

For Enterprise

Attacking BYOD Enterprise Mobile Security Solutions

Vincent Tan

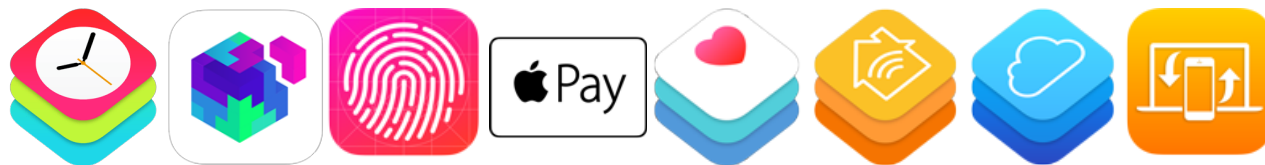
Senior Security Consultant



- Sunny Singapore
- Senior Security Consultant @ Vantage Point Security
- 4+ years hacking stuff professionally, specializing in mobile & exotic stuff

1. iOS Applications in General
2. What is BYOD? Why BYOD? Who uses BYOD?
3. Security Features of BYOD Solutions
4. Good Technology
5. iOS Jailbreaks / Attack Vectors
6. Local & Network Attacks against Good EMS
 - Story of Alice & Bob

- > 1.4m Applications¹ in iOS App Store
 - ~10% in Business Category
- 35% of Enterprises have an Enterprise App Store²
- Simple vs Complex Functionality
 - Mobile application capabilities have not caught up with device capabilities
 - Maybe 10% of apps have advanced functionality
 - MDM, Soft Tokens, Payment Applications, HomeKit.



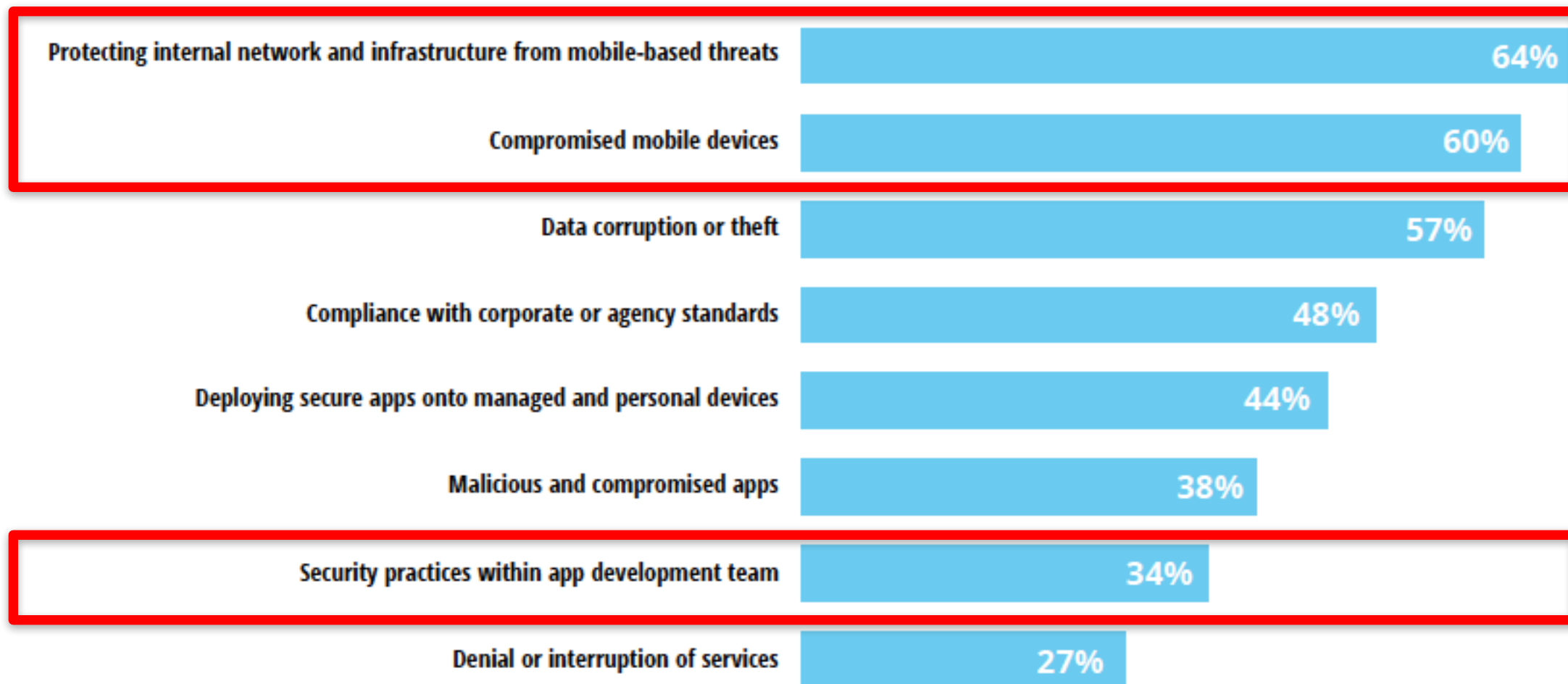
¹ <http://www.zdnet.com/article/ios-versus-android-apple-app-store-versus-google-play-here-comes-the-next-battle-in-the-app-wars/>

