RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: MBS-T09

# Mobile Vulnerabilities From Data Breach to Complete Shutdown

**Adi Sharabani**

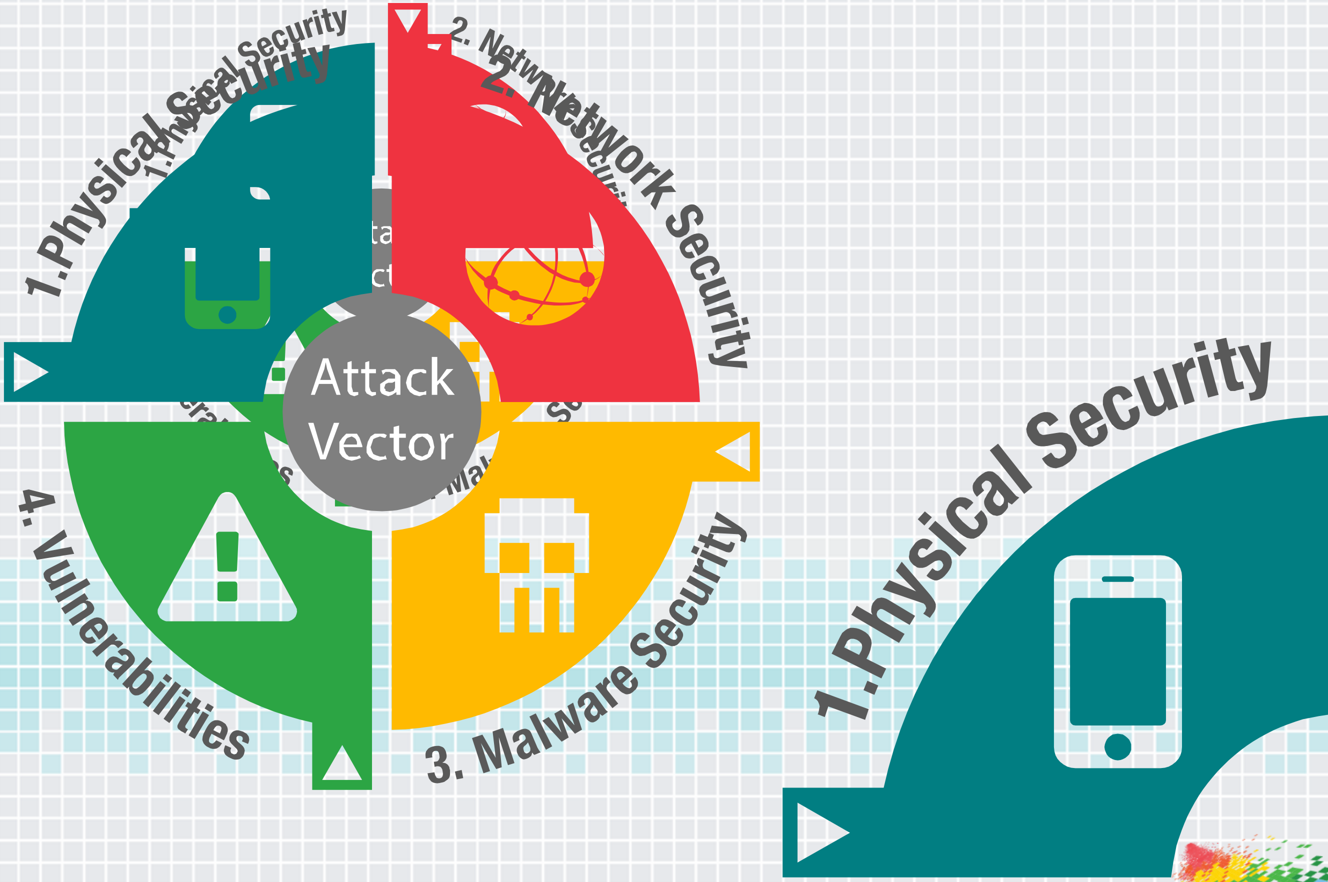
CEO and Co-Founder
Skycure
@adisharabani

