

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

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

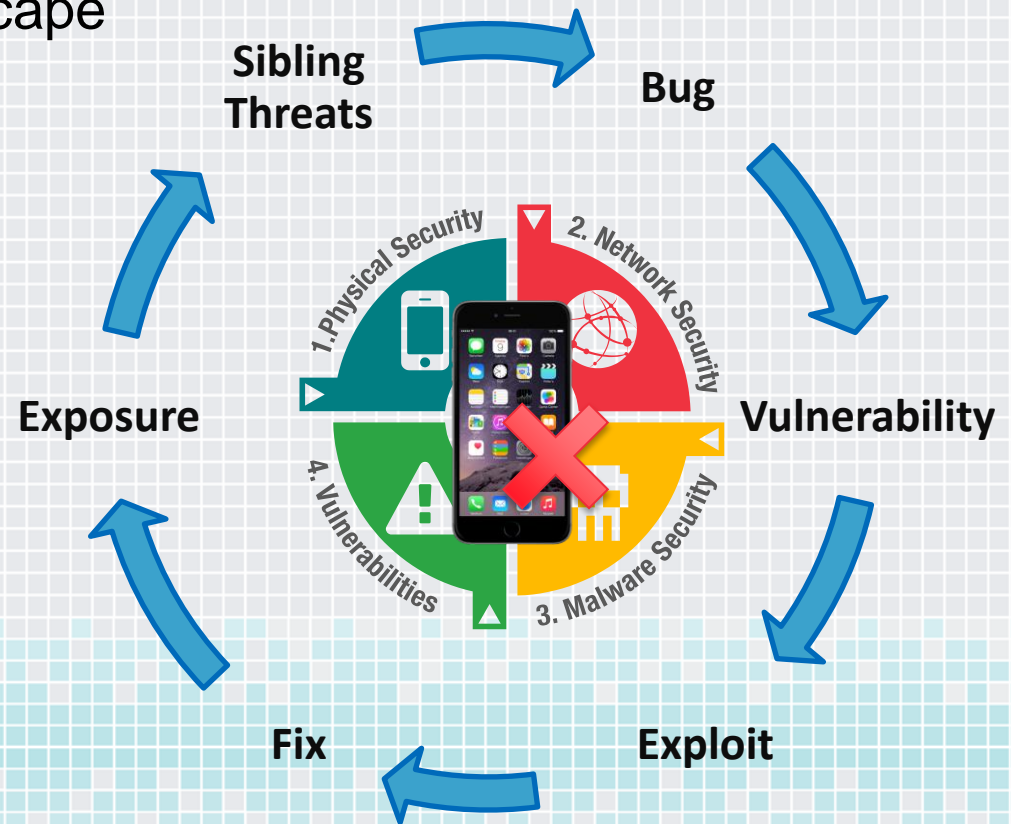
CHANGE

Challenge today's security thinking



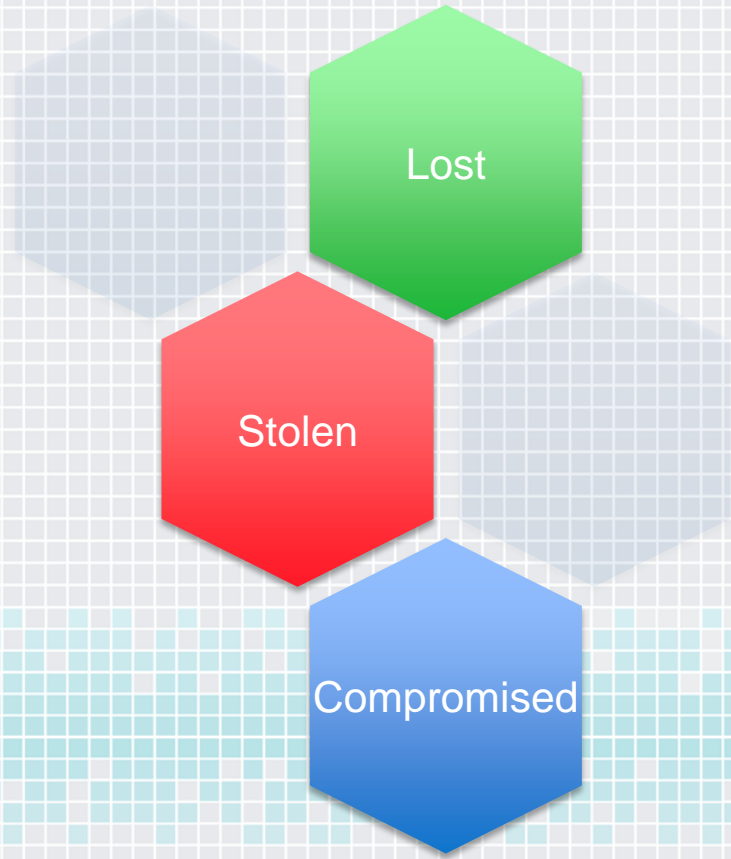
Agenda

- ◆ The Mobile Security Landscape
- ◆ SSL Stack Vulnerabilities
- ◆ No-iOS-Zone Vulnerability
- ◆ The Vulnerability Lifecycle
- ◆ Summary & Apply

