RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Mobile Security Attacks
A Glimpse From the Trenches

SESSION ID: MBS-W06

Yair Amit

CTO & Co-Founder
Skycure
@YairAmit

Adi Sharabani

CEO & Co-Founder
Skycure
@AdiSharabani

#RSAC

About the Presenters

Yair Amit

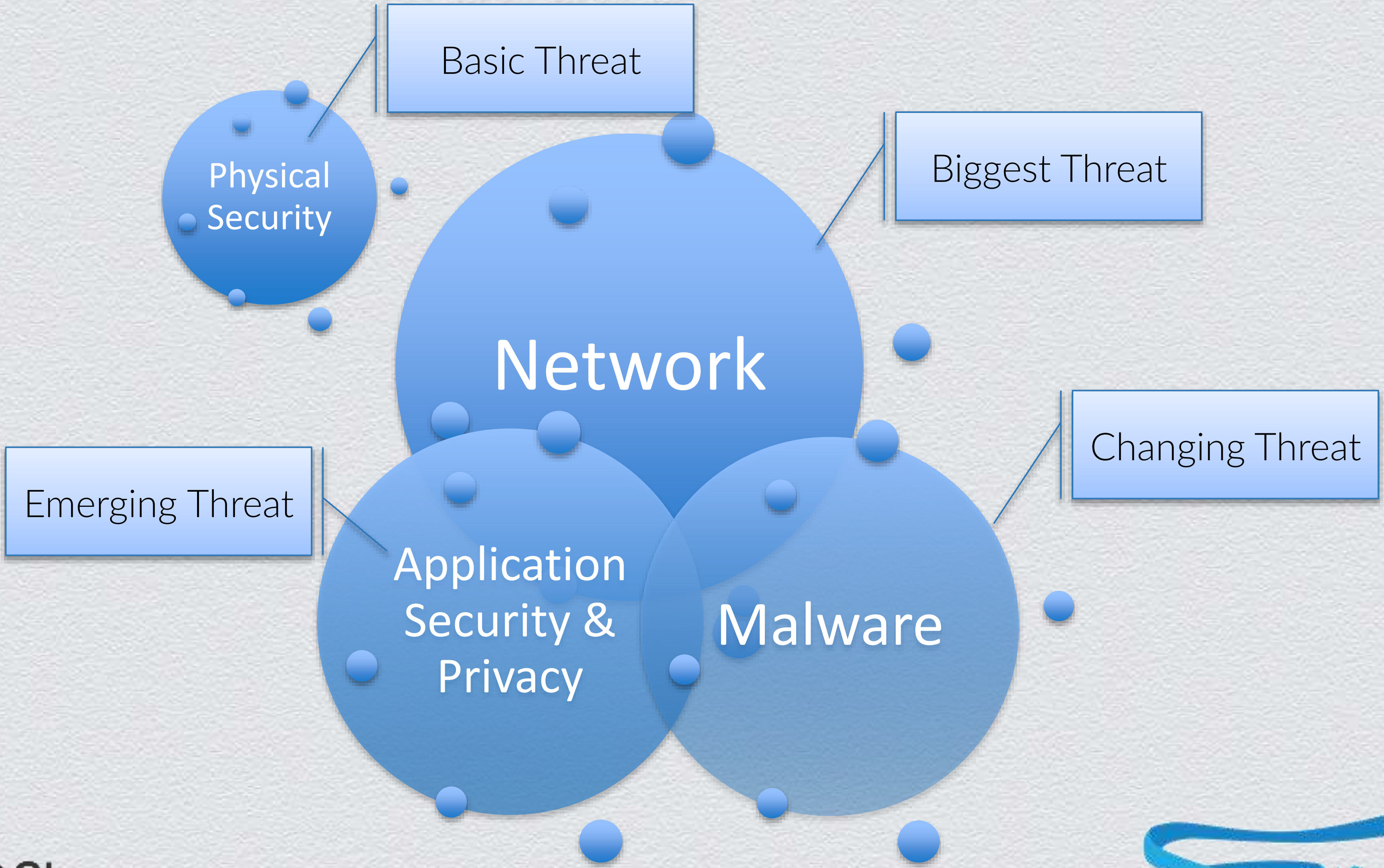
- CTO & co-founder of Skycure
- Web, network and mobile researcher
- Filed over 15 security patents
- Former manager of the Application Security & Research group at IBM

Adi Sharabani

- CEO & co-founder of Skycure
- Watchfire's research and security group [Acquired by IBM]
- Led the security of much of IBM software
- Fellow at Yuval Ne'eman's workshop
- Teacher at Ohel Shem high-school

