RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **MBS1-W02**

Mobile MFA Madness: Mobile Device Hygiene and MFA Integrity Challenges

Aaron Turner

President & Chief Security Officer
HighSide, Inc.
LinkedIn: https://www.linkedin.com/in/aaronrturner/

Georgia Weidman

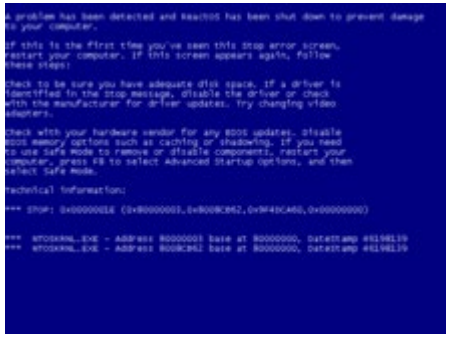
Founder & Chief Technology Officer
Shevirah, Inc.
LinkedIn: https://www.linkedin.com/in/georgiaweidman/

Session Preview

- A bit of history about MFA – how did we get here?
- Mobile MFA by the numbers – how big is this problem?
- Recent enterprise incidents involving mobile MFA
- How hard is it to compromise mobile MFA?
- Demonstrations
- Action Plans

A Brief History of Multi-Factor Authentication

- Connected tokens – Smart Cards, etc.
- Disconnected tokens – RNG's
- Windows NT 3.51 was the first enterprise-class smartcard & RNG integration
  - GINA replacement – LOTS OF BLUE SCREENS!
- US Government CAC/PIV initiative – 1999-2001
- Google's BeyondCorp initiative driving additional awareness



MFA Failures

- Early 2000's – MFA increased security-related helpdesk incidents by 5000% in one company
- 2011 – Lockheed Martin / RSA incident exposed the danger of keeping all of the MFA keys in one place
- 2017 – O2 SS7 hack intercepts SMS OTPs for German banking customers
- 2019 – dozens of incidents impacting Fortune 100 companies due to improper reliance on soft token MFA on mobile devices

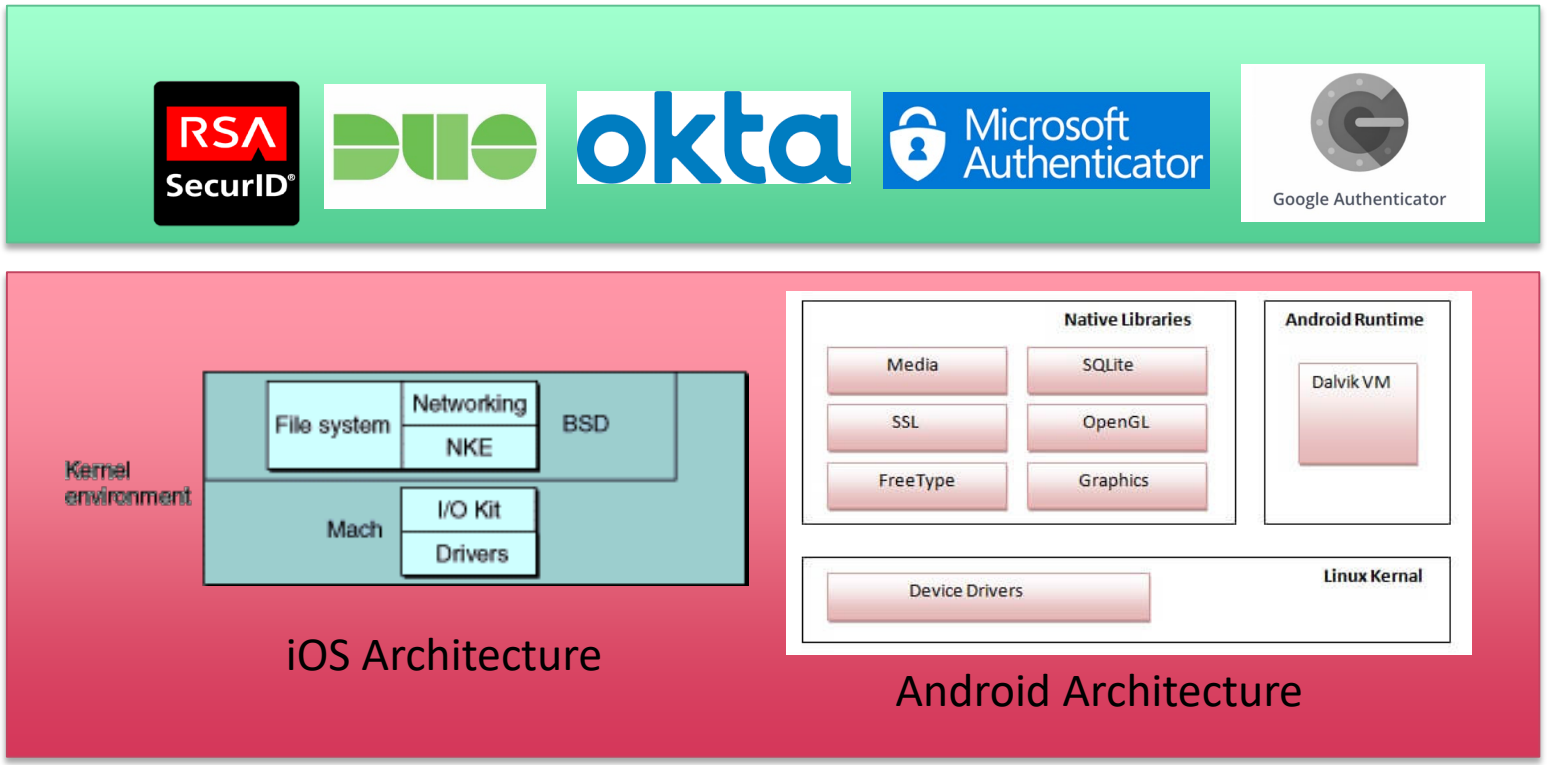
2019 – Revenge of the poorly-thought-out MFA

