RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-W10

Anatomy of an Enterprise Mobile Security Incident

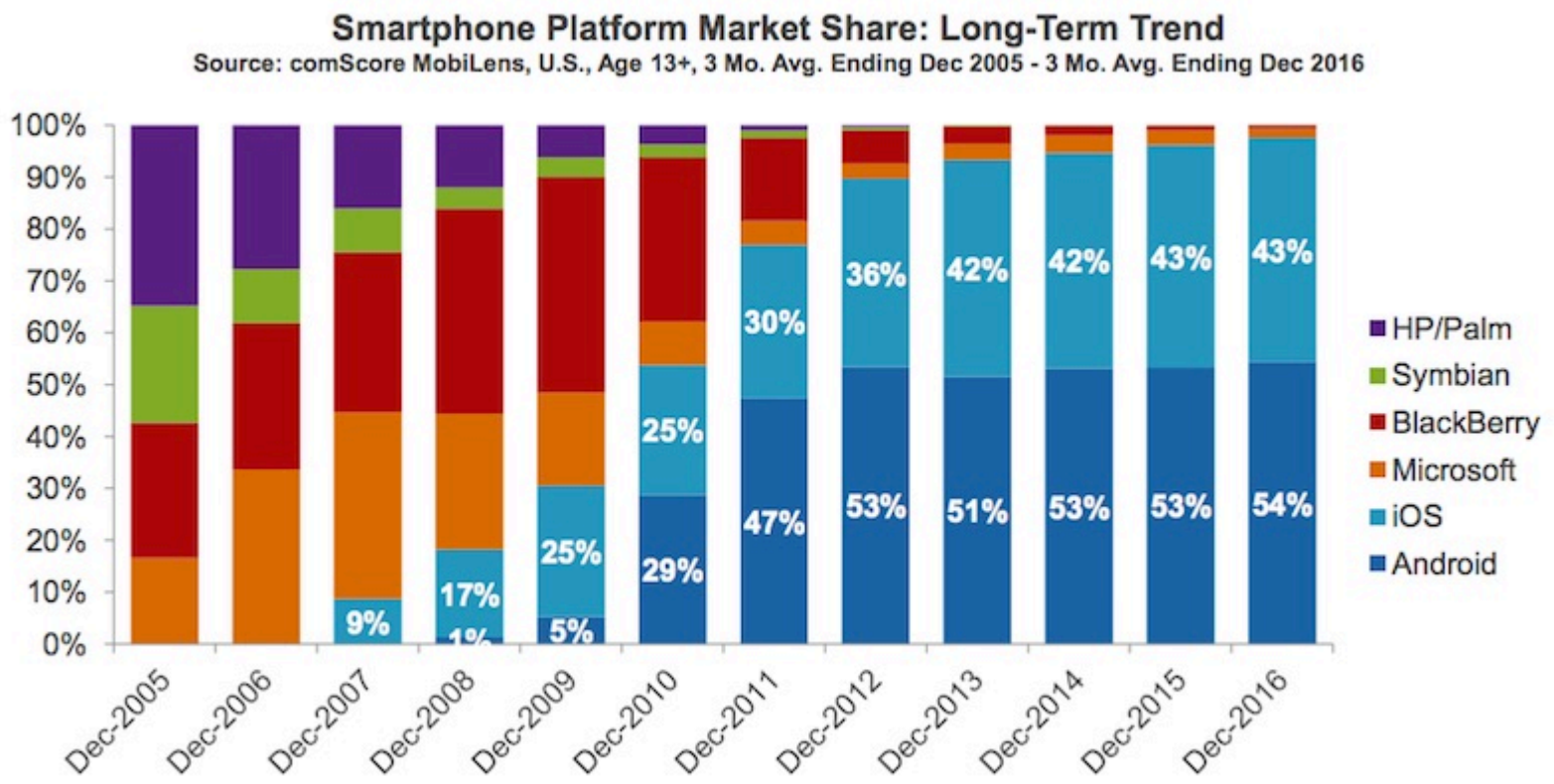
Aaron Turner
CEO – Hotshot
@AARONRTURNER

Session Outline

- The price of mobile complacency
- Understanding the enterprise mobile ecosystem
- The Venn Diagrams of Mobile Security Doom
- Step-by-step recreation efforts
- Mobile security tool evaluations
- Recommendations and roadmaps