Seamless Mobile Security

A Holistic Outlook on Mobile Security



The Physical Layer

The Physical Layer

- Threat vector
  - Device lost / Device stolen / Temporary physical access
- Basic physical security needs:
  - Remote wipe
  - Locate device
  - Backup
  - Local storage
  - Passcode protection
- The above becomes OS responsibility
- MDM provides the above OS features together with management and policy enforcement

Network Based Attacks

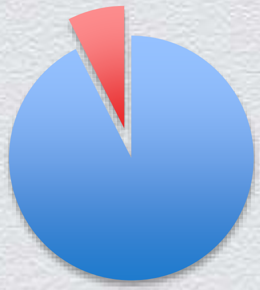
Insights from Skycure's database

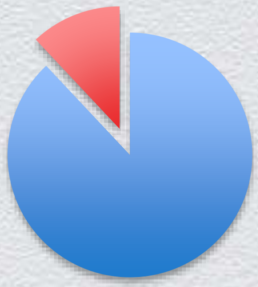
- Real-world statistics (Skycure's database)
  - 10763 scanned networks

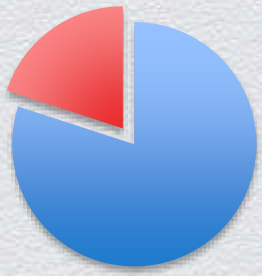
7.5%
of scanned networks **pose a threat**

12%
of all devices **connected to such networks** every **week**

20%
of all devices **connected to such networks** every **month**







Skycure

Network Based Attacks

Implementation-Based Vulnerabilities

Vs.

Design-Based Vulnerabilities

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Network Based Attacks

Implementation issues

Implementation-Based Vulnerabilities

iOS vs. Android

Implementation-Based Vulnerabilities

>> Read more

- Example I:

gotofail

Gotofail – The Code

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen) {

    …
    if ((err = SSLHashSHA1.update(&hashCtx, &clientRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
        goto fail;
    if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
        goto fail;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
     err = sslRawVerify(ctx,
                        ctx->peerPubKey,
                        dataToSign,                /* plaintext */
                        dataToSignLen,             /* plaintext length */
                        signature,
                        signatureLen);
    …
fail:
    SSLFreeBuffer(&signedHashes);
    SSLFreeBuffer(&hashCtx);
    return err;
}
```

Always goto "fail", even if err==0

Code is skipped (even though err == 0)

Function returns 0 (i.e. verified), even though sslRawVerify was not called

Implementation-Based Vulnerabilities

>> Read more

- Example II:

Heartbleed

Network Based Attacks

Design issues

Design-Based Vulnerabilities

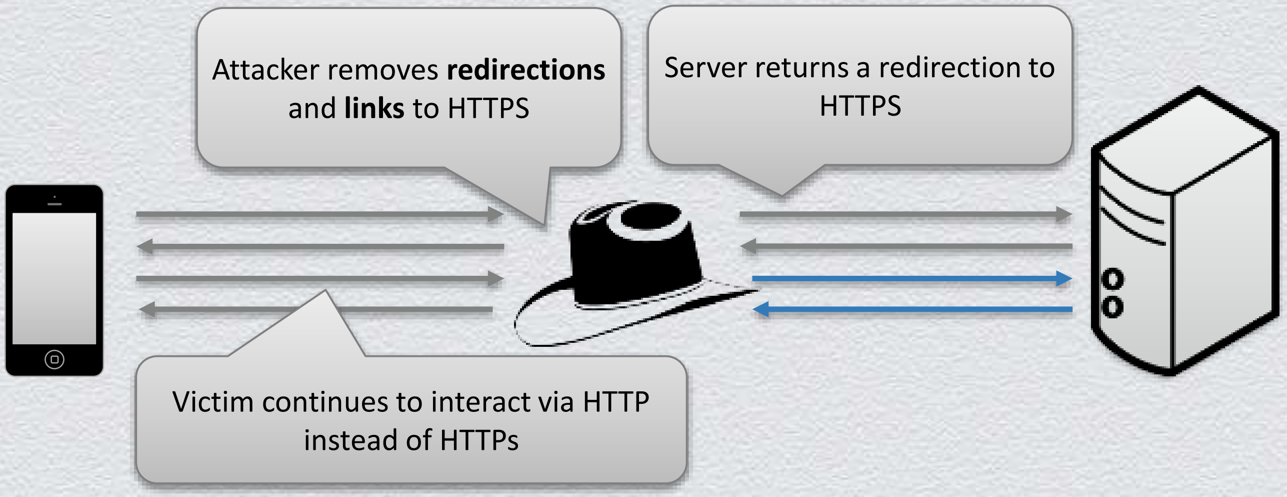
- Design issues are much more interesting
  - … and much harder to fix
- These are divided into two types:
  - General "protocol" vulnerabilities
  - Design issues affecting mobile OS
- Mobile devices are more susceptible:
  - Lack of adequate security solutions
  - Excessive use of untrusted networks

Design-Based Vulnerabilities (Generic)

>> Read more

- Example I:

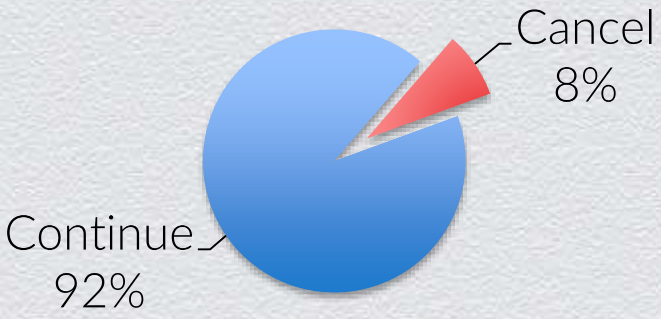
sslstrip

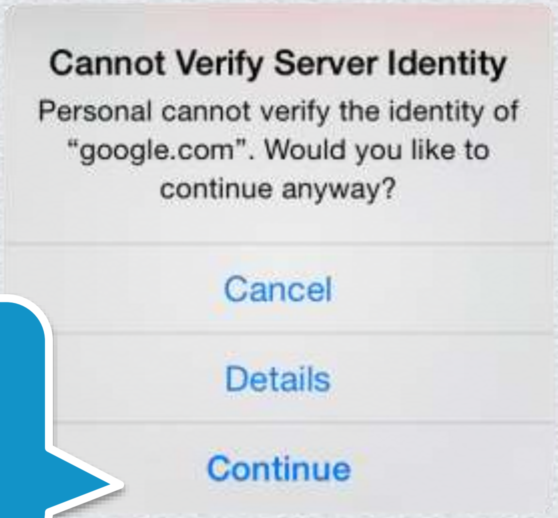

Attacker removes **redirections** and **links** to HTTPS
Server returns a redirection to HTTPS
Victim continues to interact via HTTP instead of HTTPs

Design-Based Vulnerabilities (Generic)

- Example II:

SSL decryption




Cannot Verify Server Identity

