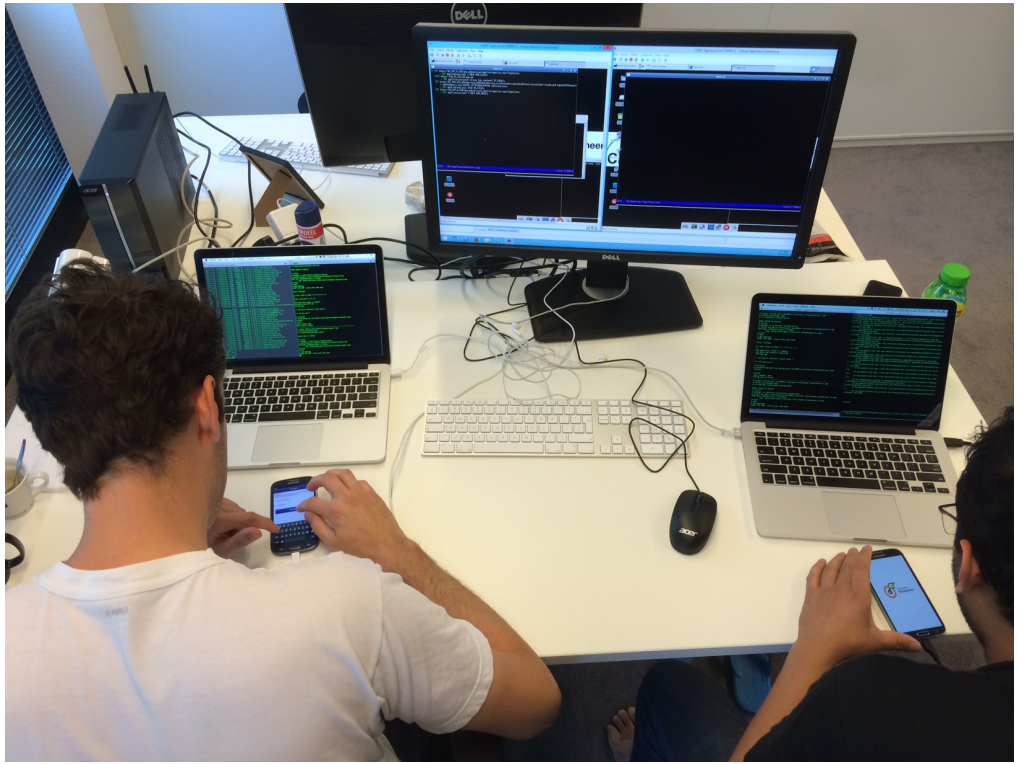
MiTM Set-up

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.



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)

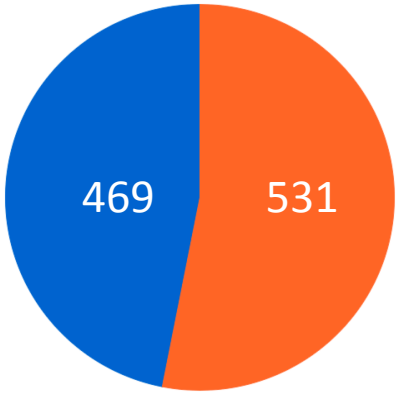
What did we see?

.. 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

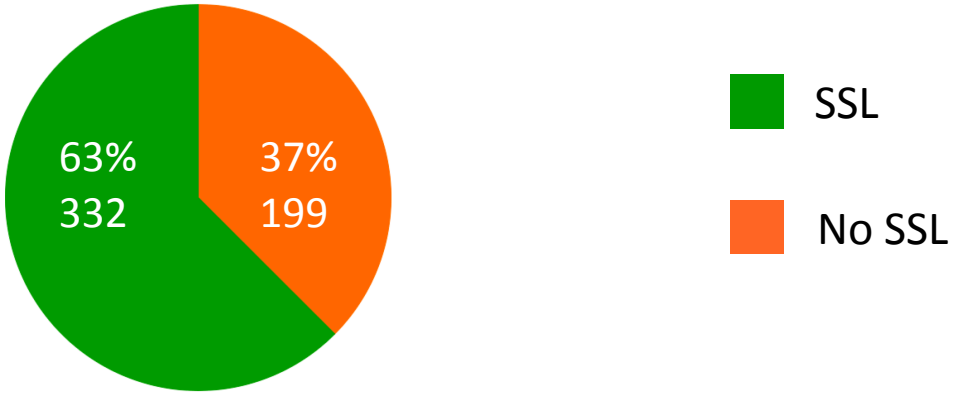


No network or no private data

Sends private data

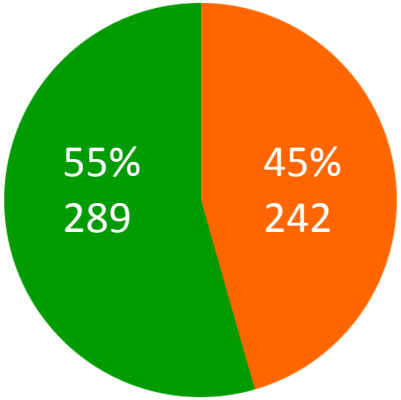
Results

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?