**Yair Amit**

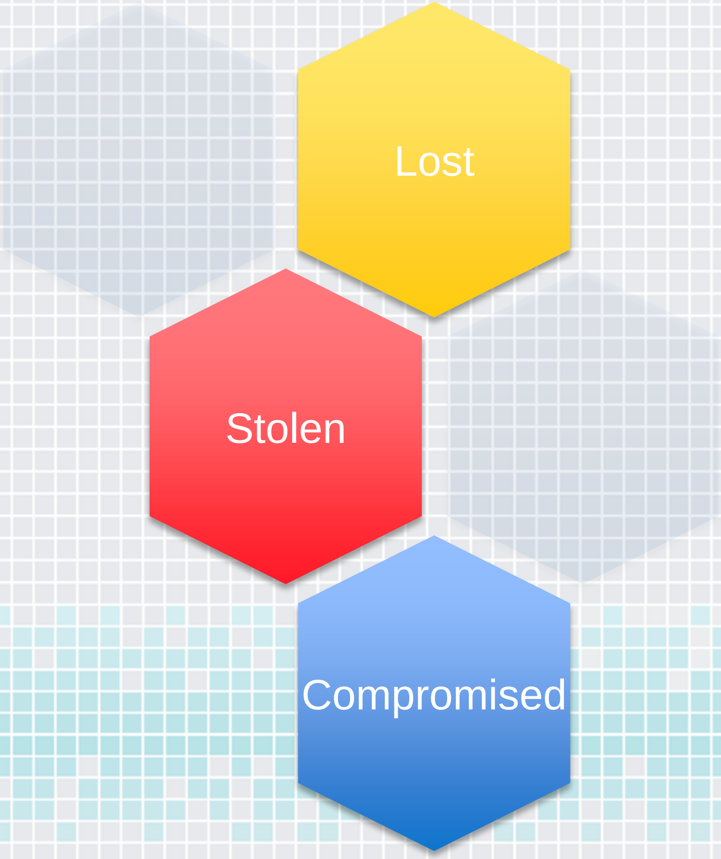
CTO and Co-Founder
Skycure
@YairAmit

#RSAC

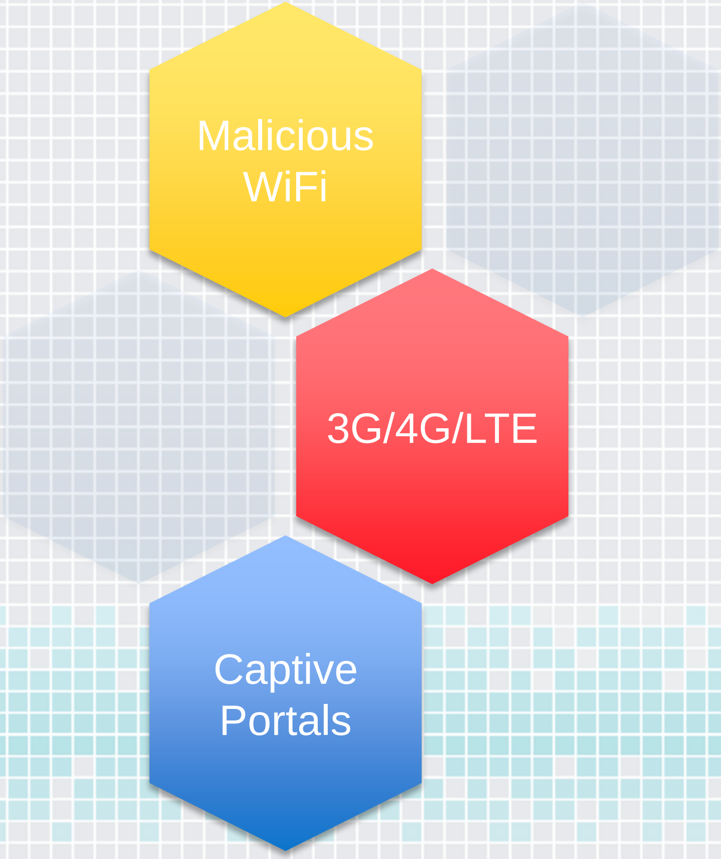
# Mobile Security Landscape



# 1.Physical Security



# 2. Network Security

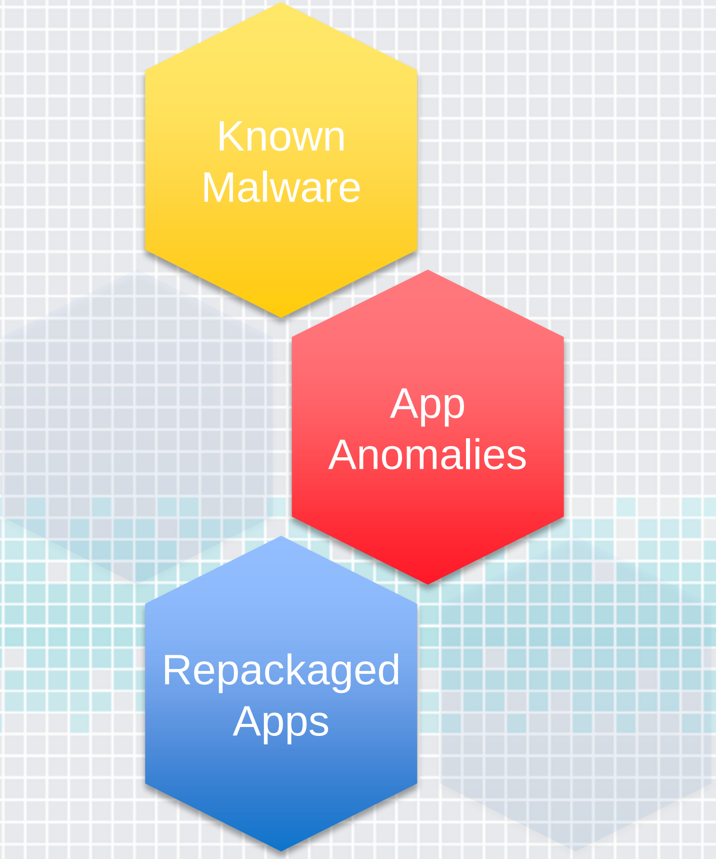


Malicious WiFi

3G/4G/LTE

Captive Portals

# 3. Malware Security

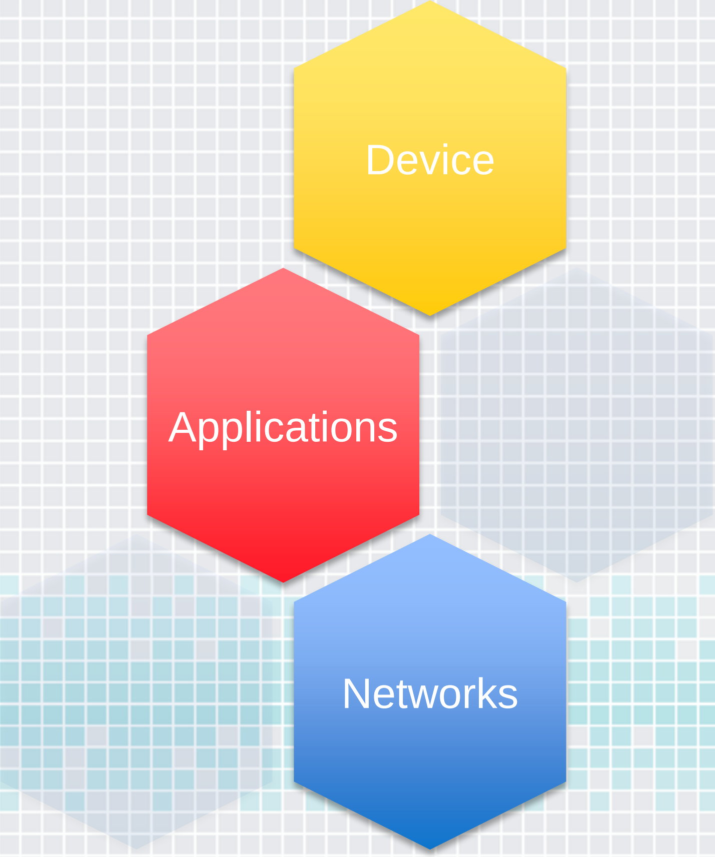


Known Malware

App Anomalies