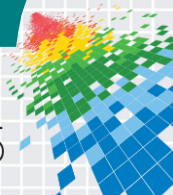


Mobile Security Landscape

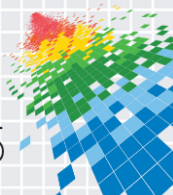
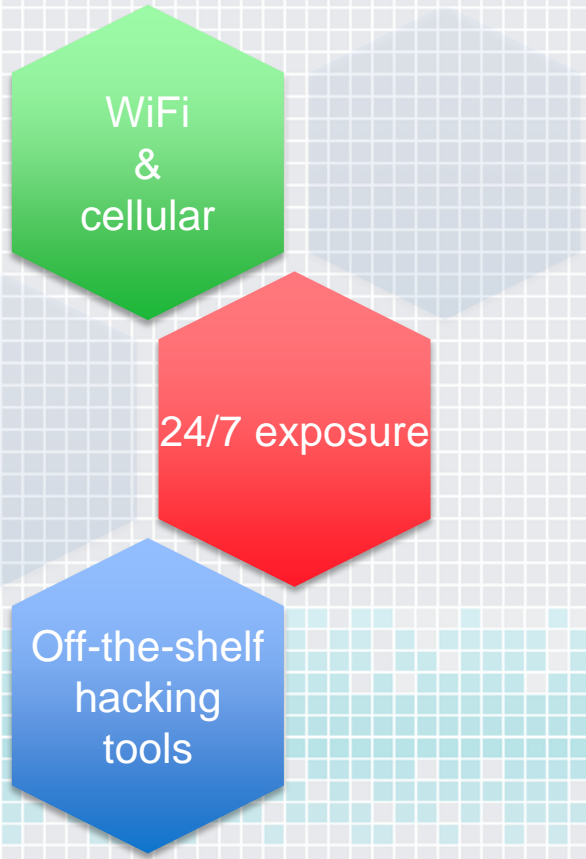




1. Physical Security

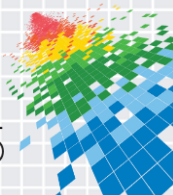
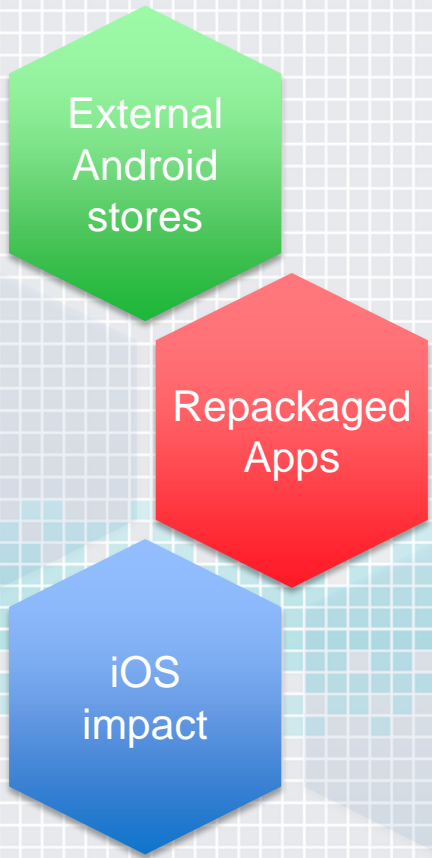