² https://go.appierian.com/rs/300-EOJ-215/images/Appierian%202016%20Executive%20Enterprise%20Mobility%20Report_FINAL_20160216.pdf?aliid=16373787

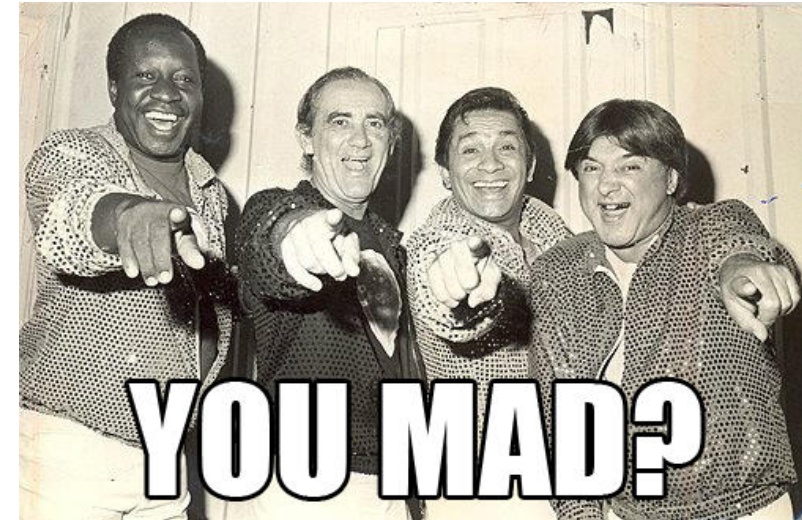
- BYOD?
 - What and Why?

Which mobile security issues are you concerned about?

Multiple responses allowed



- BYOD?
 - What and Why?
- BYOD Adoption
 - 74% using or adopting BYOD
 - Governments
- Enterprise Mobile Security
 - MAM (Mobile Application Management)
 - MIM (Mobile Information Management)
 - MDM (Mobile Device Management)



“prevent employees from opening files in unsecured apps, backing up business data to personal cloud-based services, or copying and pasting business ...”

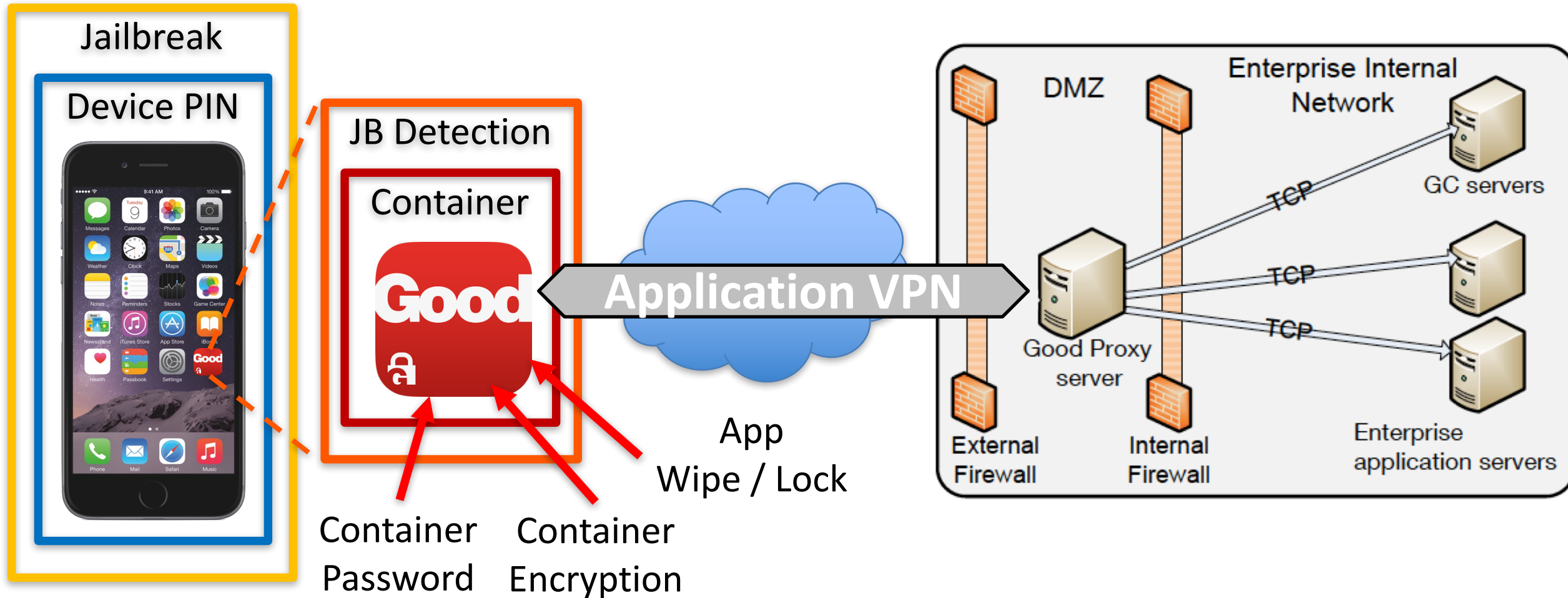
“Detect OS tampering and other policy violations”

“...remotely lock or wipe the device.”