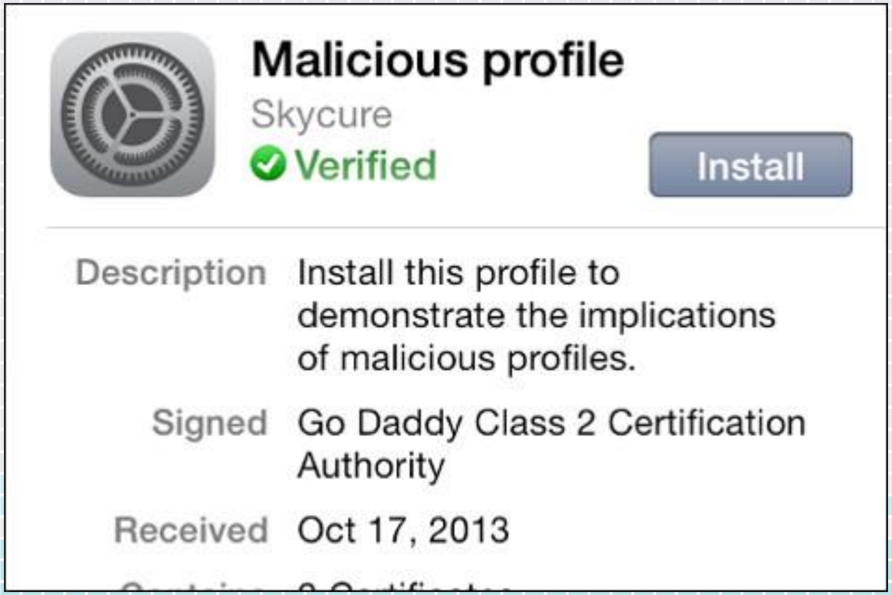
Repackaged Apps

# 4. Vulnerabilities



# Previous Disclosures by Skycure

- iOS Malicious Profiles
- Invisible Malicious Profiles
- WiFiGate
- HTTP Request Hijacking
- Linked~~In~~Out



**Malicious profile**
Skycure
✓ Verified

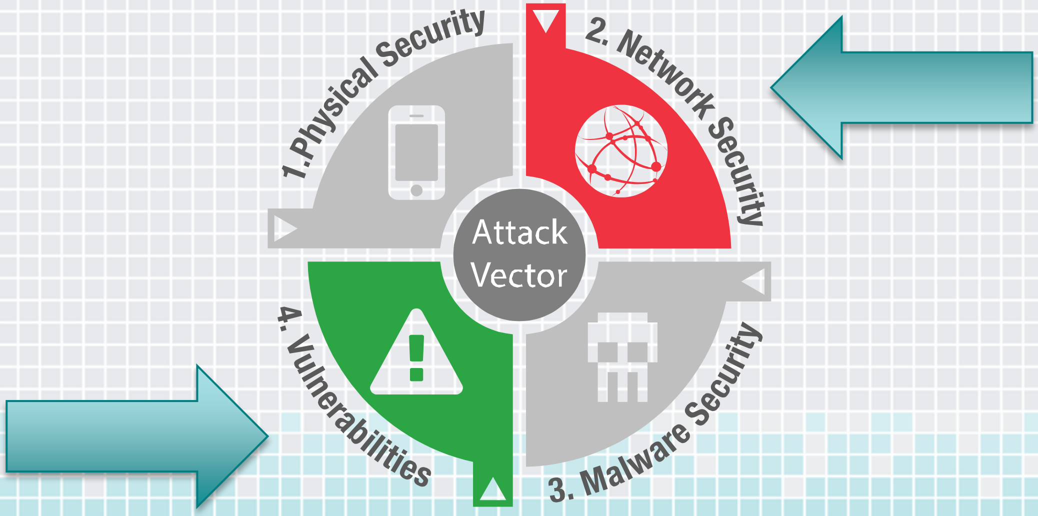
Description: Install this profile to demonstrate the implications of malicious profiles.