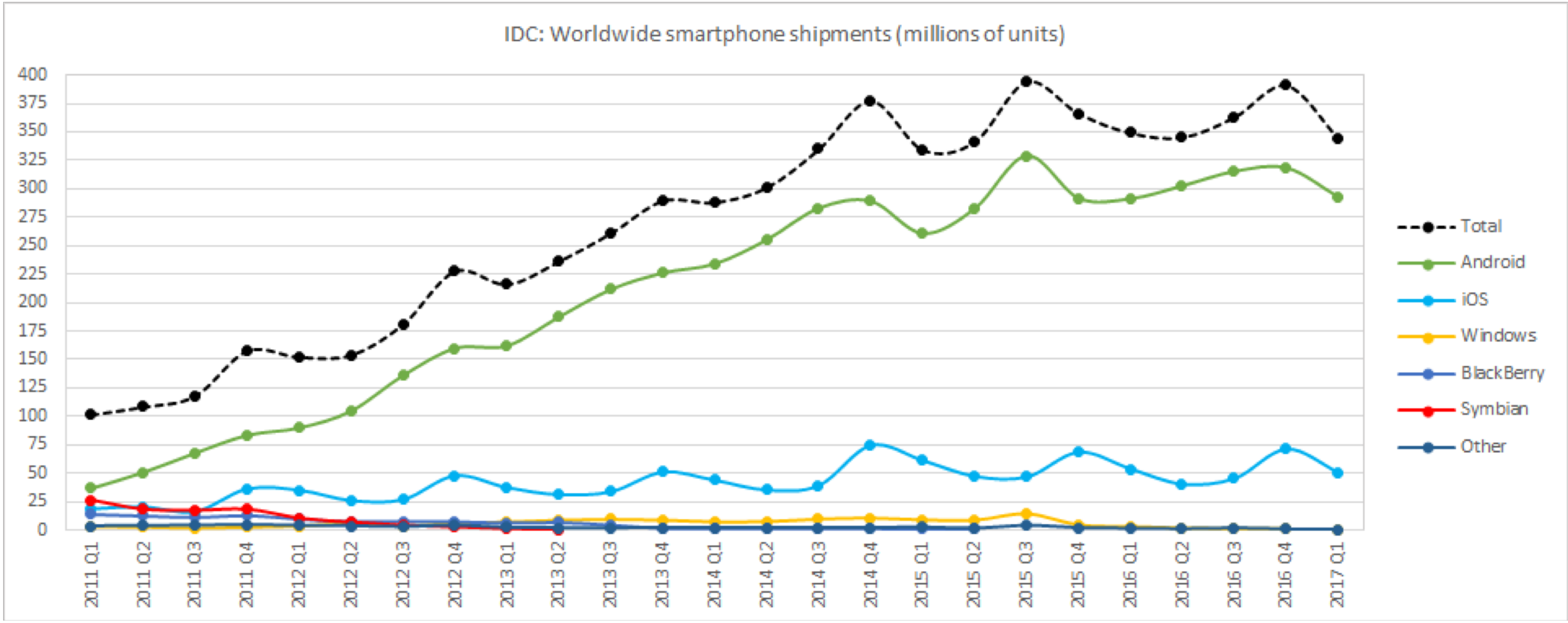
20 years of Enterprise Mobility

- One chart that pretty much tells the story of why enterprise mobile security is so awful today