- What could possibly go wrong when installing a user-mode application with sensitive cryptographic key materials on a platform with kernel vulnerabilities?
- Vulnerable iOS and Android devices attacked and MFA identities cloned
  - Attacker gained access to IaaS and SaaS administrator accounts
  - Attacker gained access to Corporate VPN
  - Attacker gained access to PAM Platform

A brief refresher on OS architectures

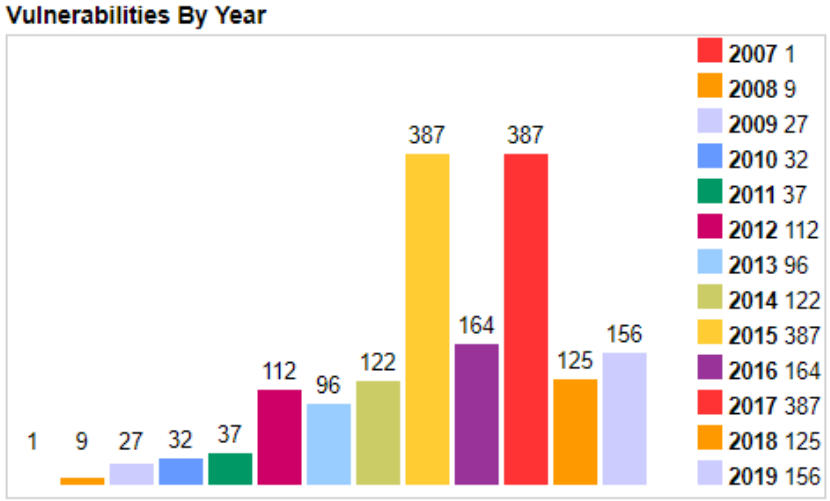
An attacker gets access to all of the application secrets here

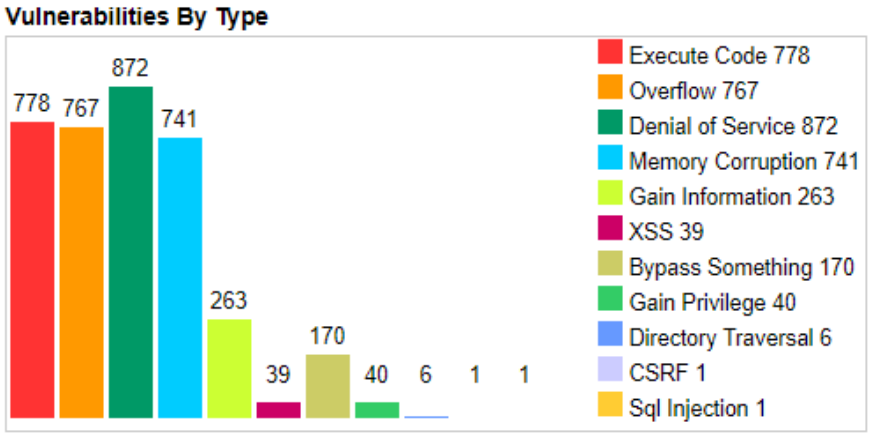
If an attacker gets a hook into the OS at the kernel level here



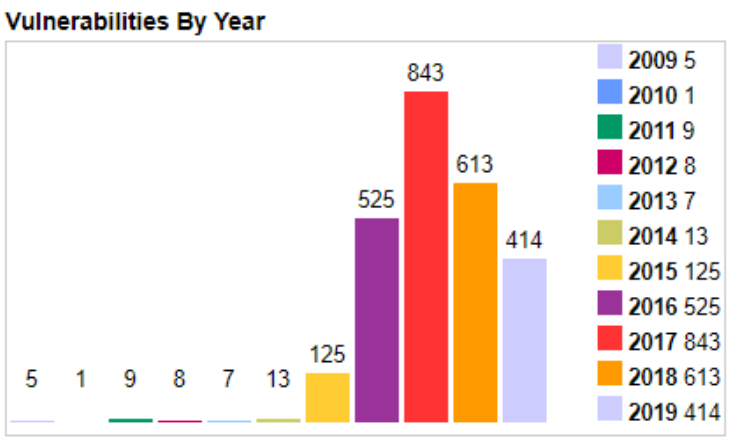
How prevalent are kernel-mode vulnerabilities?