Signed: Go Daddy Class 2 Certification Authority

Received: Oct 17, 2013

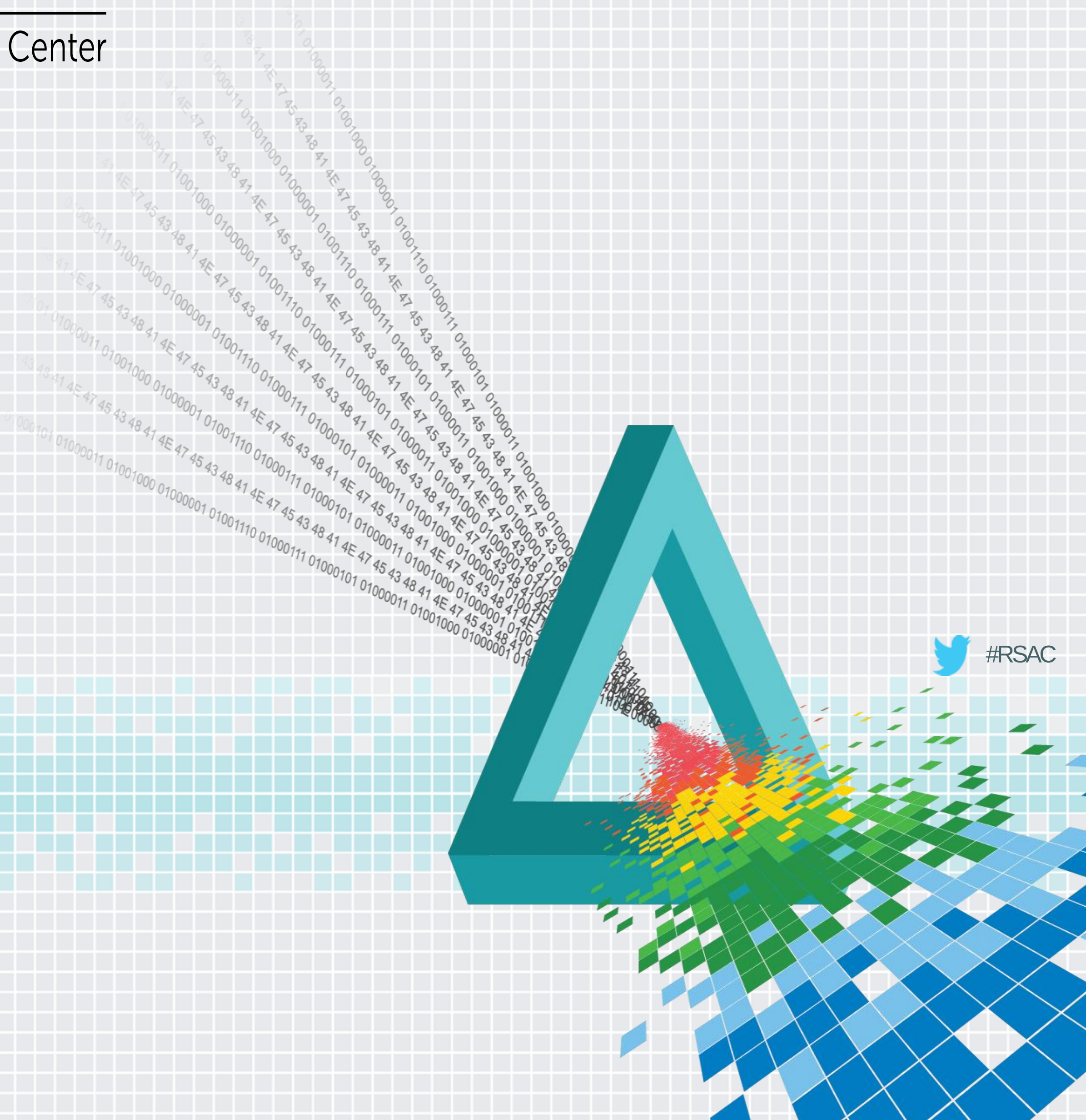
Contains: 2 Certificates

# This Year's Focus



RSAConference2015

San Francisco | April 20-24 | Moscone Center



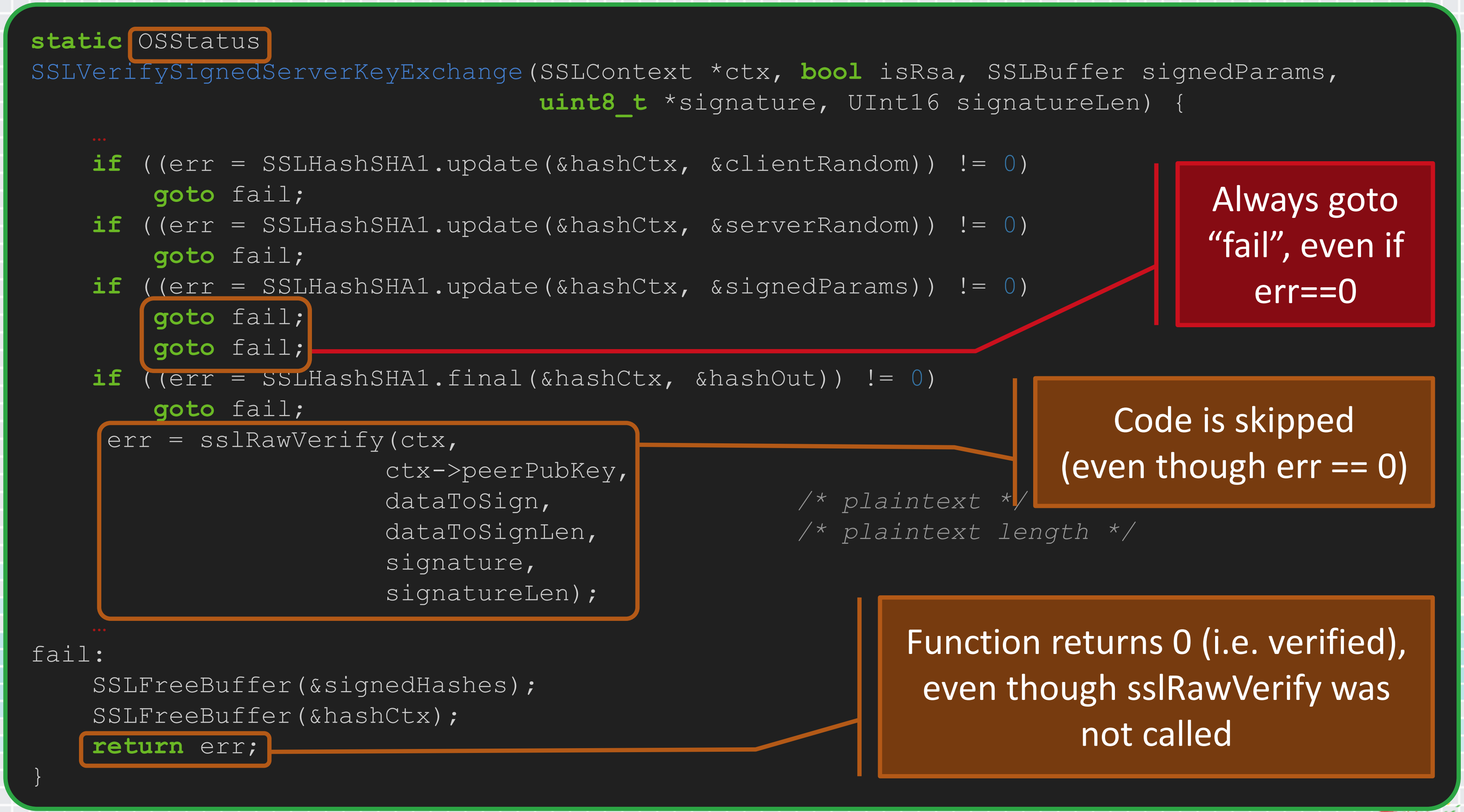
#RSAC

# Vulnerabilities

# SSL Stack

- Previous examples
  - goto fail;
  - Heartbleed
  - SSL decryption issues

# Example 1: GoToFail



```
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;
}
```

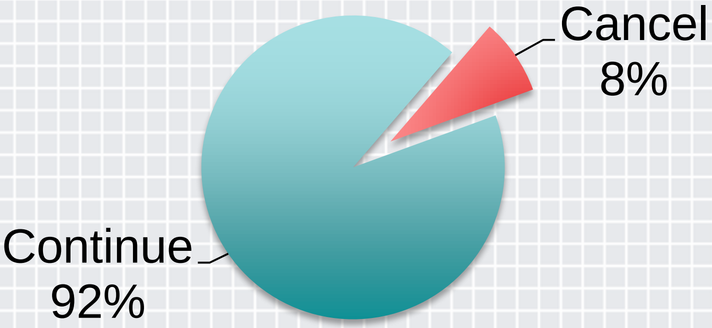
Always goto “fail”, even if err==0

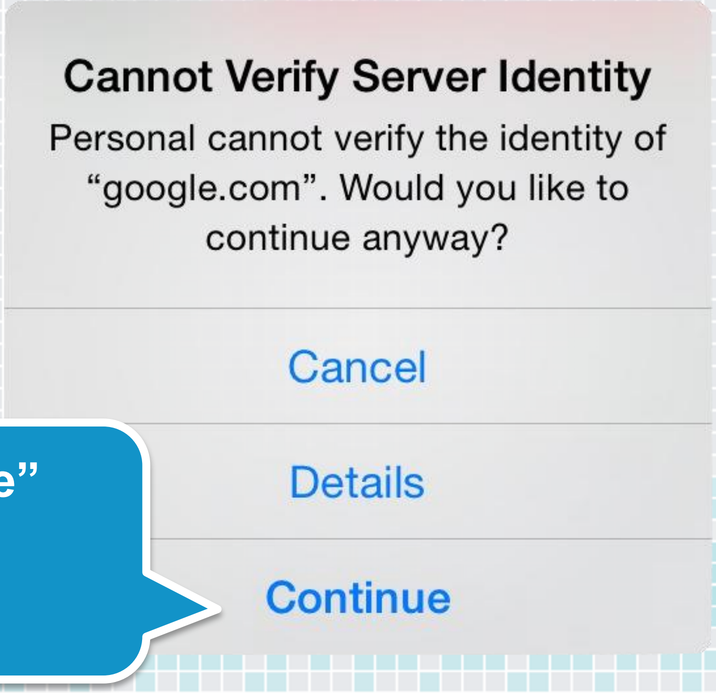
Code is skipped (even though err == 0)