Credit: comScore MobiLense

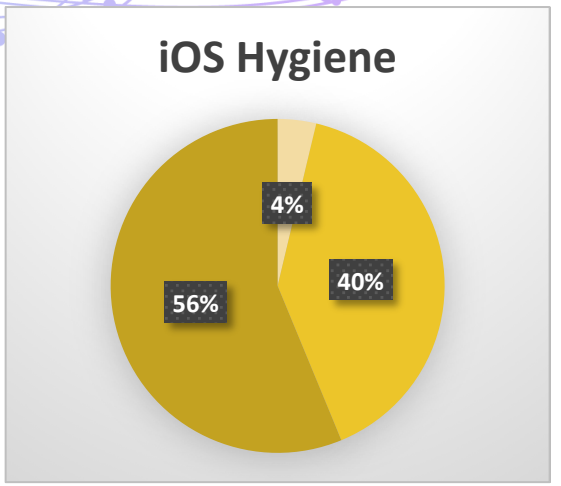
The Global View



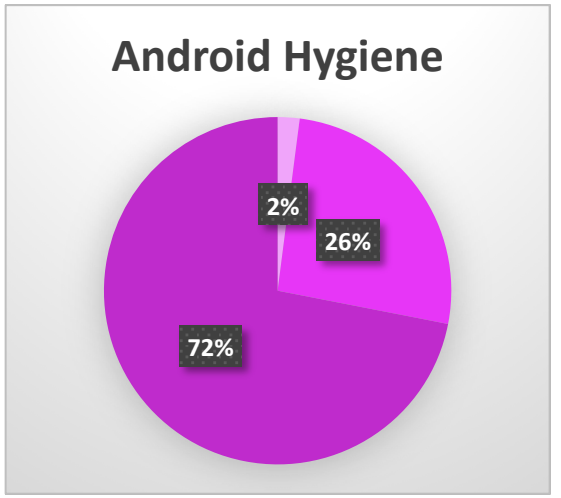
Enterprise Mobile Situation

- Among US knowledge workers in information-centric businesses, iOS continues to dominate
- Among global manufacturing, logistics, hospitality and retail customers, Android is king
- Both platforms suffer terribly from hygiene problems
  - 56% of enterprise-connected iOS devices are vulnerable to commodity exploits