2. Network Security





3. Malware Security

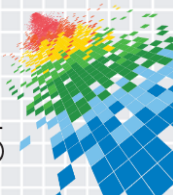




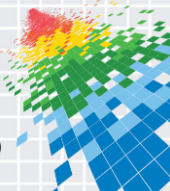
OS
&
app-level

Patching
challenges

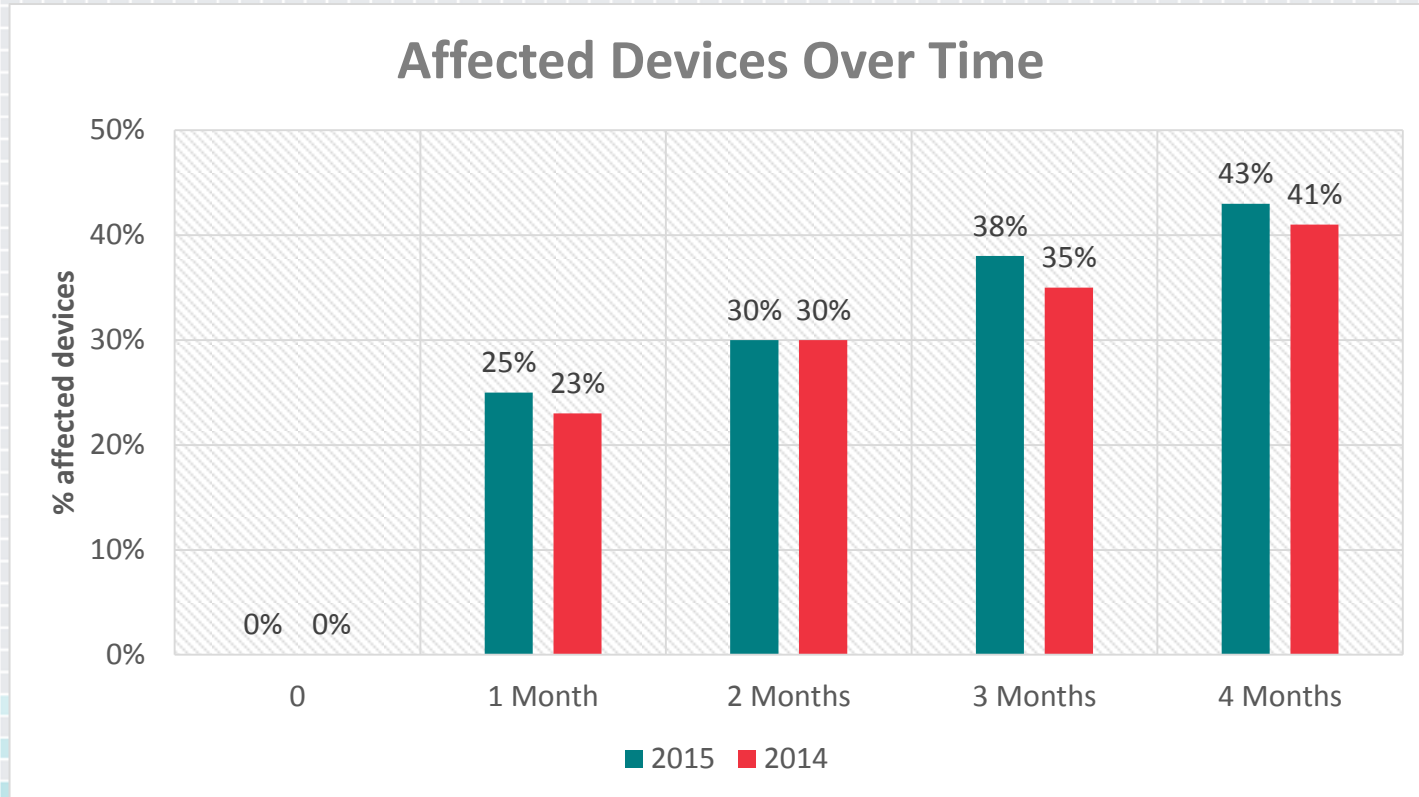
Never-ending
story



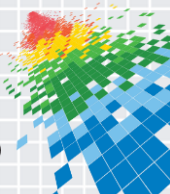
This Presentation's Focus



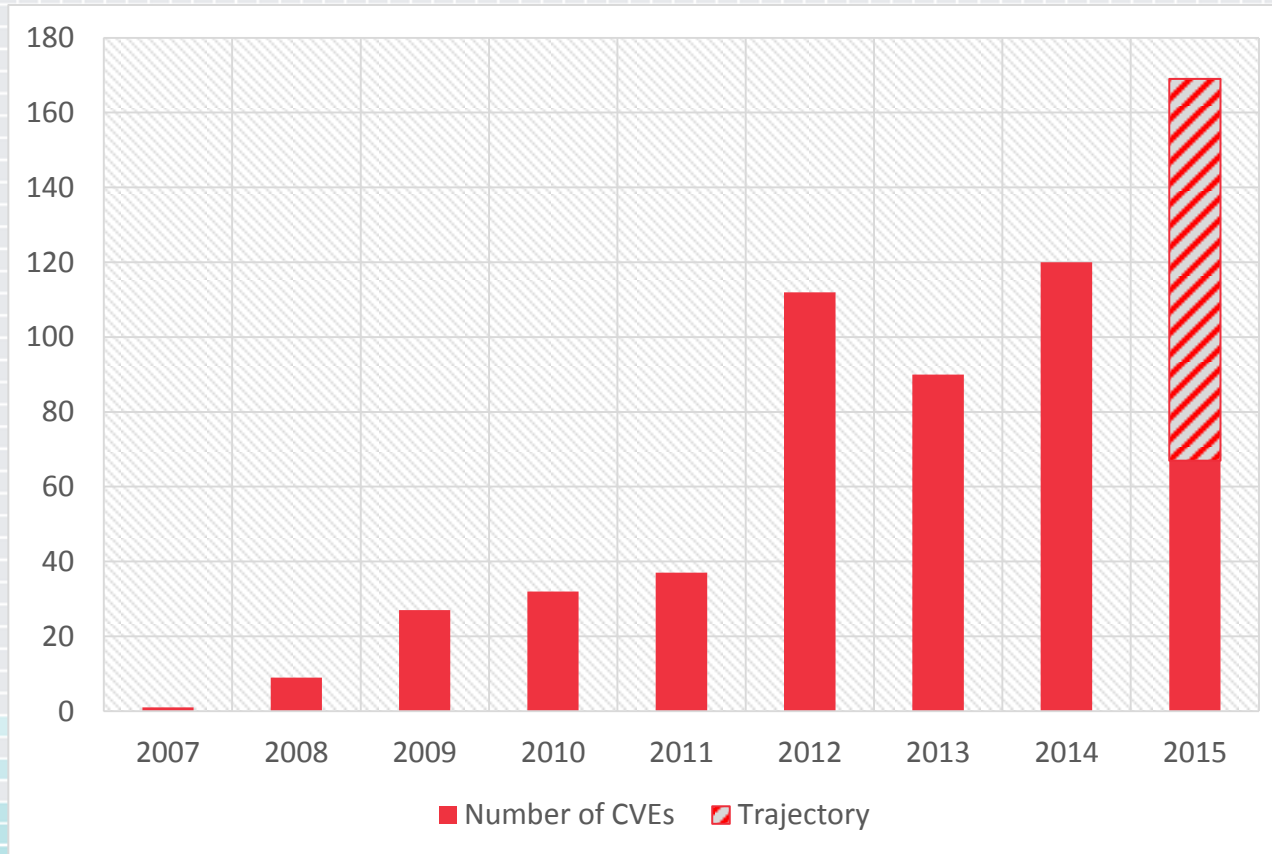
Network Incident Statistics



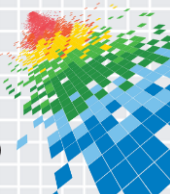
Based on Skycure Threat Intelligence



Known iOS Vulnerabilities (by Year)



Source: Skycure analysis based of CVEdetails.com