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

Source: Apple’s published source code

# Example 2: SSL Decryption





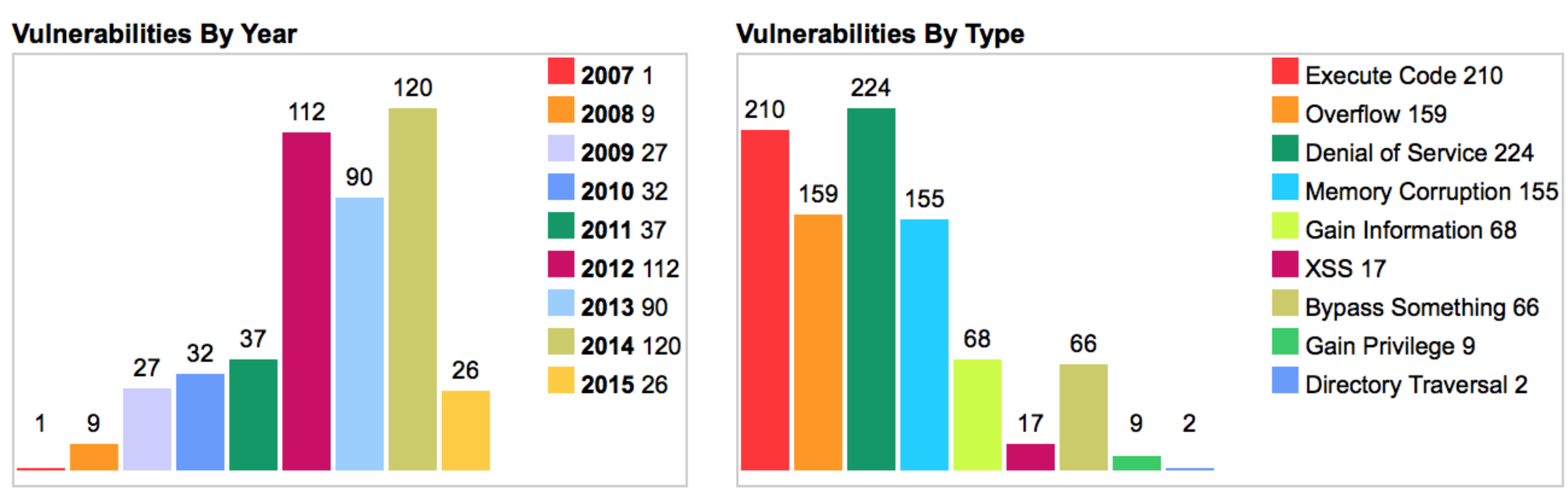
**Cannot Verify Server Identity**

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)**

# CVEs - The Numbers

## iOS CVE Stats



Source: cvedetails.com

# How to Identify These Bugs

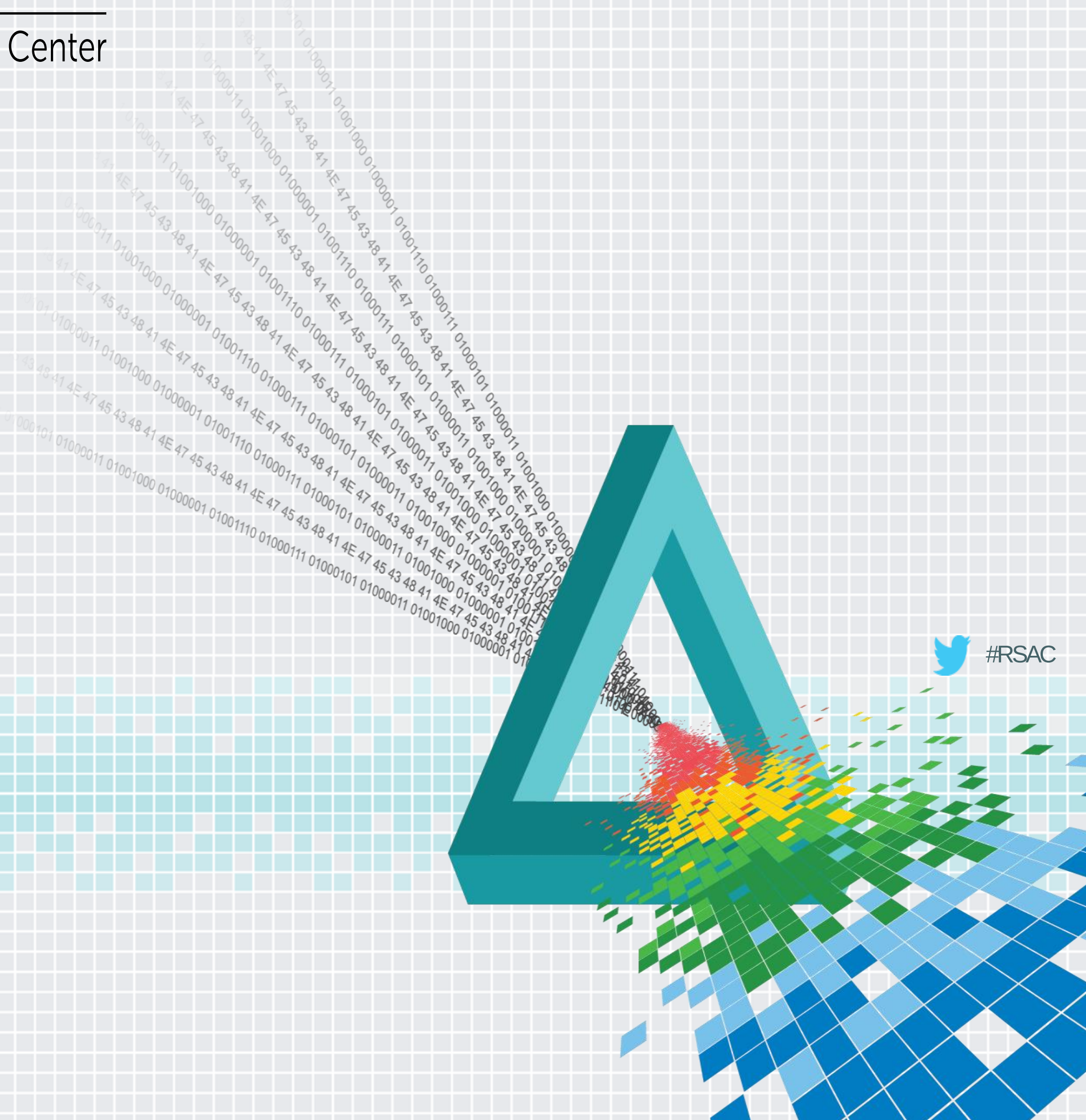
Demo

# Actual Vulnerability Numbers are Higher

- **Awareness**
  - What seems to be about quality might be about security
- **Motivation**
  - Black market
- **Finding a bug in a haystack**
  - 2014 reminded us that bugs can lie undetected for **A LOT** of years