4% - up-to-date
40% - 60 days
56% - >60 days



2% - up-to-date
26% - 60 days
72% - >60 days

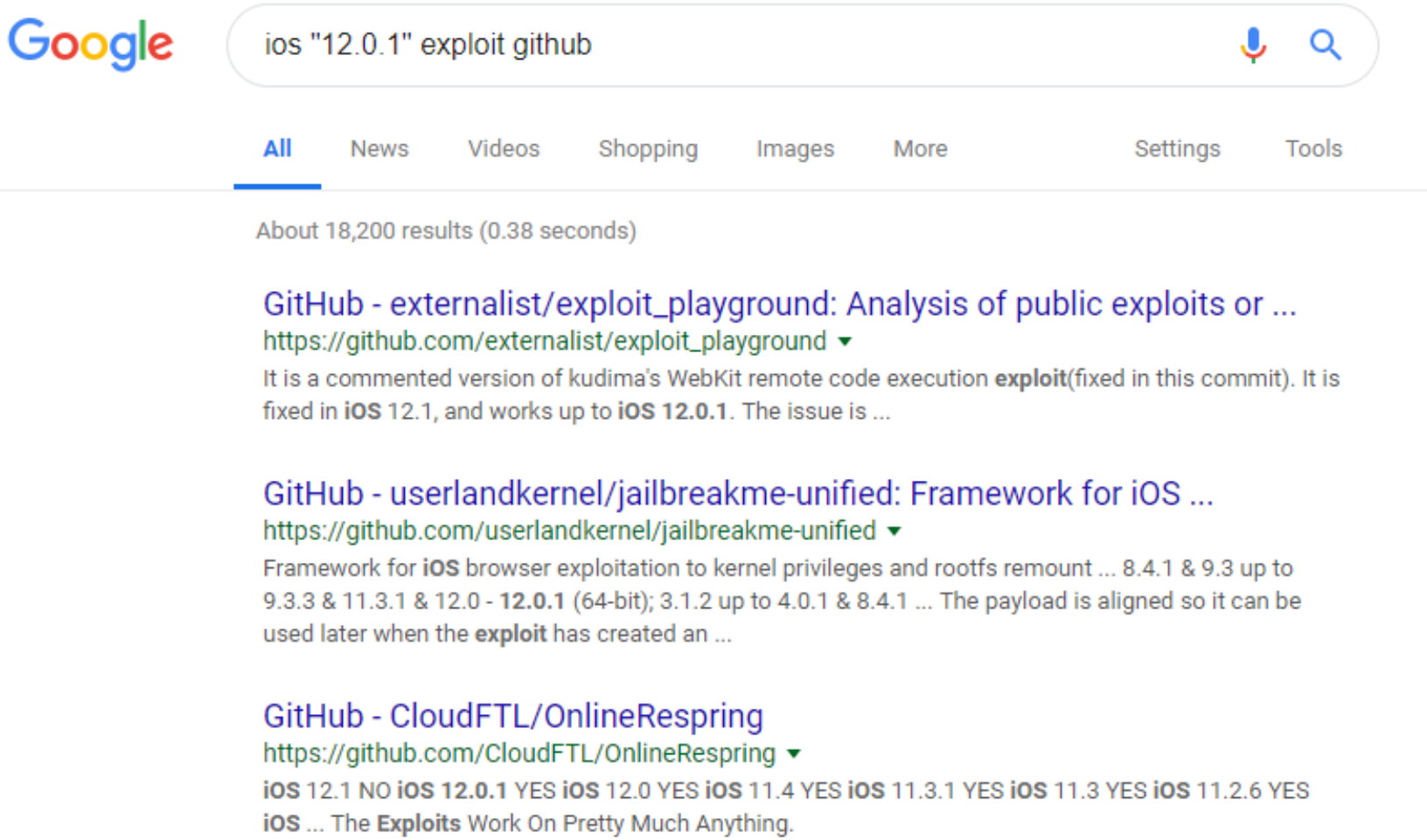


Data based upon IANS Research mobile security assessments
https://www.iansresearch.com

IANS

What is an iOS 'Commodity Exploit'?

- LMGTFY
- A non-persistent exploit/jailbreak
- Useful to get temporary access to iOS kernel
  - And all data and credentials as well



The Incident

- Global enterprise conglomerate, more than 50,000 employees worldwide
- Office 365 Global Admin travels to hostile country
- Global Admins are only required to use soft tokens while on untrusted networks
- Staff member returns to the US
- Office 365 badness ensues

The Aftermath

- No IoC's on Global Admin's Laptop
- No IoC's on Global Admin's iPhone
- But…
  - Clear evidence of unauthorized Office 365 activity and privilege abuse
- Zeroing in on the iOS device:
  - More than 60 days out-of-date, vulnerable to more than 10 exploits at the time staff member was traveling in hostile country
  - As soon as the staff member's credentials were reset and MFA soft token revoked and reissued, unauthorized access ceased

Zeroing in on the iOS device

- More than 60 days out-of-date
- Vulnerable to more than 10 exploits at the time of travel
- Credential reset and soft-token revocation and redeployment resulted in immediate stop to Office 365 privilege abuse

