

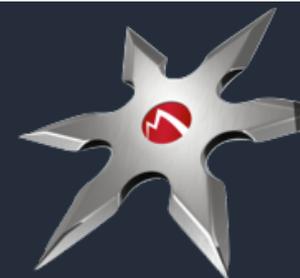


Smartwatch Risks

The new Security Risk to your Enterprise

Mike Raggio

@MikeRaggio (twitter)



#whoami

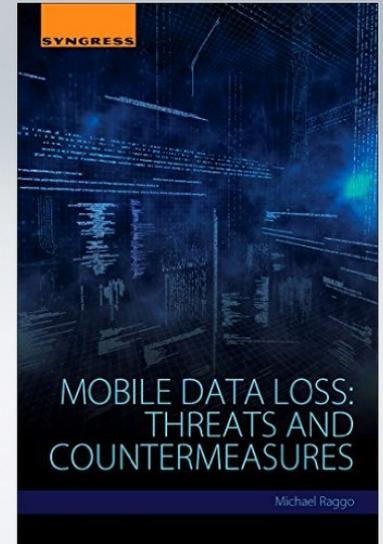
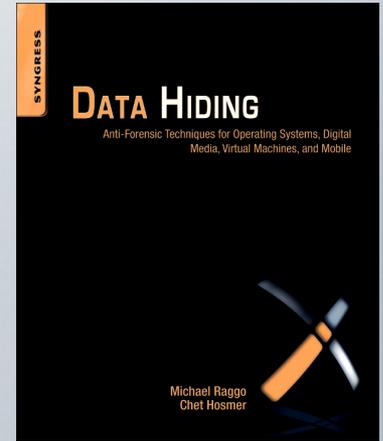
Michael T. Raggio (CISSP, NSA-IAM, ACE, CSI)

- Author, Speaker, Researcher, Governing Bodies Participant
- Mobile device ethical hacking and countermeasures
- 18 years research Steganography, Covert Communications
- Former digital forensics investigator (certified)

Presented on security at:

- Pentagon
- FBI
- Black Hat
- DEF CON
- SANS
- DoD Cyber Crime
- OWASP, ISSA

- [@MikeRaggio](#)
- Participate in PCI Council, and member of PCI Mobile Task Force
- Published Author
- Data Hiding book at the NSA National Cryptologic Museum – Ft. Meade



Research 1st released at Black Hat USA 2015 & DEF CON 23

- Released Smartwatch Security Research Paper at Black Hat
- DEF CON Demo Lab – SWATtack Smartwatch Attack Tool
- DEF CON Wall of Sheep – Remaining Covert in an Overt World



	Thursday, August 7th	Friday, August 8th	Saturday, August 9th	Sunday, August 10th
10 - 11 AM		Date Hiding: A Peek at the Latest Innovations Michael Raggo and Chet Hoemer	How Machine Learning Finds Malware Needs in an AppStore Haystack Theodora Titonis	



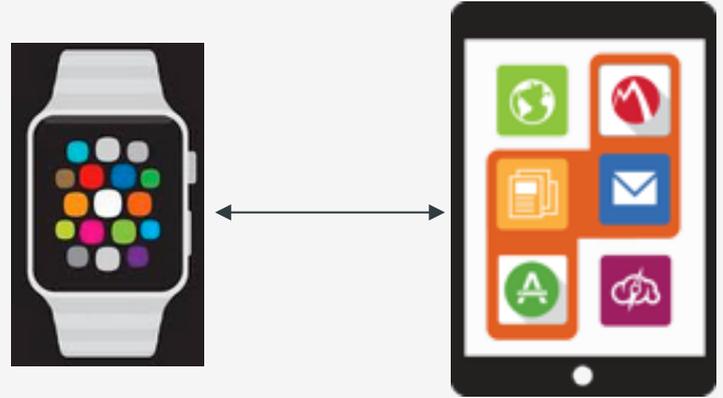
- Research is ongoing, expanding into other Smartwatches



Smartwatch Security Research Results Recap

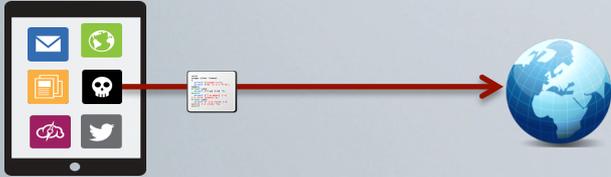
Genesis behind Research

- Got a **Samsung Gear 2 Neo** bday gift, couldn't help but hack it
- **Apple Watch** not released yet
- Did **Enterprises** understand risk of their data on these devices?
- Hadn't seen any broad research about risks, threats, hacks, etc.