RSA Conference 2015

San Francisco | April 20-24 | Moscone Center



#RSAC

# SSL Bugs

# Implications

- Data decryption
- Data leakage
- Remote control
- Denial of service

**What if the core functions were susceptible to such vulnerabilities?**

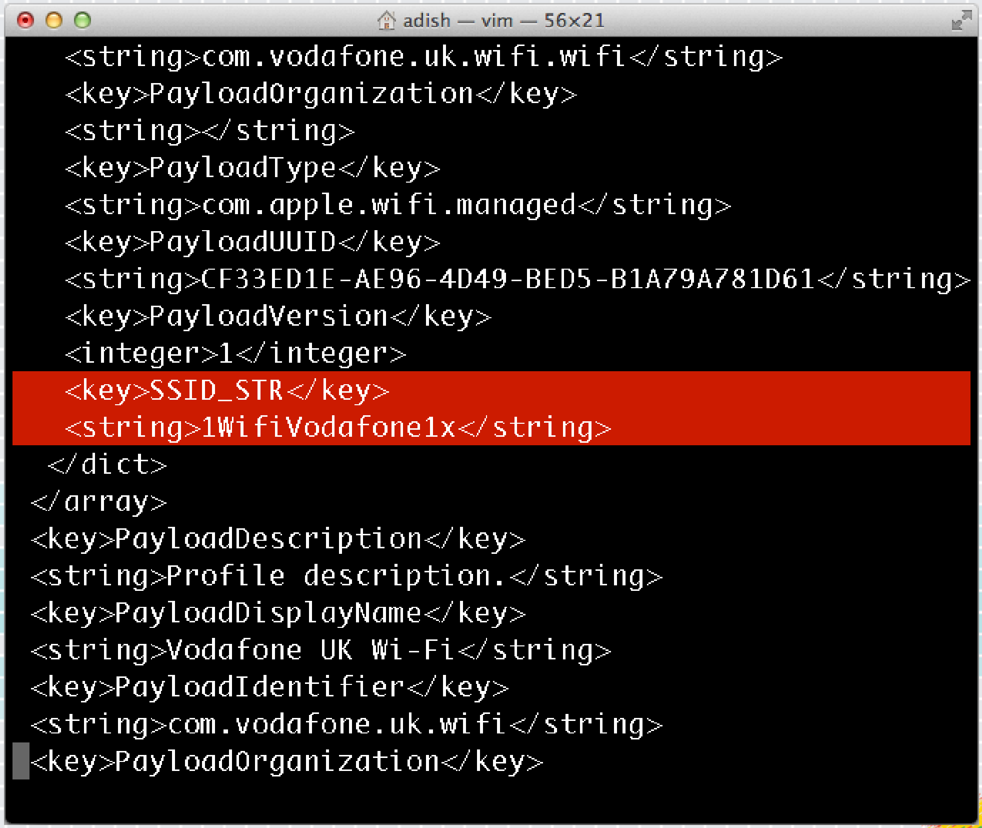
# SSL Certificate Parsing Bug

- Remote application crash (Movie)
- Technical Details

This issue is being Investigated by Apple

# What If You Never Connect to a WiFi?

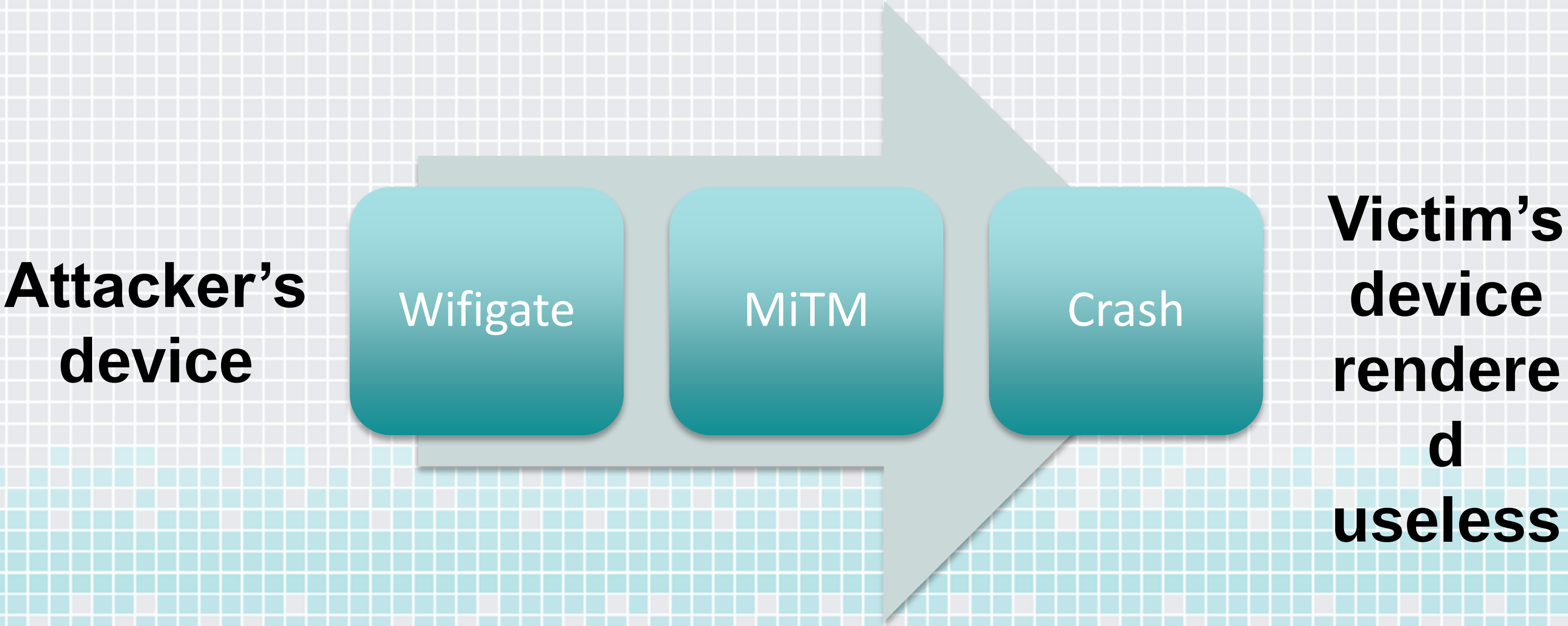
- Are you safe?
  - NO
- The bug can be combined with WiFiGate
- 3G/LTE attacks can also be used



```
  <string>com.vodafone.uk.wifi.wifi</string>
  <key>PayloadOrganization</key>
  <string></string>
  <key>PayloadType</key>
  <string>com.apple.wifi.managed</string>
  <key>PayloadUUID</key>
  <string>CF33ED1E-AE96-4D49-BED5-B1A79A781D61</string>
  <key>PayloadVersion</key>
  <integer>1</integer>
  <key>SSID_STR</key>
  <string>1WifiVodafone1x</string>
 </dict>
</array>
<key>PayloadDescription</key>
<string>Profile description.</string>
<key>PayloadDisplayName</key>
<string>Vodafone UK Wi-Fi</string>
<key>PayloadIdentifier</key>
<string>com.vodafone.uk.wifi</string>
<key>PayloadOrganization</key>
```