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...
'Krakkemikkig motortje voor horloges...
Salesforce 16% hoger op overnamegerucht
Apple vreest miljardenboete
Chrome-extensie beschermt tegen phishing
Vliegtuigen aan de grond door

Foto: Rechtenvrij

Deel op FB 445 Tweet 141 +1 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 beveiliging, waardoor data kunnen worden onderschept. Dat blijkt uit een test van beveiligingsbedrijf Securify, meldt de NOS zondagavond.

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

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

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

Deel op FB 445 Tweet 141 +1 1

Het PAROOL

nrc·next

NOS

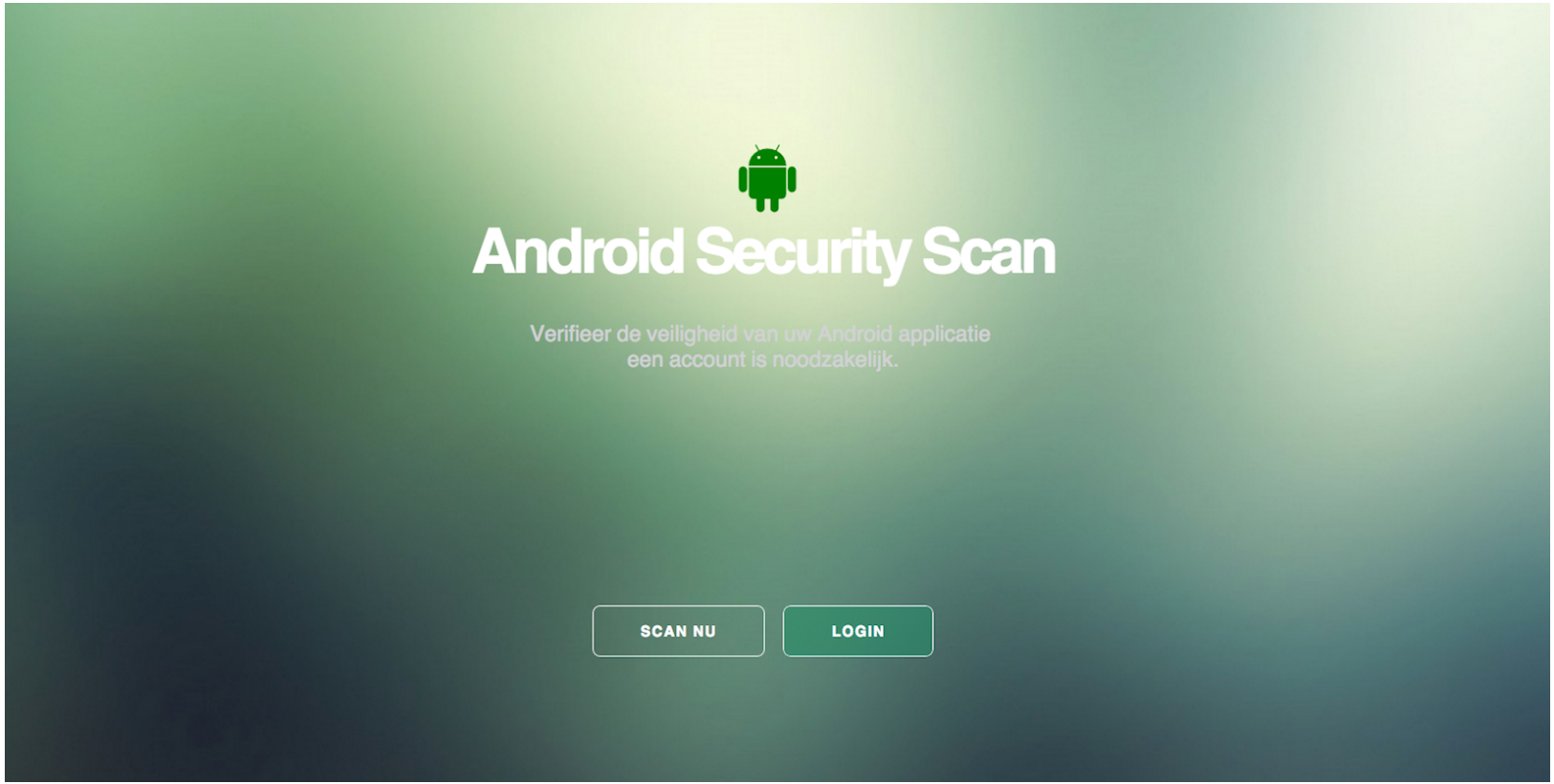
De Telegraaf

Do we care?