Personal cannot verify the identity of "google.com". Would you like to continue anyway?

92% of users click on "Continue" compromising their Exchange identity (username and password)

Design-Based Vulnerabilities (Generic)

>> Read more

- Example III:

Karma

Hak5's WiFi Pineapple

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Network Based Attacks

Mobile-specific
design issues

iOS Security Model

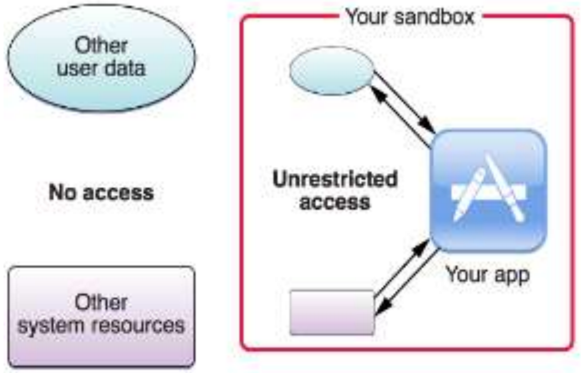
App Characteristics

- One Store
- Heavy Screening
- App Sandboxing

Profile Characteristics

- No Store
- No Screening
- No Sandboxing

iOS sandbox approach



Source: Apple's App Sandbox Design Guide

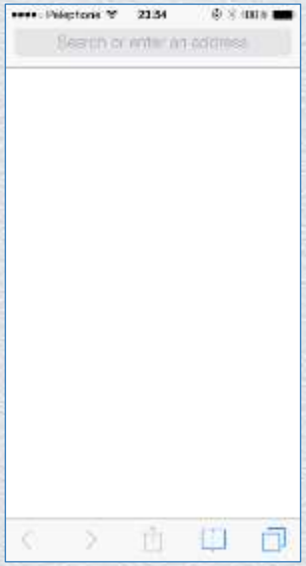
Skycure

Configuration Profiles

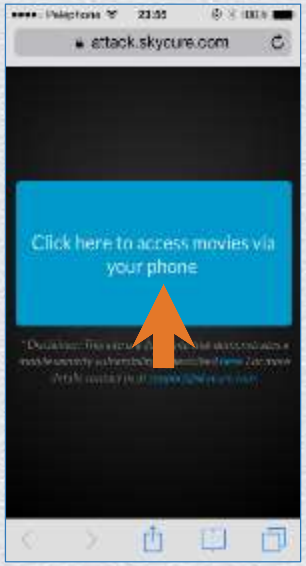
Where Do We Find Them?

- Mobile Device Management (MDM)
- Cellular carriers
    - Usually used for APN settings
- Mobile applications
- Service providers

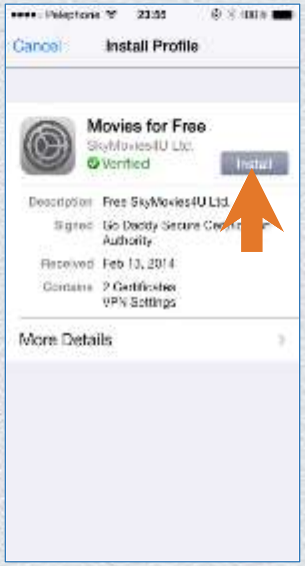
Demo: Participation Instructions



1. Open your Safari

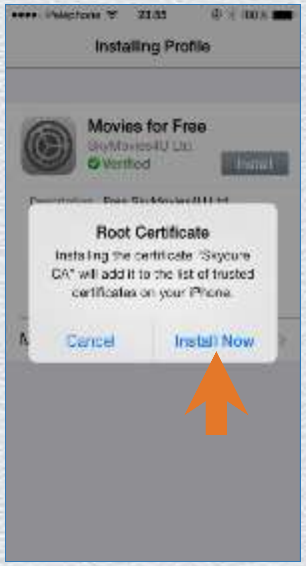


2. Tap the blue button



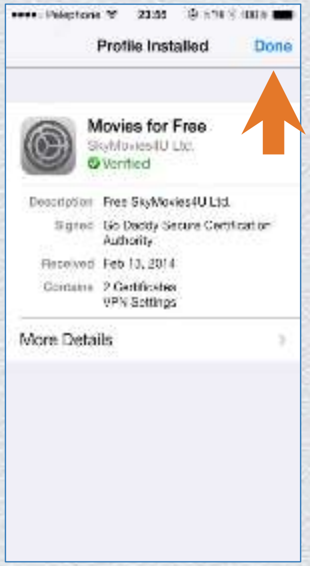
Description Free SkyMovies4U Ltd.
Signed Go Daddy Secure Certificate Authority
Received Feb 13, 2014
Contains 2 Certificates VPN Settings

3. Click on 'Install'



Installing the certificate "Skycure CA" will add it to the list of trusted certificates on your iPhone.

4. Click on 'Install Now'



Description Free SkyMovies4U Ltd.
Signed Go Daddy Secure Certificate Authority
Received Feb 13, 2014
Contains 2 Certificates VPN Settings

5. Click on 'Done'

Start demo by opening Safari and browsing to:

attack.skycure.com

Skycure

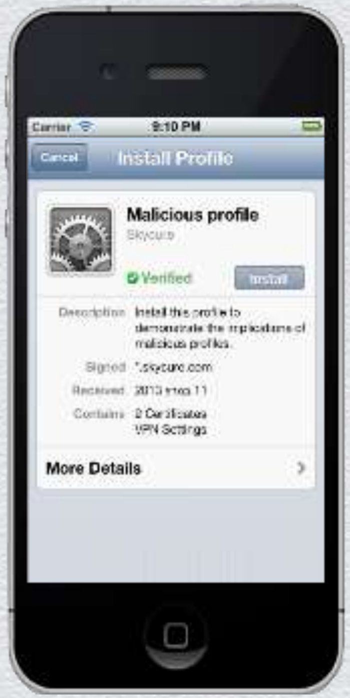
#RSAC RSACONFERENCE2014 ASIA PACIFIC & JAPAN

Malicious Profiles