Actual Numbers are Higher

- ◆ **Awareness**

- ◆ What seems to be about quality might be about security

- ◆ **Motivation**

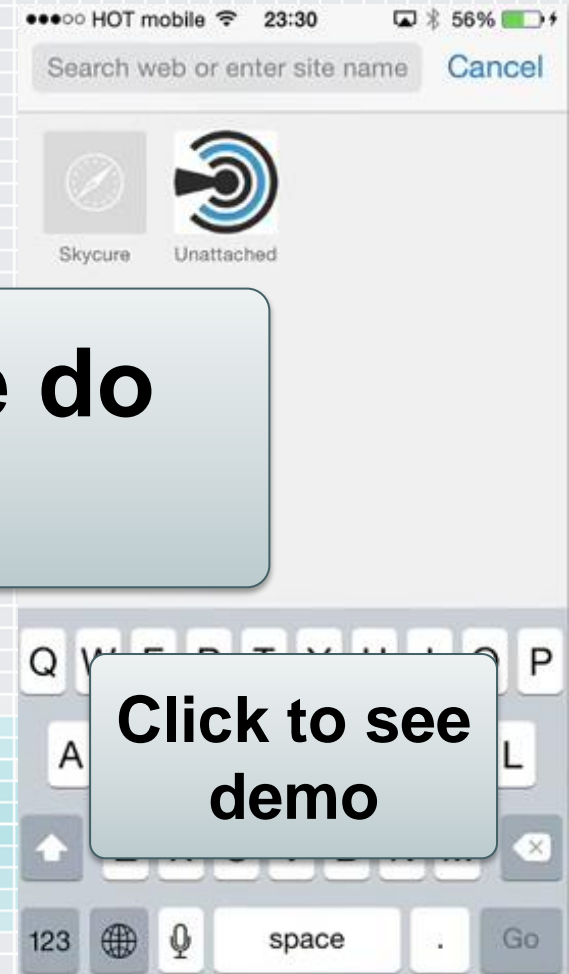
- ◆ Black market

- ◆ **Finding a bug in a haystack**

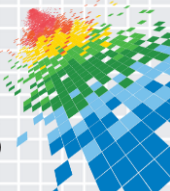
- ◆ 2014 reminded us that bugs can lie undetected for **A LOT** of years



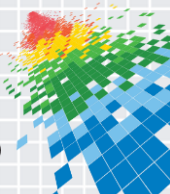
Safari Crash



So... What did we do next?



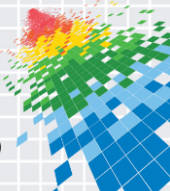
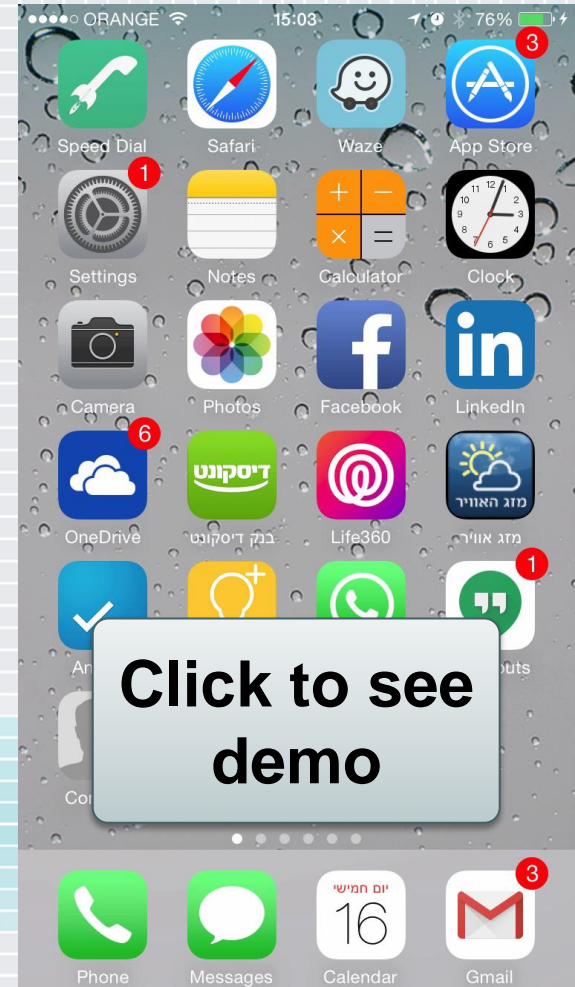
Nothing.