45 organisations contacted us for details….

We stopped chasing…

AppVer - Beta - Sneak Preview



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

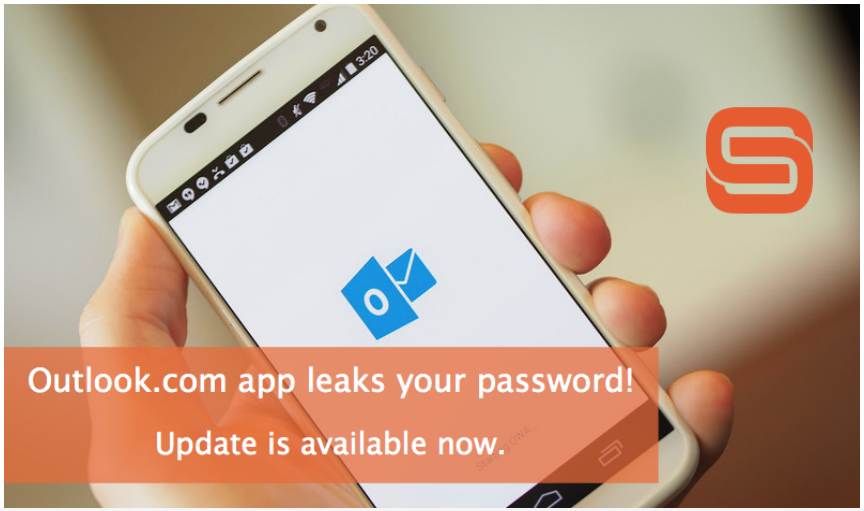
Insecure SSL/TLS

- 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	Size	Installs	Current Version	Requires Android
July 28, 2014	9.4M	10,000,000 - 50,000,000	7.8.2.12.49.7564	2.2 and up

Content Rating	Permissions	Report	Offered By	Developer
Everyone	View details	Flag as inappropriate	Outlook.com	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	Size	Installs	Current Version	Requires Android
November 20, 2014	32M	100,000,000 - 500,000,000	5.1.1.42	2.3 and up
Content Rating	**In-app Products**	**Permissions**	**Report**	**Offered By**
Medium Maturity	$0.99 - $35.17 per item	View details	Flag as inappropriate	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

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)

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."

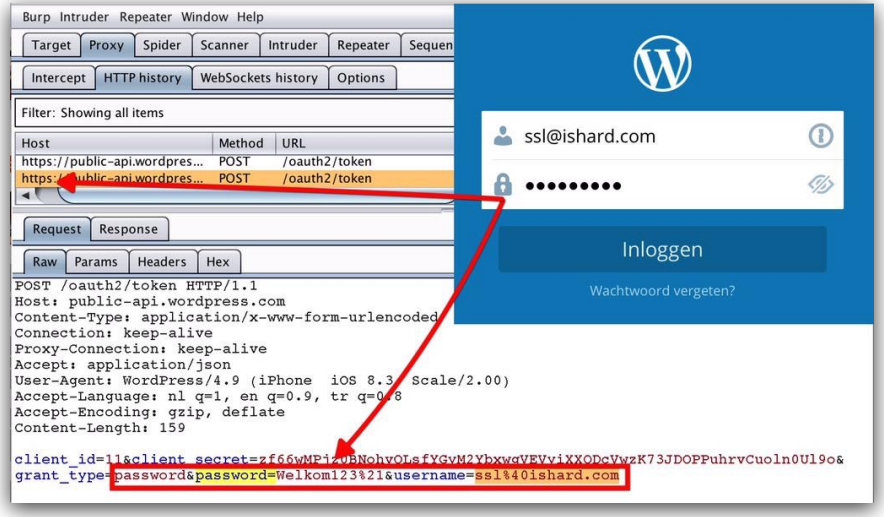
The net result for end users is that an attacker on the same wi-fi network could fairly easily view data in transit, which should otherwise have been encrypted. "Because the domain name wasn't checked, all they needed was a valid SSL certificate for any web server, something you can buy for $50," Source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