Where Do We Find Them?

>> Read more

- Malicious “service providers” (apps/services/Wi-Fis/etc.)
- Vulnerable services
- Privacy violating services



Malicious profile
Skycure
Verified
Install

Description	Install this profile to demonstrate the implications of malicious profiles.
Signed	*.skycure.com
Received	2013 [illegible] 11
Contains	2 Certificates VPN Settings

More Details

Hacker gains access to your mail, business apps, cloud services, bank accounts and more, even if traffic is encrypted

Skycure

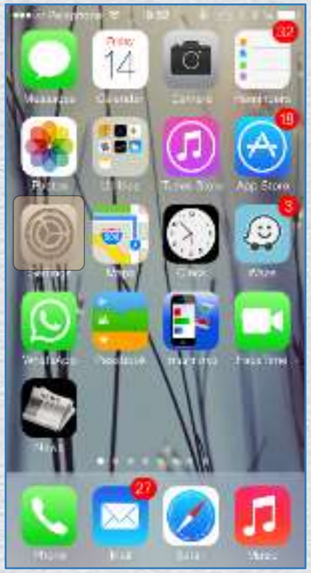
Malicious Profiles

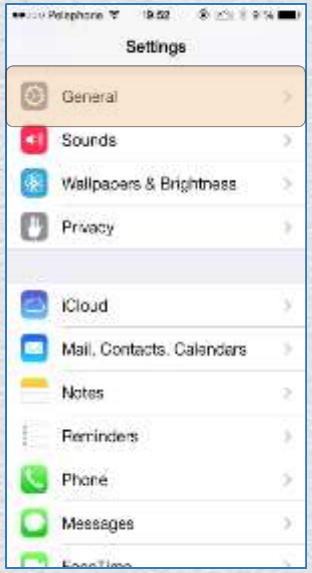
Going Viral

- Attacker hijacks victim's key identities
  - Corporate Exchange
  - Facebook
  - LinkedIn
- Attacker sends mass messages to victim's contacts, luring them to install the malicious profile
- Attack propagates

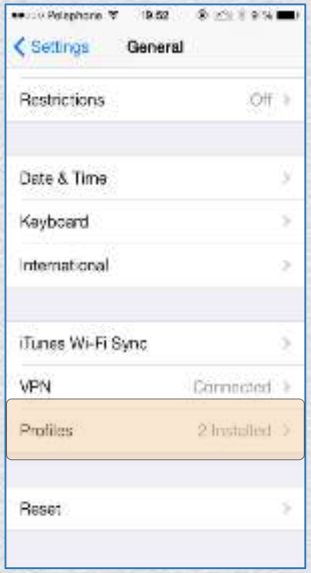
Am I Safe?

- Profile listing could indicate suspicious profiles
- Cat-and-mouse game: attackers can name their profile to look benign

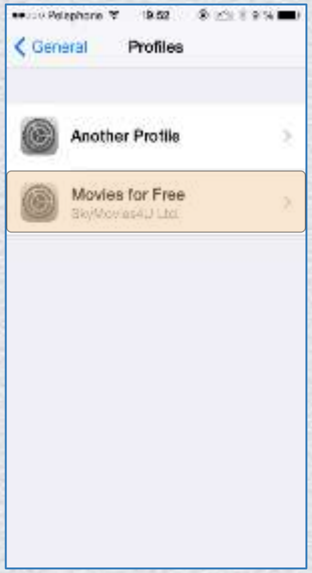



Settings

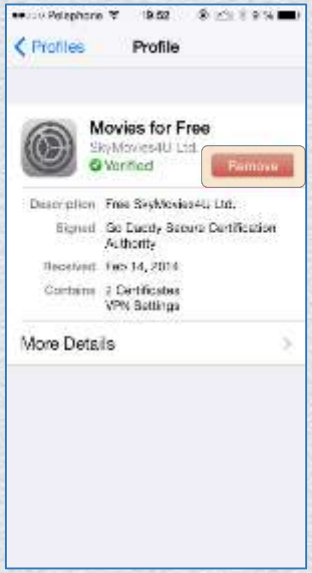
General
Sounds
Wallpapers & Brightness
Privacy
iCloud
Mail, Contacts, Calendars
Notes
Reminders
Phone
Messages
FaceTime


Settings General

Restrictions Off
Date & Time
Keyboard
International
iTunes Wi-Fi Sync
VPN Connected
Profiles 2 Installed
Reset


General Profiles

Another Profile
Movies for Free
SkyMovies4U Ltd.


Profiles Profile

Movies for Free
SkyMovies4U Ltd.
Verified
Remove

Description: Free SkyMovies4U Ltd.
Signed: Go Daddy Secure Certification Authority
Received: Feb 14, 2014
Contains: 2 Certificates, VPN Settings

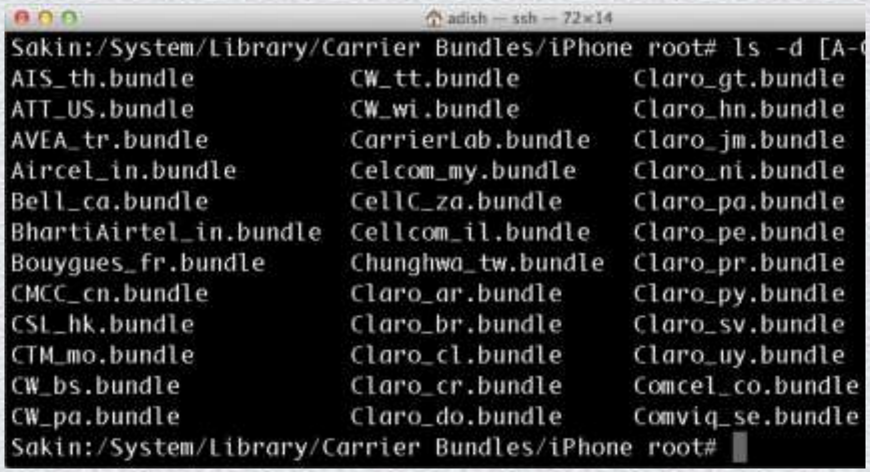
More Details

Design-Based Vulnerabilities (Mobile)

>> Read more

- Example II:

WiFiGate


adish — ssh — 72×14