Smartwatch Threat Vectors

Do the pairing apps exhibit suspicious behaviors? Data exfiltration



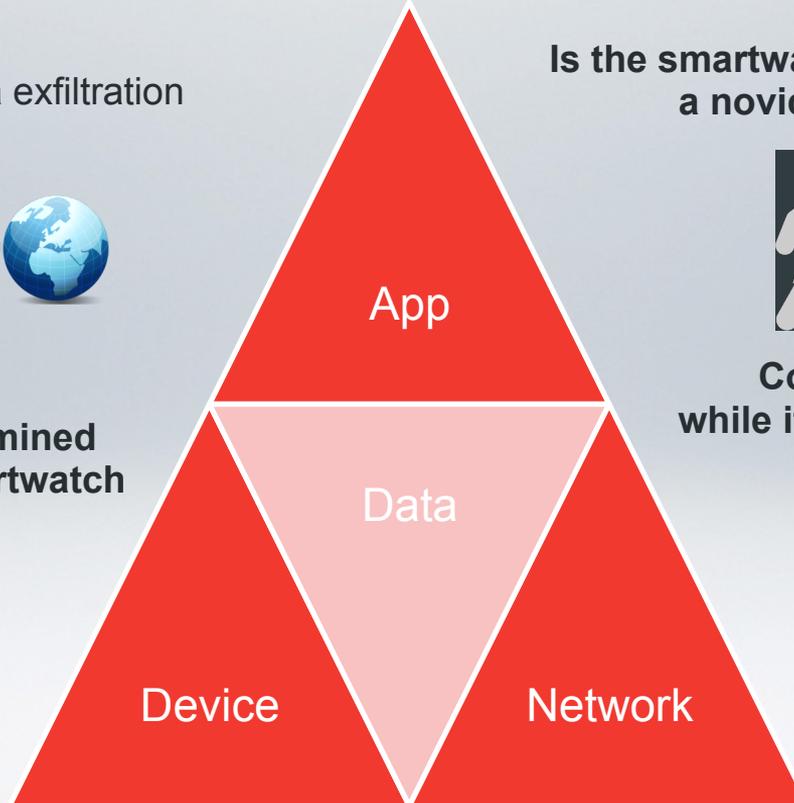
Lost/Stolen – could a determined attacker break into the smartwatch and steal data?



Is the smartwatch secure enough to prevent a novice attacker from viewing data?

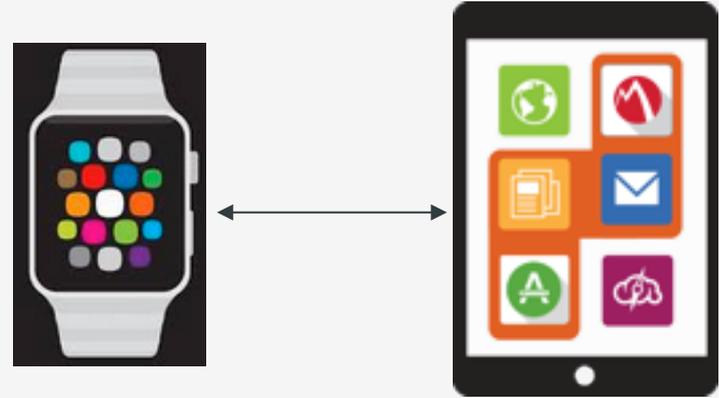


Could someone intercept data while it's paired to the smartphone or spoof the smartphone?



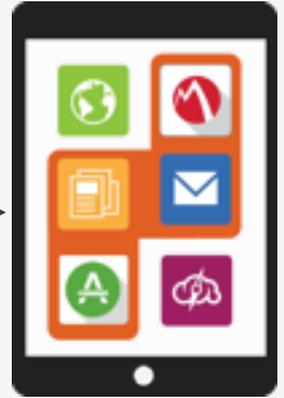
Smartwatch Security Research - Background

- Smartwatches pair with your phone using a **Pairing App**
- **PIN is proximity-based**
- **Notifications** - Allows for notifications from apps to be sent to smartwatch
- **Email** – view and respond to emails
- **SMS messages** - view and respond to messages
- **Apps** - Apps can be loaded on smartphone that support smartwatches, thus allowing additional apps on smartwatch



Smartwatch Misconceptions

- **Smartwatches don't always require a pairing app, it simply greatly enhances the experience**
- **Apple Watch** - Other smartwatches can pair with the Apple iPhone, *not just the Apple Watch*
- **Most pair over bluetooth, but a few can use WiFi**
- **Broad assortment of smartwatch Operating Systems** – Watch OS, Android Wear, Tizen (Samsung), Nucleus, and many more!!!