But We Did Research Another Bug...

- ◆ Quick findings:
 - ◆ iOS devices
 - ◆ A specific network
 - ◆ Almost any app crashes

- ◆ Further analysis:
 - ◆ SSL certificate parser bug



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center



SSL Stack Issues

goto fail;

Heartbleed

SSL decryption

...



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;
        goto fail;
    if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
        goto fail;
    err = sslRawVerify(ctx,
                      ctx->peerPubKey,
                      dataToSign,
                      dataToSignLen,
                      signature,
                      signatureLen);
    /* plaintext */
    /* plaintext length */
    ...
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?

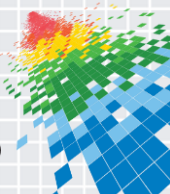
Cancel

Details

Continue

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

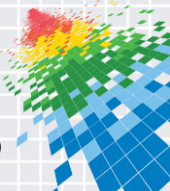
Source: Skycure Threat Intelligence



SSL Bugs - Implications

- ◆ Data decryption
- ◆ Data leakage
- ◆ Remote control

In our case, none of the above was feasible



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

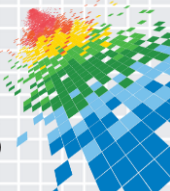
Going back to our crash...



Is This Really Interesting?

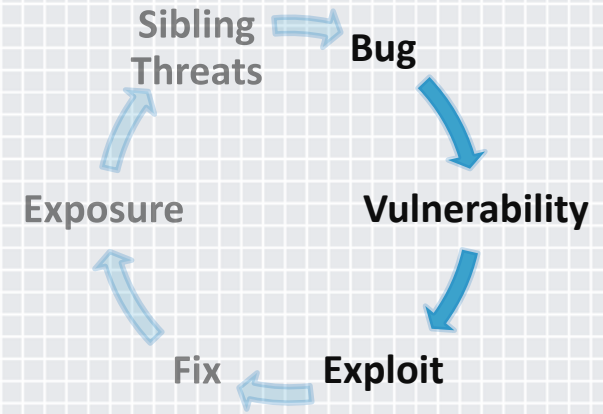
- ◆ Current attack flow:
 - ◆ Attacker creates a malicious “Free Public Wifi” network
 - ◆ Victim connects to the network
 - ◆ All apps constantly crash

- ◆ Problems with the attack:
 - ◆ Victim needs to connect to the malicious network
 - ◆ Victim likely to understand the issue relates to the network
 - ◆ Victim can simple switch to another network to resolve the impact



Is Manual Connection Required?

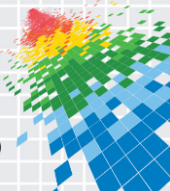
- ◆ WiFi auto connect:
 - ◆ Karma attacks
 - ◆ WiFiGate
- ◆ Cellular attacks:
 - ◆ Fake towers



So, Is This Interesting Now?

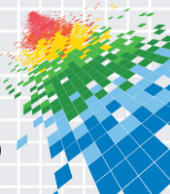
- ◆ Current attack flow:
 - ◆ Attacker forces nearby victims to connect to the malicious network
 - ◆ No victims' action required
 - ◆ Users cannot use any SSL-enabled iOS apps

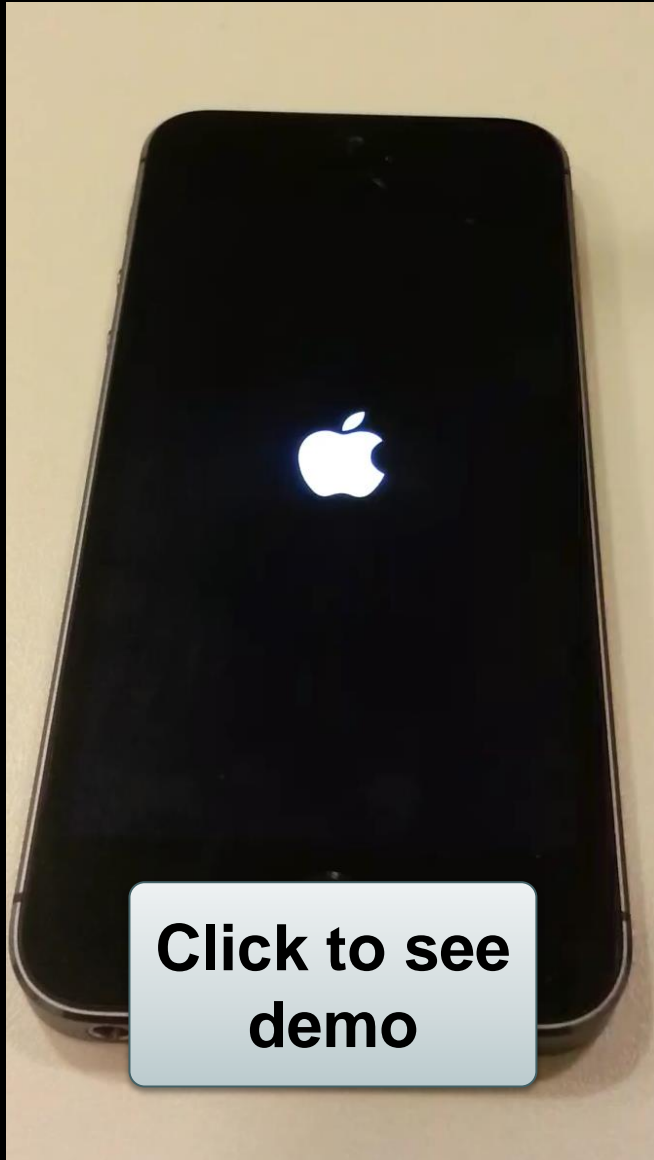
- ◆ Problems with the attack:
 - ◆ Victims can still determine the attack is associated with the network
 - ◆ Victims can move to “airplane mode” or switch to another network