# The iOS-Shield

- A nearby attacker (or dedicated hardware) can force the bug via a network interface.



# What’s The Fix?

Pending Apple’s patch release

# So Far…

- We have covered
  - Inception
  - Detection
  - Research
  - Vendor patch

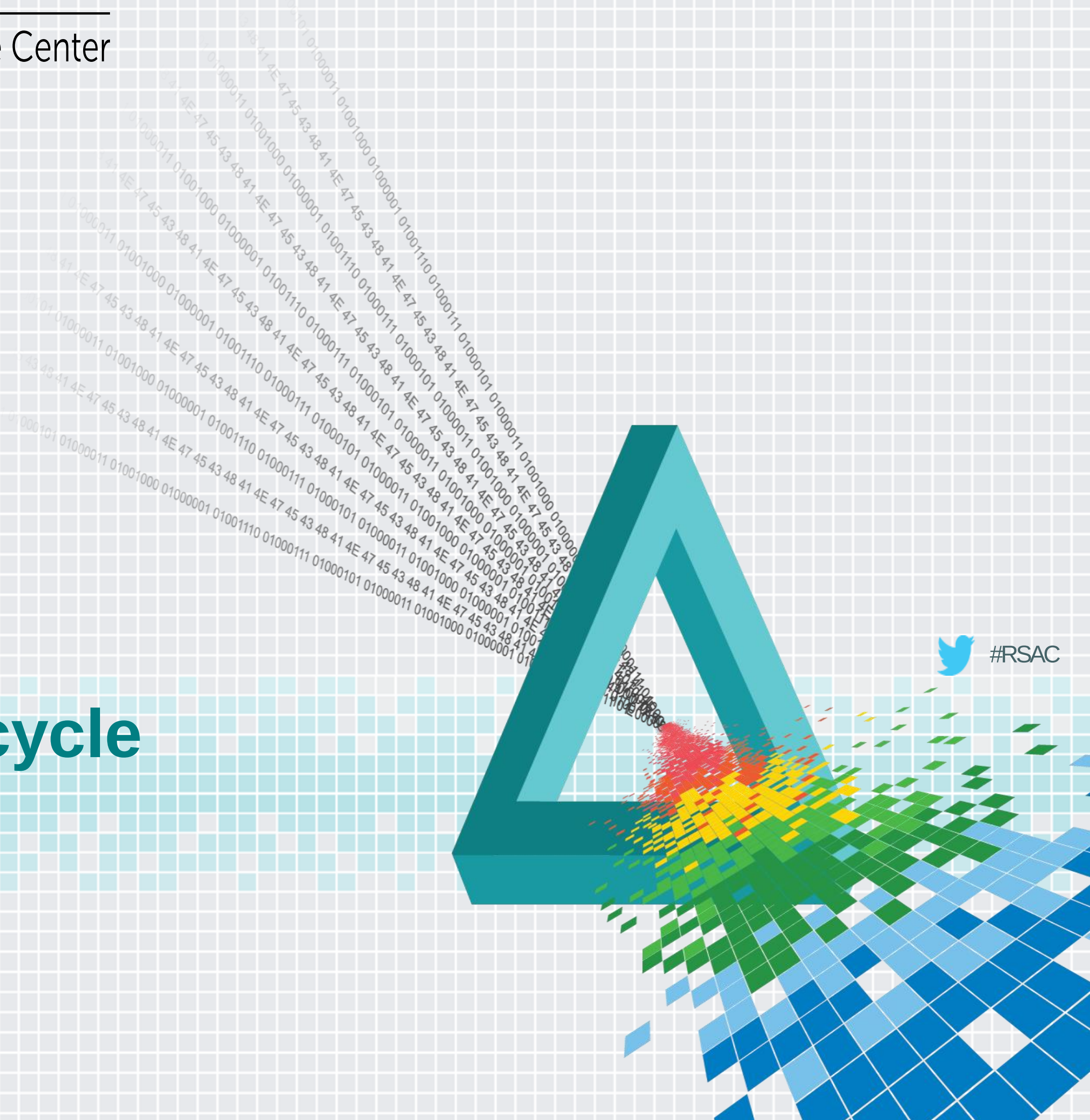
**Does the vulnerability story end here?**