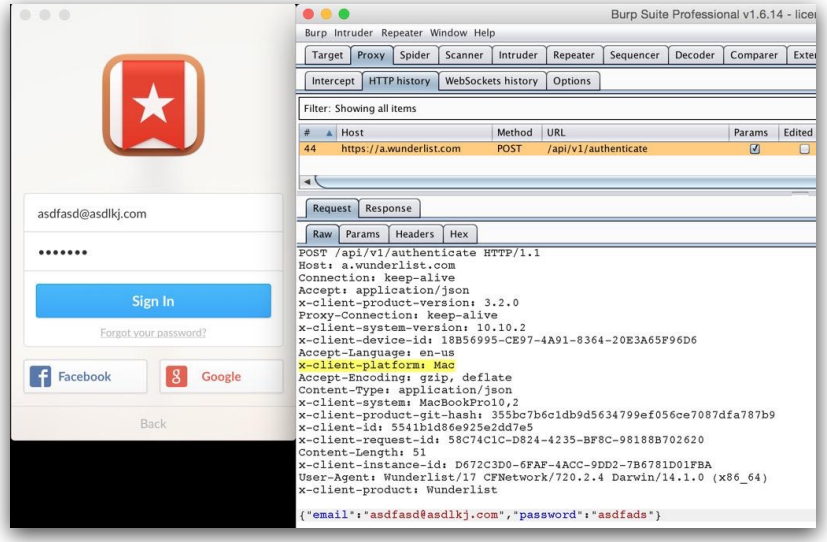
Read this

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

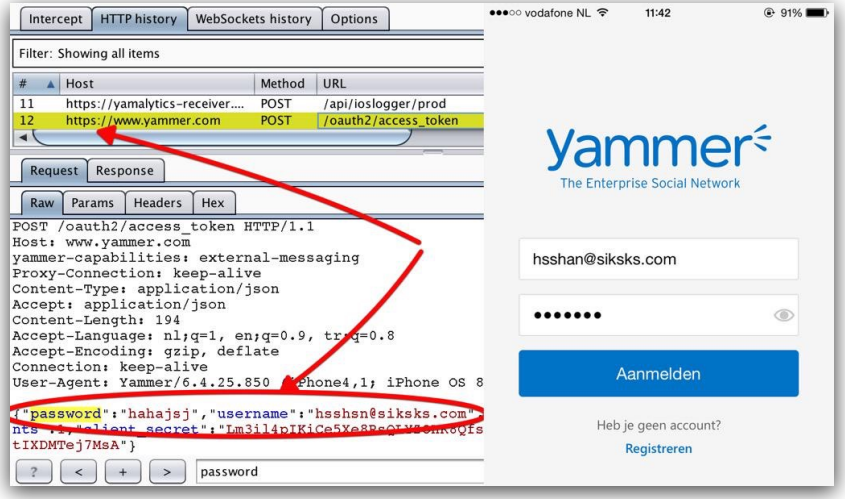
→ Read More

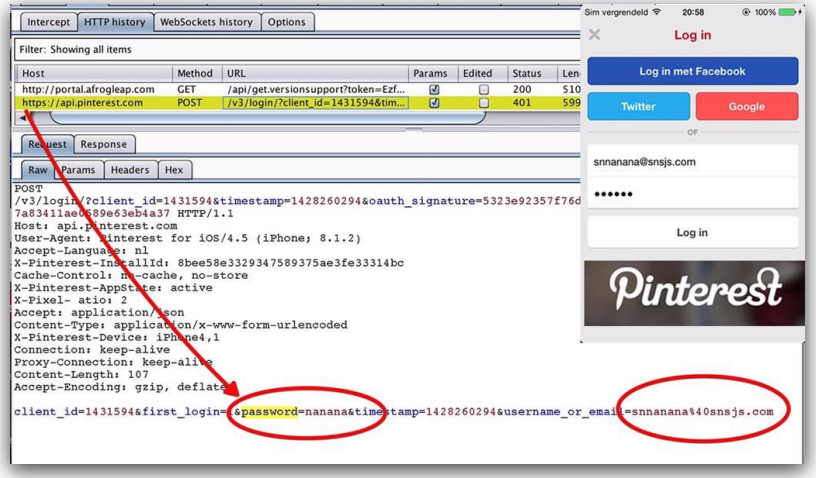
We find these bugs in iOS as well!





We find these bugs in iOS as well!





Security Summary for Yammer by Microsoft

Want full details on these apps? Get Free Report!

2	2
Vulnerable Apps	Apps Use AFNetworking

High Priority Affected Apps

1. Yammer
   - **Version**: 6.4.24 — **Libraries**: AFNetworking v2.5.1 — SSL Vulnerable
   - **Version**: 6.4.27 — **Libraries**: AFNetworking v2.5.2 — 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

Securify