But What About the OS?

- ◆ Unsurprisingly, iOS system processes also use SSL 😊
- ◆ Impact: iOS crash





iOS crashes

Device restarts

iOS Bug exploited again

iPhone crashes again

and again

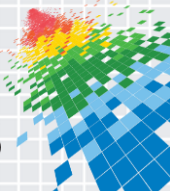
and again

and again

So, Now it is Interesting...

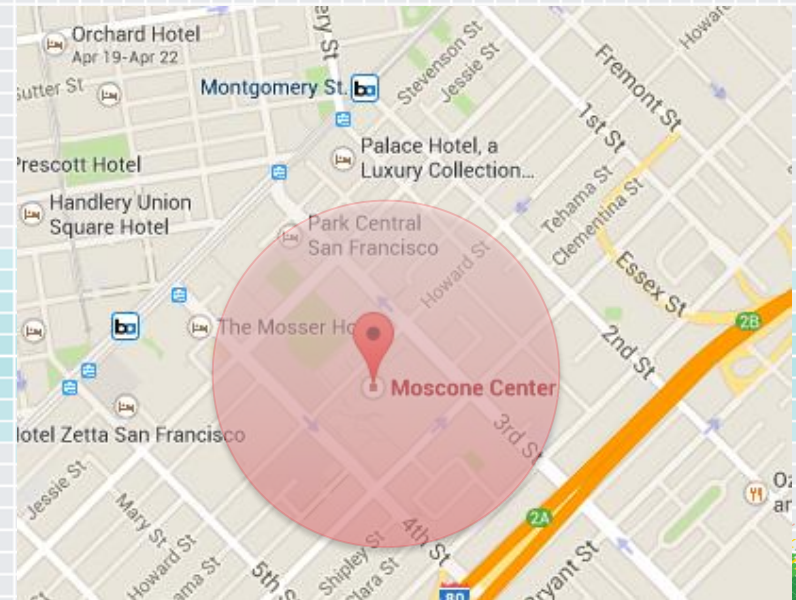
- ◆ Current attack flow:
 - ◆ Attacker forces nearby victims to connect to the malicious network
 - ◆ No victims' action required
 - ◆ iOS devices in range could get into a DoS restart loop

- ◆ Result:
 - ◆ No-iOS Zone

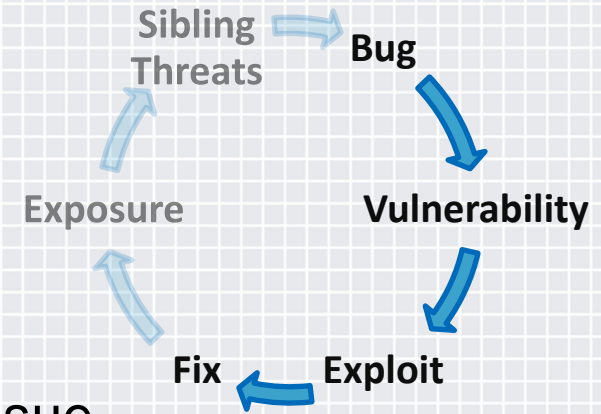


“No-iOS Zone” Attack

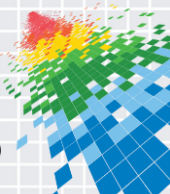
- ◆ iOS users in range are unable to use their mobile devices
 - ◆ No WiFi, no offline work, no phone calls, no airplane mode...
- ◆ Potential areas that may be attractive for attackers:
 - ◆ Political events
 - ◆ Economical & business events
 - ◆ Wall Street
 - ◆ Governmental and military facilities



Disclosure & Fix Process



- ◆ Issue reported to Apple on Oct. 2nd, 2014
- ◆ We have been working with Apple to fix the issue
- ◆ 8.3 release seem to resolve some of the issues
- ◆ The threat has not yet been confirmed as resolved
- ◆ We will update more on our blog:
 - ◆ <https://blog.skycure.com>