Smartwatch Security Research Lab

Tested 4 Smartwatches
Apple Watch, Samsung Gear 2 Neo, Moto 360, U8



**Samsung
Tizen**



**Apple
watchOS**



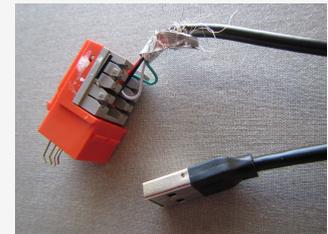
U8 Nucleus



**Android Wear
(Moto 360)**

Moto 360

- **Runs Android Wear**
- **No PIN protection** on the one we purchased
- But there is an **Android Wear update (5.1.1)** that adds (optional) **PIN protection**
- **No device encryption**
- Debugging challenging as **no direct connect microUSB**
- Can debug over bluetooth (through smartphone)
- Can also debug with **Hardware Hack to access Android Debug Bridge => YouTube Videos**
- Note that Android Wear does a key exchange to debug...



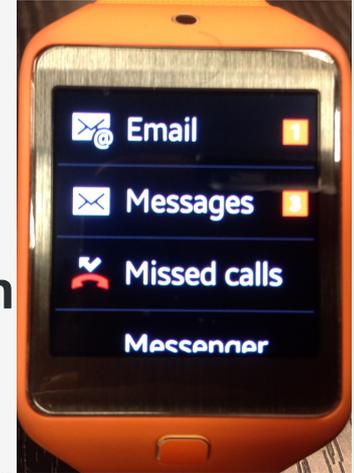
U8

- **Made in China**
- **Bought on Ebay**
- Simulate a user buying a random smartwatch off Ebay
- Runs an embedded OS - **Nucleus**
- **Pairs with Android and iOS**
- **No PIN protection** on the one we purchased
- **User manual guides user to random URL to download App outside of Google Play**
- **Pairing App** found to have a **backchannel communication back to China to random IP**



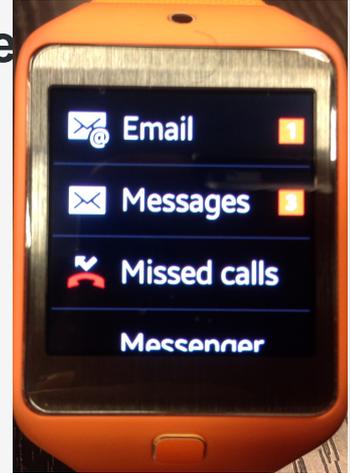
Samsung Gear 2 Neo

- **Runs Tizen, not Android Wear**
- **Pairs with Android devices**
- **Can sync with PC or Mac** with Kies – common Samsung media backup software
- **Like iTunes, requires a PIN to be entered (if one exist on the smartwatch) to allow sync**
- **Offers a developer mode on Gear** to allow developer design access, but commonly used by users for customizing and rooting their smartwatch



Samsung Gear 2 Neo

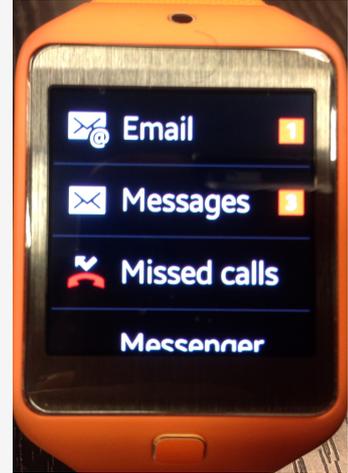
- Simulated a lost device with PIN protection to determine if an attacker could access the data on the smartwatch
- Found vulnerability in Samsung Smartwatch (Samsung Gear 2 Neo) – PIN bypass vulnerability
- Worked with Samsung through responsible disclosure
- Samsung *promptly* issued a patch (Huge thanks to Samsung for remaining highly engaged with us)



Samsung Gear 2 Neo

Details:

- PIN protected watch face, but not USB CLI access
- “sdb” (similar to ADB – Android Debug Bridge) allowed CLI access, with *no password* to user’s media directory
- Also allowed access to system directories including system logs and password file
- **Worked with Samsung through responsible disclosure. Samsung *promptly* issued a patch (Huge thanks to Samsung for remaining highly engaged with us)**



Ingredients

- **Samsung Kies (mostly for smartwatch drivers)**
- **Tizen SDK**
- **Windows (Mac OS X Tizen SDK unstable)**
- **USB cable**
- **Python**
- **My tool **SWATtack****



Wrote SWATtack – Smartwatch attack tool

- **SWATtack** - written in Python
- Identify vulnerabilities in smartwatches
- Can also be repurposed for forensic acquisition
- E.g. Bypass PIN protection and copy data from smartwatch (Samsung Gear 2 Neo)

Command Prompt

G:\tizen-wearable-sdk\tools>

File Home Share View

This - Gear 2 - Search Gear 2 Neo (EC4A)

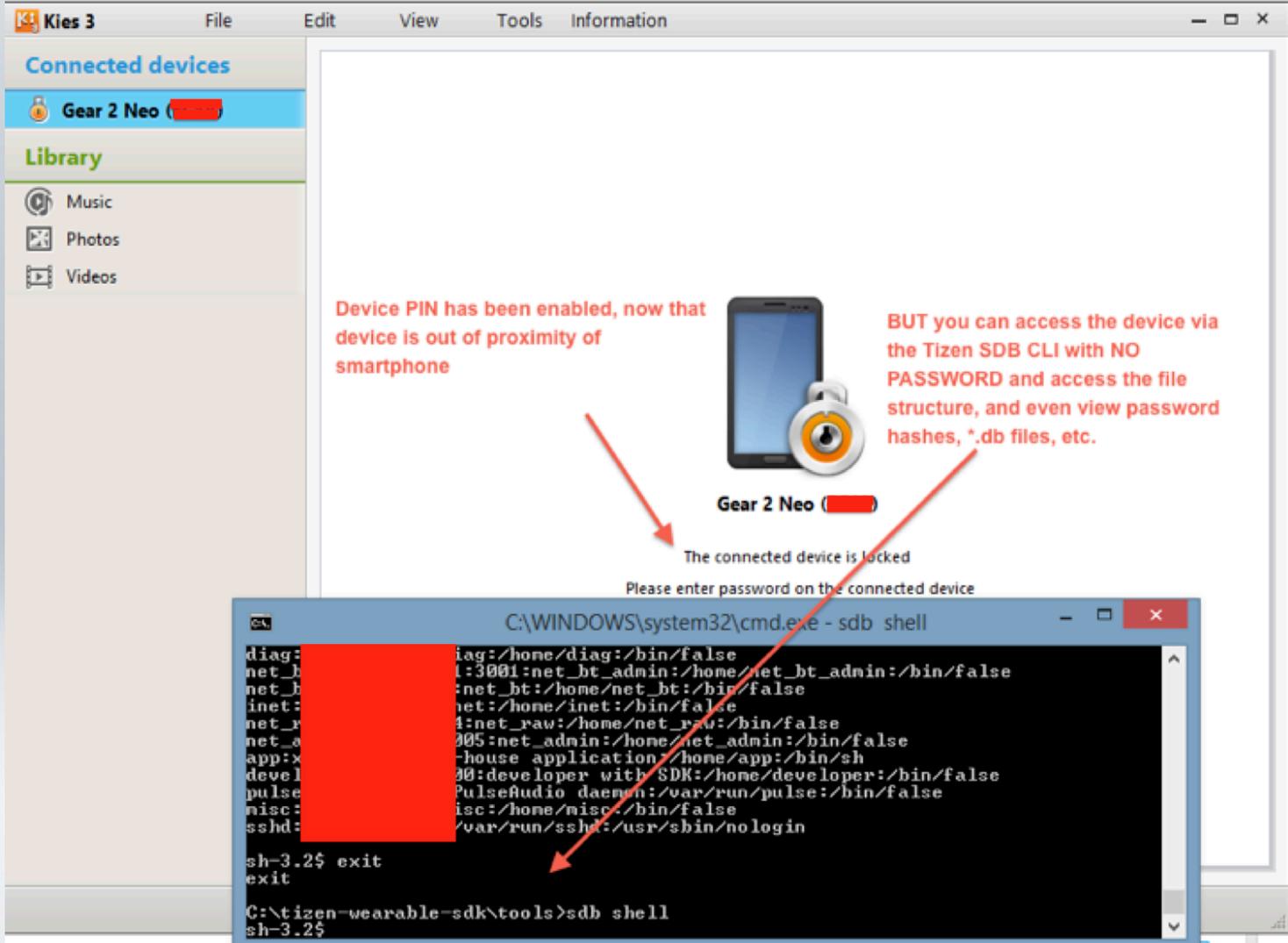
This folder is empty.