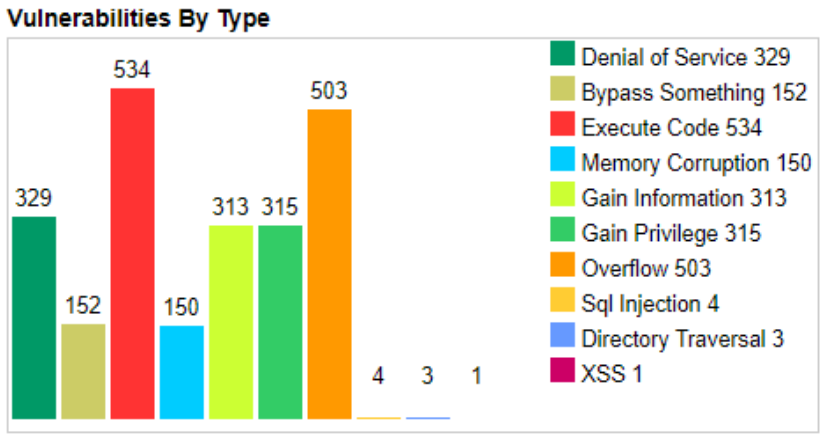
iOS Vulnerabilities





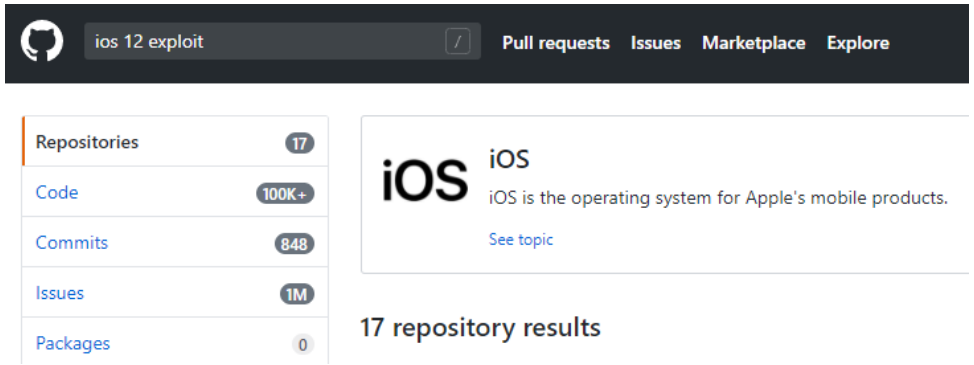
Android Vulnerabilities

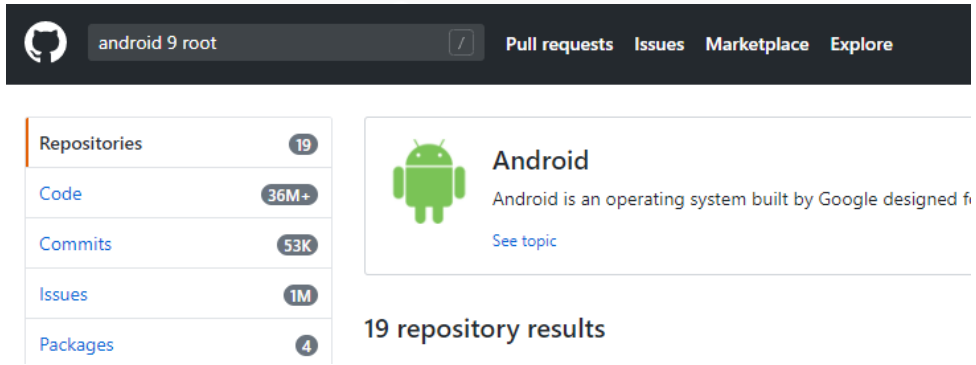




https://cvedetails.com

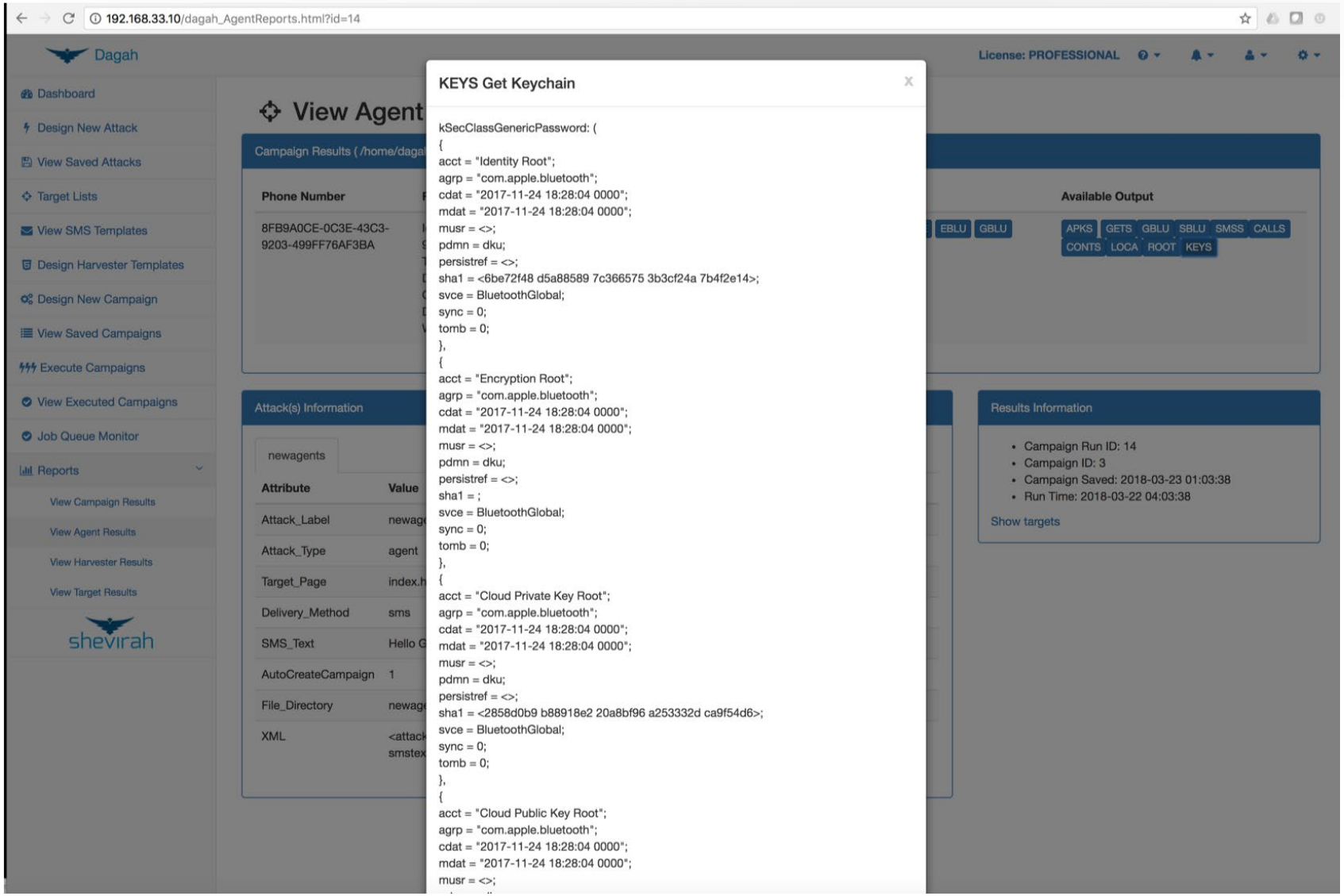
How easy is it to get exploits for these vulnerabilities?





- Not hard!
- Enterprises essentially have 28 days from the date of the release of a remotely-exploitable iOS/Android vulnerability before GitHub code is posted for public use

iOS Remote Exploit MFA Demo



Mobile OS vulnerabilities' impact on enterprises

- Based on IANS Research data, 40% of devices in the Fortune 500's mobile fleets have not had their OS updates installed within 6 weeks
- 90% of Fortune 500 organizations are using mobile MFA for access to critical systems and data
- Rough guess: over 5,000,000 vulnerable mobile MFA installations with access to critical systems and data

Action Plan

- If you're relying on mobile MFA, device hygiene is key
  - Only allow iOS devices which support Version 13 to install MFA applications
    - iPhone 8 and later is safest bet
    - iPhone XS and 11 are the only ones not vulnerable to "checkm8"
  - Only allow Android devices with Android 9 and 10 to install MFA applications
    - Pixel 3 & later for best options
    - Android One devices can work in a pinch
    - Stay away from Samsung devices due to fraudulent software update history
- Best way to accomplish this:
  - Block out-of-policy mobile OS devices from receiving enterprise email and MFA invitations

RSAConference2020

Questions?

aaron@highside.io georgia@shevirah.com