HTTP Request Hijacking

Disclosed by Skycure
at RSA Europe 2013

```
- (void)fetchArticles
```

```
NSURL *serverUrl =
```

```
[NSURL URLWithString:@"http://journal.skycure.com"]
```

```
NSMutableURLRequest *request =
```

```
[NSMutableURLRequest requestWithURL:serverUrl];
```

```
[request setValue:@"application/json"  
forHTTPHeaderField:@"Content-Type"]
```

```
self.connection =
```

```
[NSURLConnection initWithRequest:request delegate:self];
```

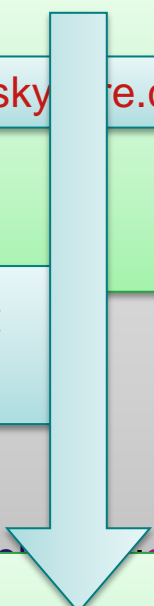
```
NSURL *serverUrl =
```

```
[NSURL URLWithString:@"http://attacker.site/skycureJournal"]
```

```
NSMutableURLRequest *request =
```

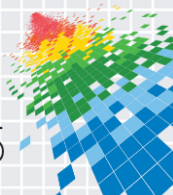
```
[NSMutableURLRequest requestWithURL:serverUrl];
```

HTTP Request
Hijacking



Further Research

No-iOS
Zone + HRH = No-iOS



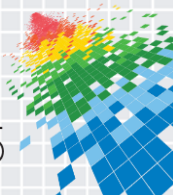
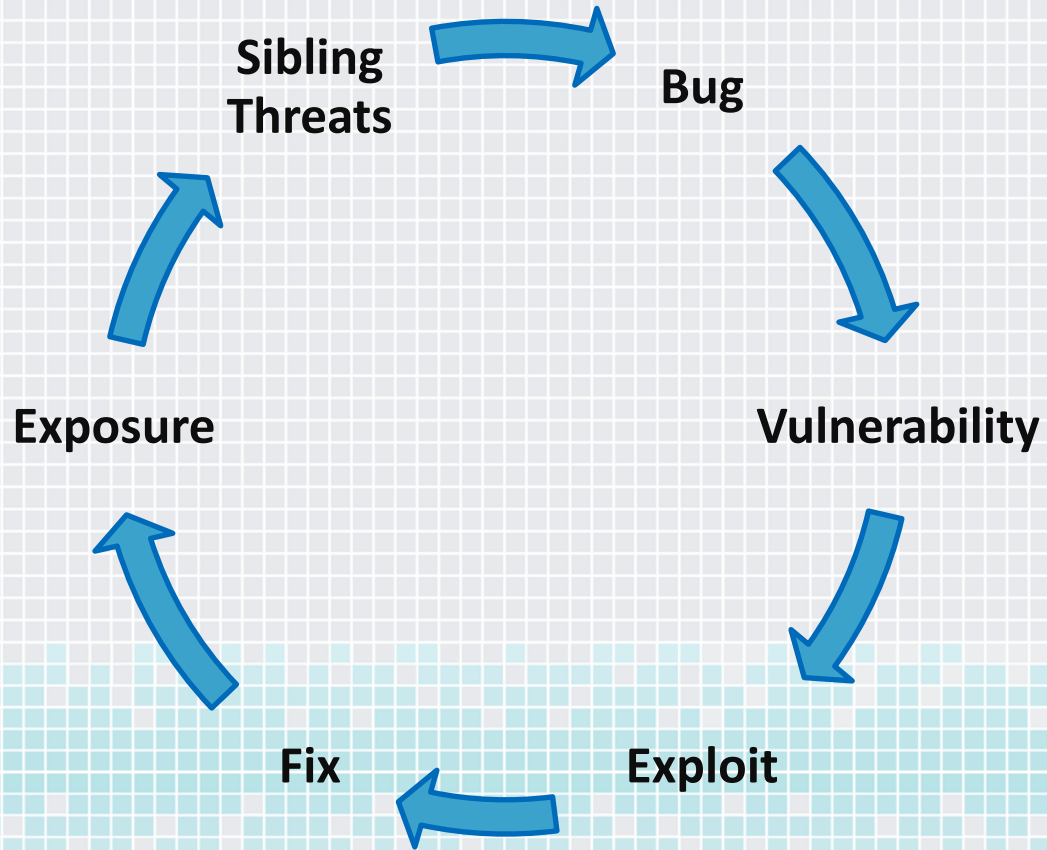
RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Vulnerability Lifecycle