- ★ Favorites
 - Desktop
 - Downloads
 - Recent places
 - SkyDrive
- OneDrive
- This PC**
 - Desktop
 - Documents
 - Downloads
 - Music
 - Pictures
 - Videos
 - OS (C:)
- Network

0 items

Taskbar icons: Windows Start, File Explorer, Google Chrome, Microsoft Edge, Internet Explorer, VLC, JCI, M, and a printer icon.

8:58 PM
8/9/2015



SWATtack

```
C:\WINDOWS\system32\cmd.exe
c:\Python34>swattack4.py
SWATtack, by Mike Raggo www.spyhunter.org, Open Source, intended for ethical use
and forensic purposes

SWATtack begin sequence...

We're in! SWATtack acquire data
pulled          .charging.log.5          100%          4MB
pulled          thumb_default.png       100%          5KB
pulled          smallbeer.jpg           100%          57KB
pulled          Screenshot (1).png      100%         271KB
pulled          smallbeer.jpg           100%          57KB
pulled          Over the horizon.mp3     100%          2MB
pulled          smallbeer.jpg           100%          57KB
pulled .jpg-b0e0247053231fc91f86daaf192378dc.jpg 100%          16KB
pulled .jpg-7dfb57467add64f238212933282bfea0.jpg 100%          16KB
pulled .png-87cccb8e0e433e756cfec1ae56a18a95.png 100%          92KB
pulled .mp3-20a0deaf18f5d6f3d63686f24a18715c.png 100%          18KB
pulled .jpg-36e1d55a8241c6f8de526bf4a6f23fc3.jpg 100%          16KB
pulled Voice 001_W_20150808_110733.m4a 100%         136KB
pulled          AccCheck.dll            100%          79KB
pulled          wstraceutilresources.dll 100%          14KB
15 file(s) pulled. 0 file(s) skipped.
/opt/usr/media          844 KB/s (8828237 bytes in 10.205s)

SWATtack acquisition complete!!!

Frank - I've walked a white line my entire life, Im not about to screw that up.
Nada - White line's in the middle of the road, that's the worst place to drive.

- They Live
RIP - Rowdy Roddy Piper

c:\Python34>
```

Apple Watch

- **Runs WatchOS (WatchOS 2)**
- **All Apps can send notifications** from iPhone to Watch
- **Apps which add WatchKit extension can display App on device** (not all Apps)
- **Setup prompts for PIN**
- **Includes data protection type encryption**
- For details on the **Apple Watch security specs** checkout the **Apple Security Guide:**
- https://www.apple.com/business/docs/iOS_Security_Guide.pdf