```
Sakin:/System/Library/Carrier Bundles/iPhone root# ls -d [A-
AIS_th.bundle            CW_tt.bundle         Claro_gt.bundle
ATT_US.bundle            CW_wi.bundle         Claro_hn.bundle
AVEA_tr.bundle           CarrierLab.bundle    Claro_jm.bundle
Aircel_in.bundle         Celcom_my.bundle     Claro_ni.bundle
Bell_ca.bundle           CellC_za.bundle      Claro_pa.bundle
BhartiAirtel_in.bundle   Cellcom_il.bundle    Claro_pe.bundle
Bouygues_fr.bundle       Chunghwa_tw.bundle   Claro_pr.bundle
CMCC_cn.bundle           Claro_ar.bundle      Claro_py.bundle
CSL_hk.bundle            Claro_br.bundle      Claro_sv.bundle
CTM_mo.bundle            Claro_cl.bundle      Claro_uy.bundle
CW_bs.bundle             Claro_cr.bundle      Comcel_co.bundle
CW_pa.bundle             Claro_do.bundle      Comviq_se.bundle
Sakin:/System/Library/Carrier Bundles/iPhone root# 
```

App Level Security

App Level Security & Privacy

- Mobile OS enforce additional security models
  - Sandbox
  - Better updates
  - Controlled application stores
- App-level issues are now on the rise

App Vulnerabilities

App Level Vulnerabilities

- Example I:

Plain HTTP

Daaa!

App Level Vulnerabilities

>> Read more

- Example II:

Certificate Pinning

Certificate Pinning