# What About?

RSAConference2015

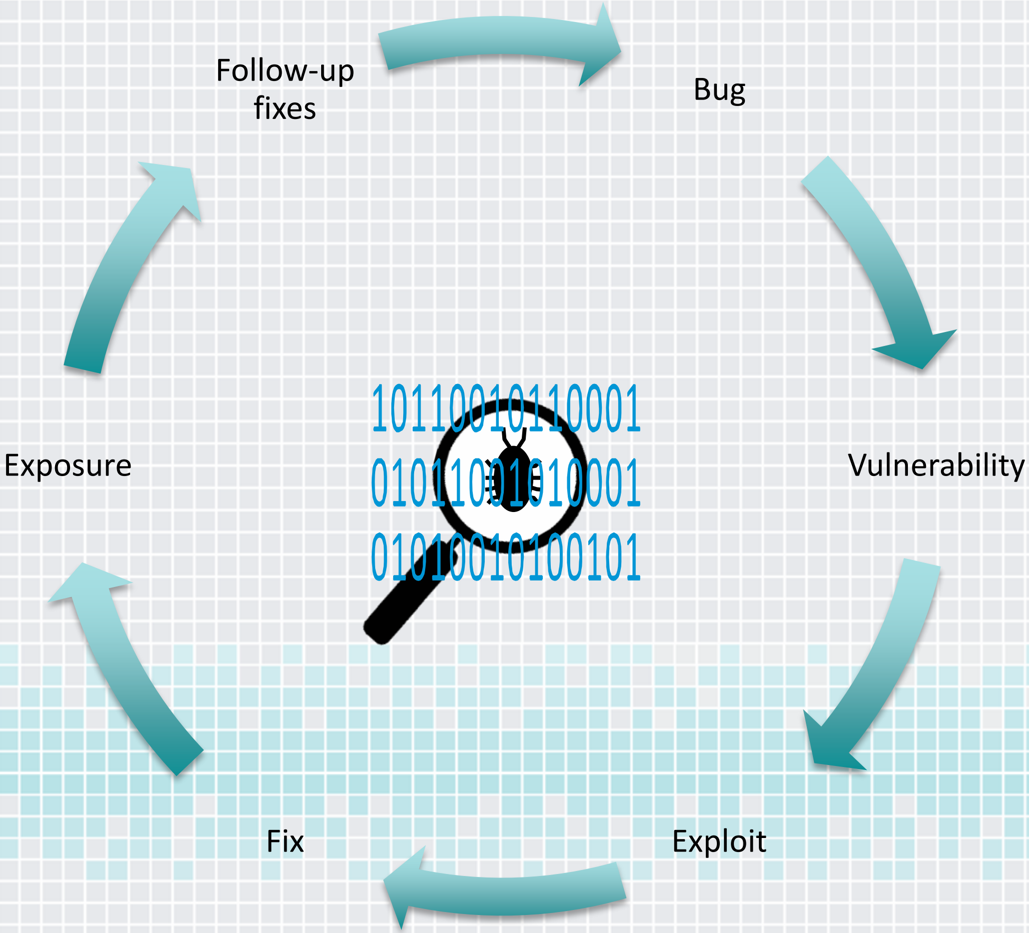
San Francisco | April 20-24 | Moscone Center

# Vulnerability Lifecycle



#RSAC

# Vulnerability Lifecycle



Bug

Vulnerability

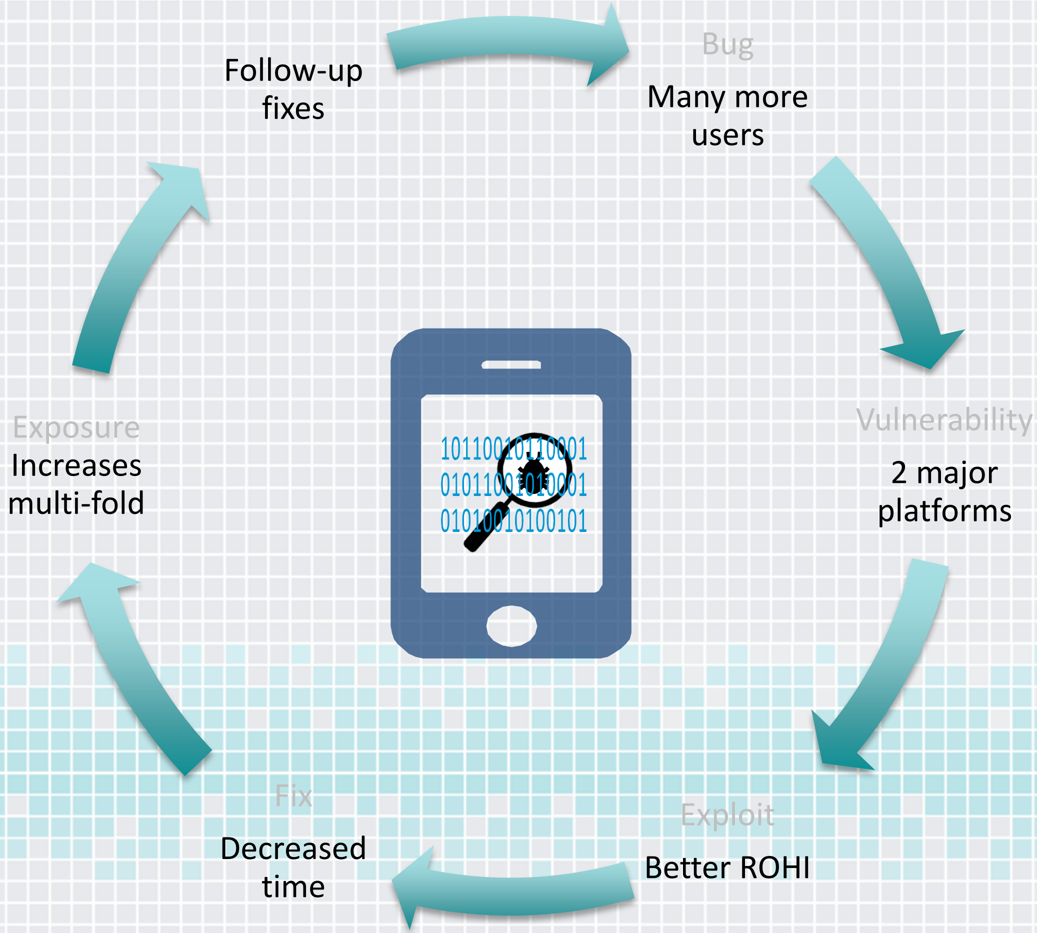
Exploit

Fix

Exposure

Follow-up fixes

# Vulnerability Lifecycle – Mobile



Bug

Many more users

Vulnerability

2 major platforms

Exploit

Better ROHI

Fix

Decreased time

Exposure

Increases multi-fold

Follow-up fixes

You can rest now …
After 18 months of exposure

# Summary

- Mobile security is here to stay
  - Physical
  - Network
  - Malware
  - Vulnerabilities
- System and app level vulnerabilities are on the rise
- OS vendors should employ a multi-platforms oriented vulnerability patching process
- The importance of enterprise mobile defense increases

# Apply What You Have Learned

## Researchers Perspective

- Any bug has the potential to transform into a security issue
  - Be persistent!
- Utilize the public tools offered by the industry to boost your efforts
  - Don’t reinvent the wheel
- Follow responsible disclosure guidelines
  - It is the key for a better functioning world

# Apply What You Have Learned

## Security/Remediation Perspective

- Personal level
  - Maintain an up to date operating-system
  - Update the apps that you are using
  - Be alerted and aware of evolving threats
    - Network layer
    - Third-party app stores
    - OS misconfigurations and vulnerabilities
- Organizational level
  - (Same as above) ^ 2
  - Deploy a mobile threat defense solution for visibility and protection

# Next Steps

contact@skycure.com

https://www.skycure.com

https://blog.skycure.com

@YairAmit, @AdiSharabani, @SkycureSecurity

/Skycure