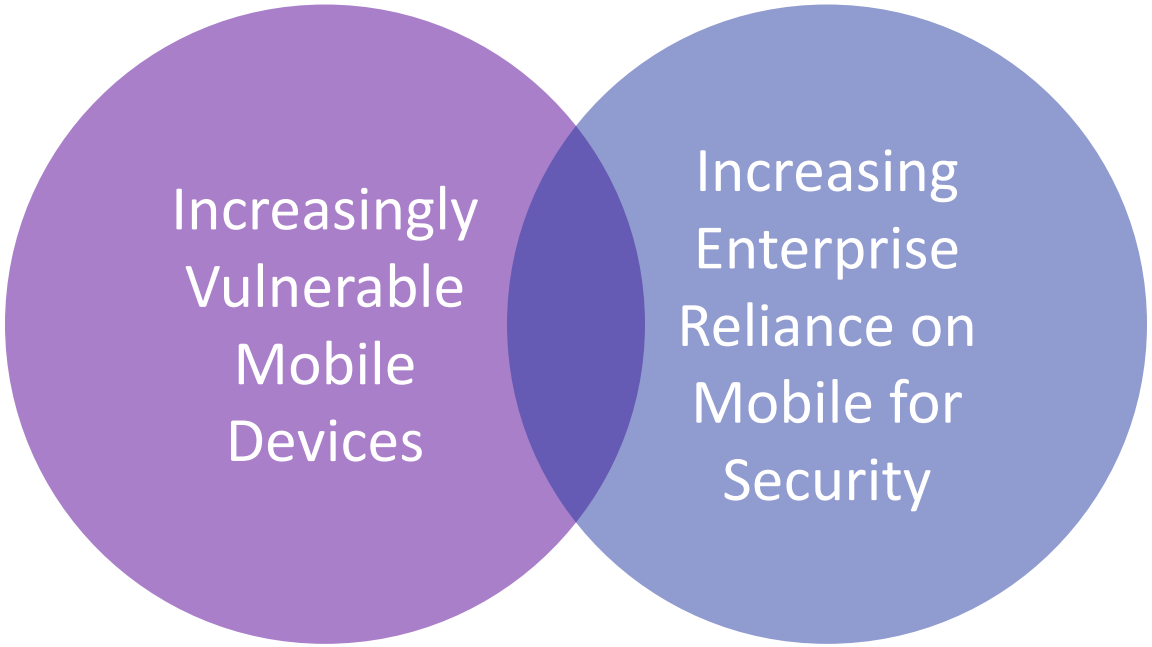
Trying to Explain the Unexplainable

- Client asks team to create a report outlining potential ways that the scenario could be explained
- Collaboration among a group of iOS and Office 365 experts yields a theory:
  - Staff member was targeted with iOS exploit while in hostile country
  - Non-persistent jailbreak uses kernel vulnerability to gain access to stored credentials and cryptographic secrets in iOS keychain
  - Attackers inject stolen credentials and cryptographic secrets into attack device, essentially cloning user's credentials and MFA soft token
  - Evidence of the attack deleted when iOS device is rebooted

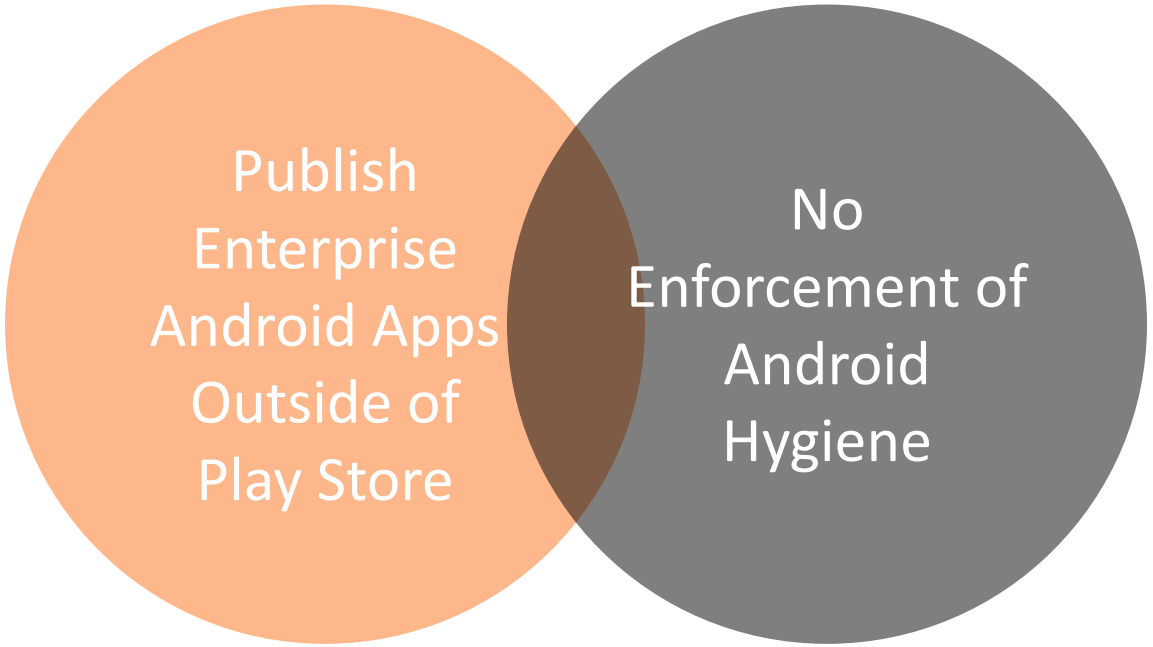
This is not supposed to happen!