A Long Way to Go

- Almost all major apps today lack SSL Pinning
  - Susceptible to attacks such as malicious profiles by design
  - Also exploited when attacker gains access to a trusted CA
- Slow adoption should not come as a surprise
  - Implementation challenges
    - Less flexibility
    - Can become a nightmare if done wrong…

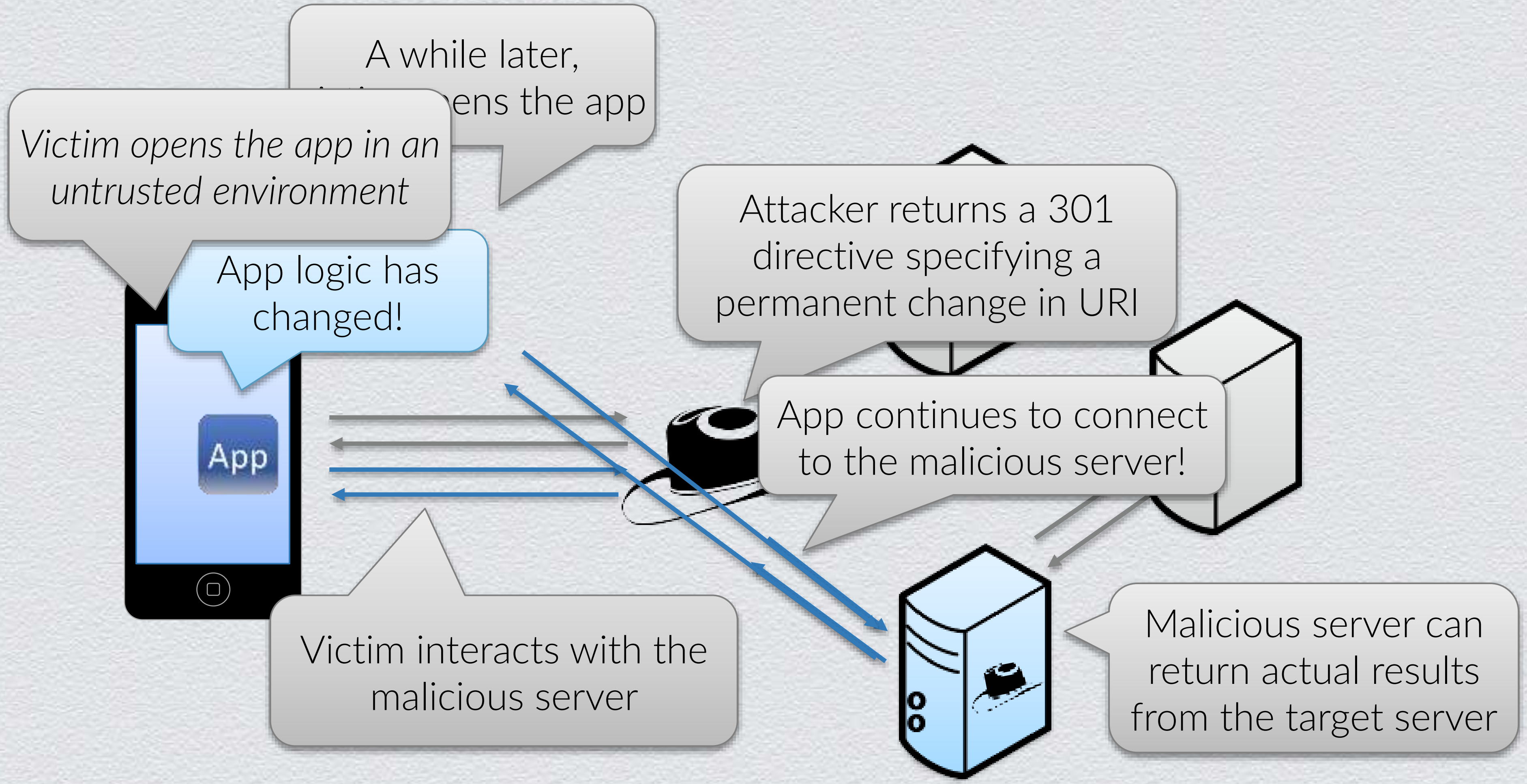
App Level Vulnerabilities

- Example III:

HTTP Request Hijacking

>> Read more

HRH – Attack Flow

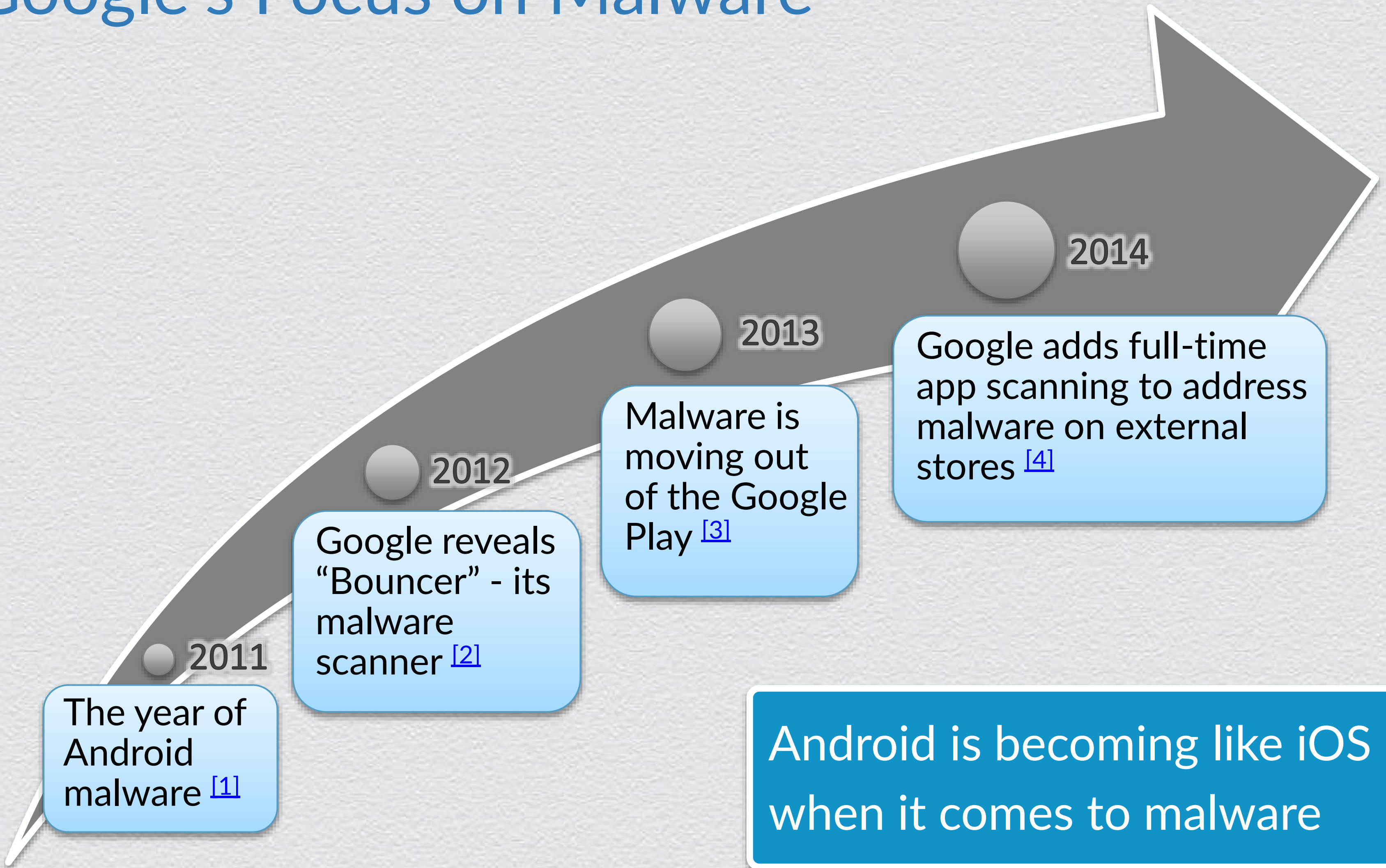

Victim opens the app in an untrusted environment
Victim interacts with the malicious server
A while later, ens the app
App logic has changed!
Attacker returns a 301 directive specifying a permanent change in URI
App continues to connect to the malicious server!
Malicious server can return actual results from the target server
App

Skycure

#RSAC RSACONFERENCE2014 ASIA PACIFIC & JAPAN

Malicious Apps

Google's Focus on Malware



2011

The year of Android malware [1]

2012

Google reveals "Bouncer" - its malware scanner [2]

2013

Malware is moving out of the Google Play [3]

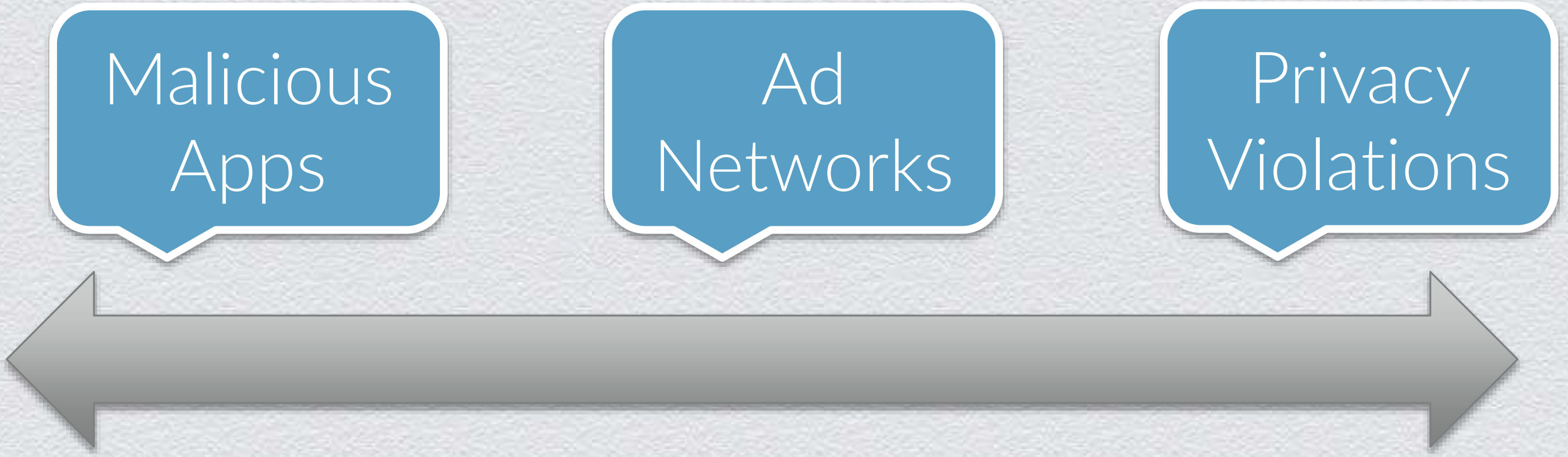
2014

Google adds full-time app scanning to address malware on external stores [4]

Android is becoming like iOS when it comes to malware

The Maliciousness Axis

- While OS anti-malware techniques advance, there are other similar problems (harder to address)



The Maliciously Vulnerable App

- Malicious services sometimes try to justify their actions
  - "I need all your key-strokes to provide you with a better service"
- We are concerned about the Maliciously-Vulnerable app:
  - App with semi-naive service is created
  - App does not pose a privacy/security issue
  - App is approved to go on AppStore/Google Play.
  - App has a special crafted carefully thought vulnerability
  - Vulnerability used as a backdoor to escalate app for malicious activity

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Summary

Summary

- The physical layer
  - Becomes the OS responsibility
- Network based attacks
  - Implementation vulnerabilities
  - Design vulnerabilities
    - Generic vs. mobile specific
- App level
  - Vulnerabilities
    - HTTP/S, Certificate Pinning, HTTP Request Hijacking
  - The "maliciousness" axis
    - Malware ⇔ Ad Networks ⇔ Privacy Violations

Thank you!

- twitter: @YairAmit, @AdiSharabani
- email: {yair,adi}@skycure.com
- blog: http://www.skycure.com/blog

Seamless Mobile Security
Skycure