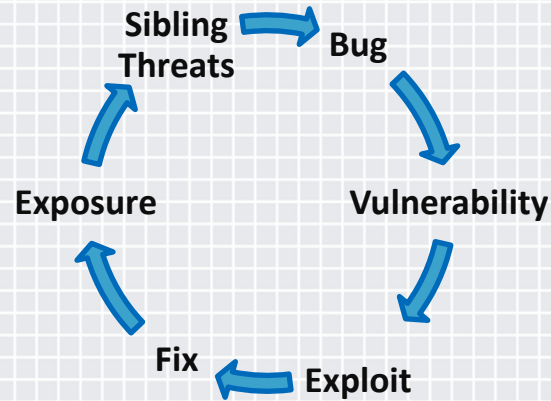
Vulnerability Lifecycle



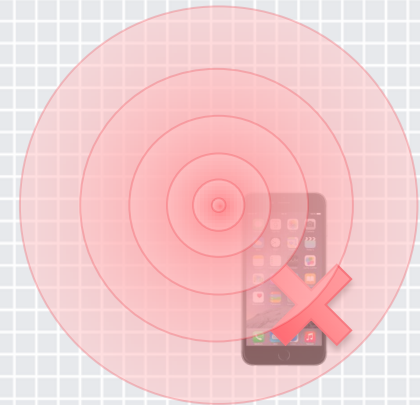
Summary



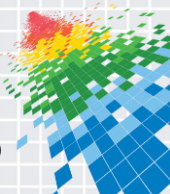
Mobile Security Landscape



The Vulnerability Lifecycle

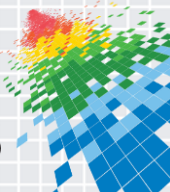
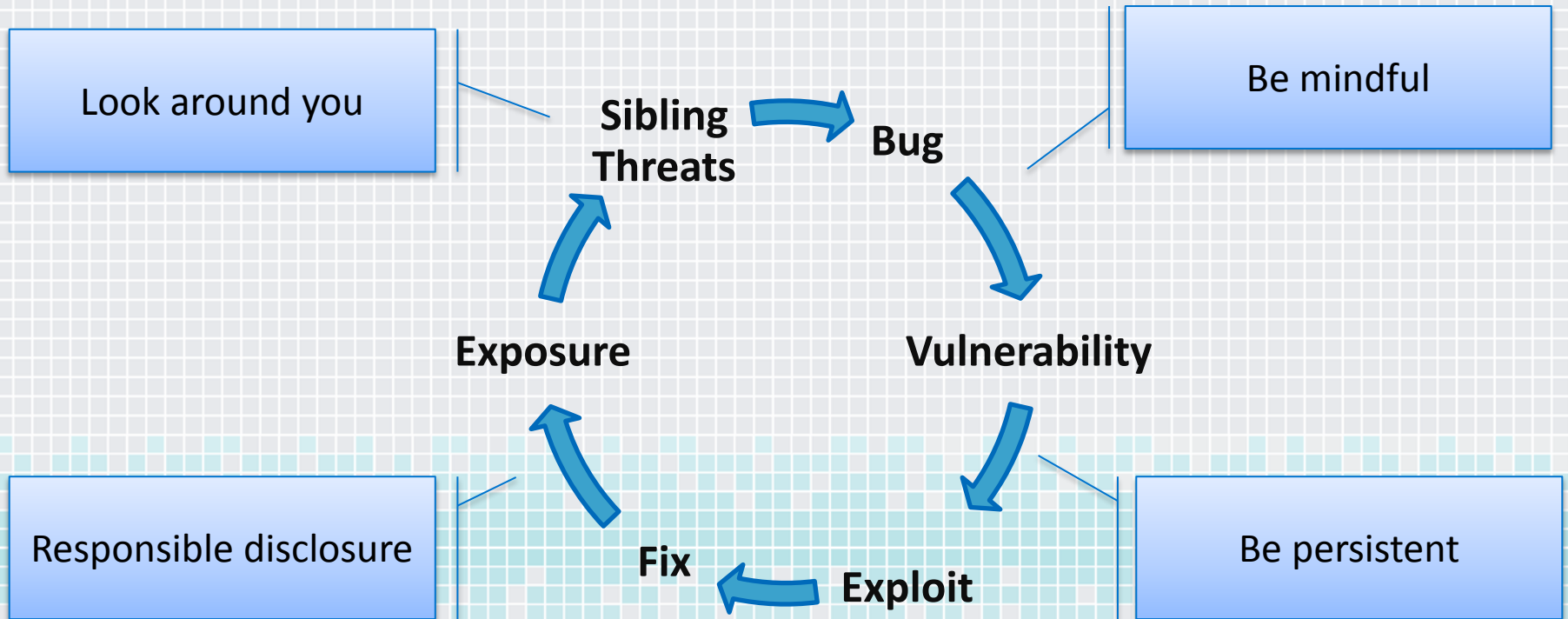


No-iOS Zone Vulnerability



Apply What You Have Learned

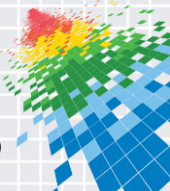
Researchers' Perspective



Apply What You Have Learned

Security/Remediation Perspective

- ◆ Personal level
 - ◆ Updates (both OS & apps)
 - ◆ Awareness (mobile threats are constantly evolving)
- ◆ Organizational level
 - ◆ (Same as above)²
 - ◆ Deploy a mobile threat defense solution for visibility and protection
- ◆ Vendors
 - ◆ OS vendors should employ a multi-platforms oriented vulnerability patching process



Next Steps



contact@skycure.com



<https://www.skycure.com>



<https://blog.skycure.com>



[@YairAmit](#), [@AdiSharabani](#), [@SkycureSecurity](#)



[/Skycure](#)