- Nearly all vendors offering soft token solutions claim to leverage iOS's secure enclave encryption facility
  - The secure enclave is essentially a cryptographic co-processor which helps improve the integrity of encryption operations on iOS devices
    - For more information, read the 'Storing Keys in the Secure Enclave' article in the Apple developer documentation
- Soft tokens store secret data in keychain locations which can expose soft tokens to remote attacks
- Result: a kernel-mode exploit could successfully steal the MFA soft token secrets, clone them to an attacker device and the back-end system would be none the wiser

Mobile Security Venn Diagrams of Doom



Fortune 1000 Mobile Trend



Top 5 Financial Services Org

The Mobile Identity Problem

- When you don’t enforce any sort of software integrity on mobile endpoints, but…
- Implement software-based systems to attempt to drive integrity into identity and access processes…
- Bad things are going to happen

Mobile security tools will help!

- MAM, MDM, MTD… to the rescue!
  … or not...

What can you do to a vulnerable iPhone with MTD installed?

- A remarkable amount of badness
- IANS Research evaluated two market-leading MTD platforms through a series of penetration tests
- Rules of the game: Target devices had to be 60 days out-of-date (in-line with 60% of this customer's mobile fleet)
- The worst-case scenario:
  - IANS successfully compromised one MTD's VPN credentials and injected an unauthorized root of trust into the certificate store

iOS Function Evaluation	1	2
Kernel execution		
Operating memory protection		
File system integrity		
Security secret store integrity		
Cryptographic store integrity		
Application execution integrity		
Physical-layer network integrity		
Application-layer network integrity		

MTD Detection Failed	
MTD Detection Failed but slight advantage	
MTD Detection Succeeded	

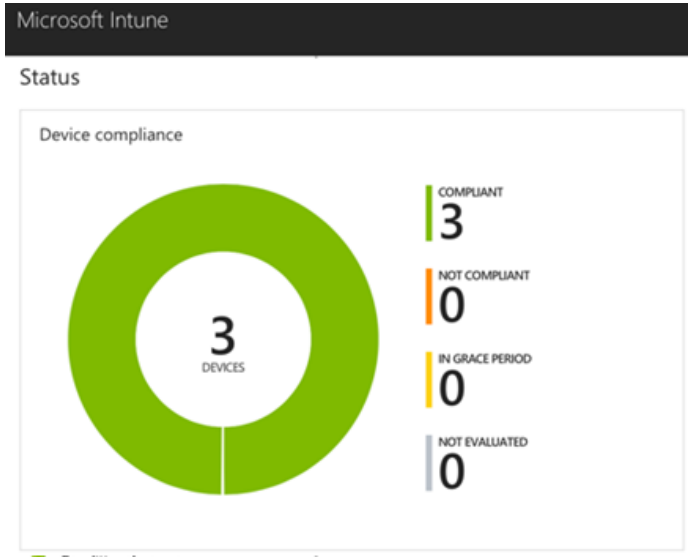
```
Type: "Generic Password"
Account = "Password1"
Access Group = "DPT4QME9Y6.com[redacted]
Creation Date = "2018-02-09 18:27:07 +0000"
User Defined Attribute: Password1
Modified Date = "2018-02-09 18:27:07 +0000"
Accessible: "When Device is Unlocked"
Service: VPN Service
Password: Password1
```

What can you do to a vulnerable mobile device with InTune?

- When you have a kernel-mode exploit, application/user controls are not effective AT ALL
- IANS Research coordinated review of both iOS and Android devices managed by InTune

Function Evaluation	iOS	And.
Kernel execution		
Operating memory protection		
File system integrity		
Security secret store integrity		
Cryptographic store integrity		
Application execution integrity		
Physical-layer network integrity		
Application-layer network integrity		

InTune Security Detection Failed	
InTune Security Detection Succeeded	



Vulnerability Management on Mobile is Important!

- Groundbreaking research:
  - Installing security updates on mobile devices significantly reduces the risks associated with attacks on mobile devices
- There are really only 2 paths forward at this time:
  - iOS: only allow iOS devices to connect to enterprise resources if they have the latest security updates
  - Android: only allow Pixel or Android One devices to connect to enterprise resources if they have the latest security updates

Once updates are installed, key policies to enforce

- iOS security policies
  - Prohibit untrusted TLS certificates
  - Block documents in unmanaged apps
  - Treat AirDrop as unmanaged destination
- Android security policies
  - Only allow Android for Work capable devices
  - Block sharing from work to personal profile
  - Prevent users from manually adding or removing work profiles
  - Enforce Verify Apps for work and personal profiles

But none of these matter on a vulnerable mobile device!