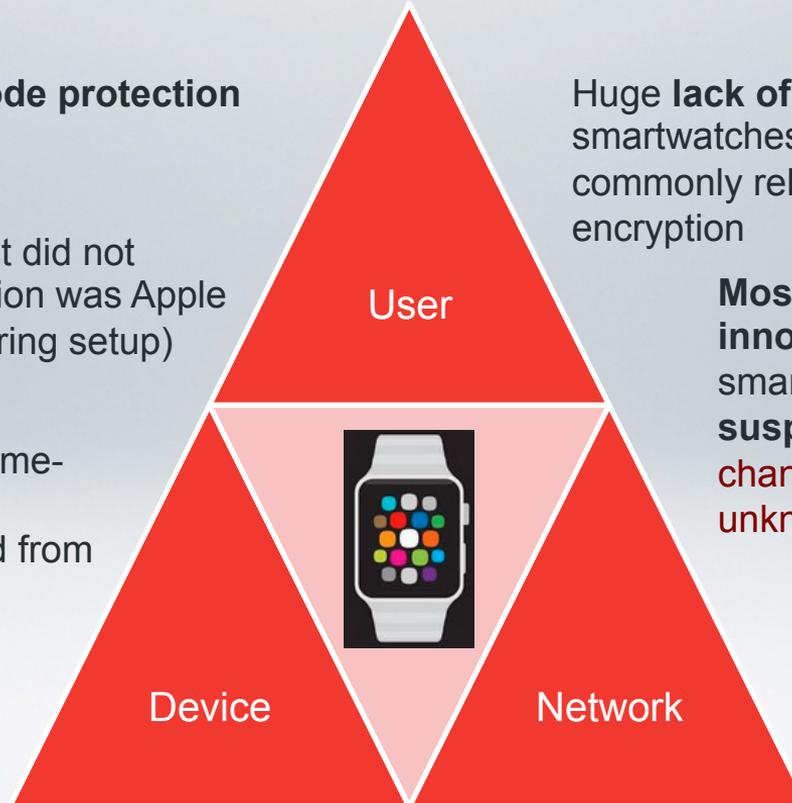


Wide variance of Smartwatch Security RISKS!!!

Only some have PIN/Passcode protection options

PIN is not required, and most did not prompt to enter a PIN (exception was Apple Watch which prompts user during setup)

PIN is proximity-based not time-based (loses pairing with smartphone locks, or removed from wrist it locks)



Huge **lack of encryption** across most smartwatches test (except Apple Watch), commonly rely on app developers to add encryption

Most pairing Apps were innocuous, but the Chinese smartwatch tests had some **suspicious behaviors** (e.g. **back channel communication with unknown IPs**)

Found vulnerabilities in Samsung Smartwatch (Samsung issued patch)

MobileIron.com Smartwatch Research Results

Analysis	Motorola Mobility Moto 360	Shenzhen Qini U8	Samsung Gear 2 Neo	Apple Watch
Platform/OS	Android Wear	Nucleaus	Tizen	Watch OS
PIN/Passcode Option	Added in Android Wear 5.1.1	None found	Optional, no user prompt	Optional User Prompted
Encryption	Optional at App Level	None found	Optional at App level	Yes, Watch Data Protection and optional App Level
Lost/Stolen Protection	Locks when pairing lost (if enabled)	Alerts (buzz)	Locks when pairing lost (if enabled)	Locks when removed from wrist

Best practices guidance

When pairing a smartwatch to a smartphone, is all of the corporate data synced?

- **While although you can get notifications on the device, unless the App (or Container) allows viewing the data on the device, the data itself is limited to the smartphone (or tablet where applicable)**
 - **iOS apps require the WatchKit extension**
 - **Android/Tizen require a container policy to allow it (default blocked)**

Best practices guidance

Can I remove corporate data from the Smartwatch?

- For **iOS Managed Apps** (Apps distributed by EMM/MDM), when a device is retired or quarantined, these managed Apps are removed from both the iPhone “and” the Apple Watch – **thus removing corporate data (and profiles) from the Apple Watch**

Best practices guidance

- If I'm an admin, can I detect smartphones that have a paired smartwatch?
 - Sort of...
 - There is an **API that allows EMM to detect** specifically an Apple Watch paired with an iPhone
 - More broadly, you can identify **pairing Apps** from the EMM App inventory

Best practices guidance

- **Educate your users, and update your documented security policies**
 - **Encourage users to set a PIN, reminding them that they will be protecting their personal data as well. This won't require them to enter the PIN every 15 mins, only when the device is unpaired, lost/stolen, or removed from their wrist**
 - **PIN also protects Apple Pay on the Apple Watch**

MobileIron.com Research Paper Download

MobileIron Analysis of Smartwatch Security Risks to Enterprise Data

v1.2



MKT-9170 | © 2015 MobileIron, Inc.

Analysis	Motorola Mobility Moto 360	Shenzhen Qini U8	Samsung Gear 2 Neo	Apple Watch
Platform/OS	Android Wear	Nucleus	Tizen	Watch OS
PIN/Passcode Option	Added in Android Wear 5.1.1	None found	Optional, no user prompt	Optional User Prompted
Encryption	Optional at App Level	None found	Optional at App level	Yes, Watch Data Protection and optional App Level
Lost/Stolen Protection	Locks when pairing lost (if enabled)	Alerts (buzz)	Locks when pairing lost (if enabled)	Locks when removed from wrist

<https://www.mobileiron.com/en/whitepaper/smartwatches-wearables-and-mobile-enterprise-security>

Great, where can I download **SWATtack**???

- **February 26, 2106** from one of two sites:
- **Python-Forensics.org** (My friend Chet Hosmer)
- **Spy-Hunter.com** (my personal research site)
- **MobileIron.com** – Detailed Research Paper



MobileIron®

Mike Raggo

@MikeRaggo

@DataHiding