“Protect mobile apps and servers from being hacked...”



Enterprise Mobile Security Features



- Acquired by Blackberry in Nov 2015
- Top 5 EMS Solution Providers



- Acquired by Blackberry in Nov 2015
- Top 5 EMS Solution Providers
- GFE received CC EAL4+ in 2013 and GD solution in 2016
- GD platform used as a foundation to the GCS to replace GFE
- GD platform allows developers to create and distribute apps that integrates with the GD services framework

GFE vs GCS

	Good For Enterprise (GFE)	Good Collaboration Suite (GCS)
Email	✓	Good Work
MDM	✓	✓
File Share	Local File Storage Only	Good Share – Access enterprise file share
Instant Messaging	✗	Good Connect
Intranet Access	✗	Good Access
Cloud Deployment	✗	✓
Integrated MAM	✗	✓
Common Platform	✗	✓

iOS Versions	7.0 7.0.0	7.1 7.1.2	8.0 8.1	8.0 8.3	8.1.3 8.4	9.0 9.0.2	9.1 9.3.3	10.0
Jail Broken?	evasi0n7	Pangu	Pangu8	TaiG	TaiG	Pangu9	Pangu	Not Public

- Check out Stefan Esser's talk on "iOS 678 Security - A Study In Fail"



What about root?

- Non-Jailbroken Devices?
 - Resign via developer certificate
 - But apps will need to be reactivated

- Physical Access

- DROPOUTJEEP (think NSA, GCHQ)
 - Lost Devices / Stolen Devices

- Remote Attacks

(TS//SI//REL) The initial release of DROPOUTJEEP will focus on implant via close access methods. A remote installation capability for a future release.



Stefan Esser
@0n1c

Follow

Looks like someone removed the harddisk and did not correctly slip it into holes when closing the notebook



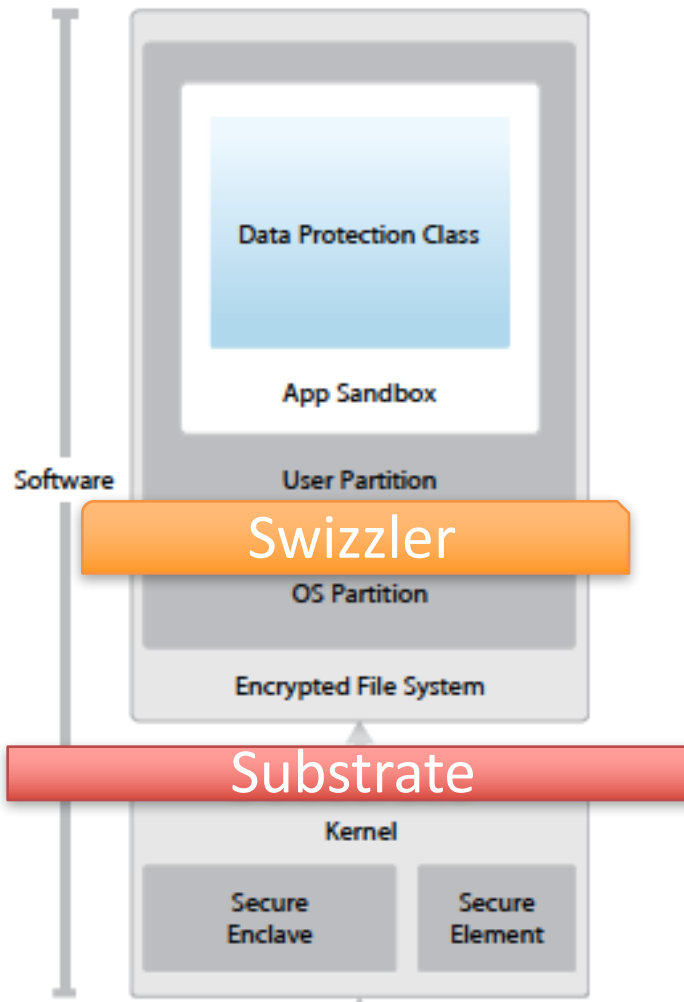
¹ <http://www.tripwire.com/state-of-security/vulnerability-management/creating-iphone-rootkits-and-like-the-nsas-dropout-jeep/>

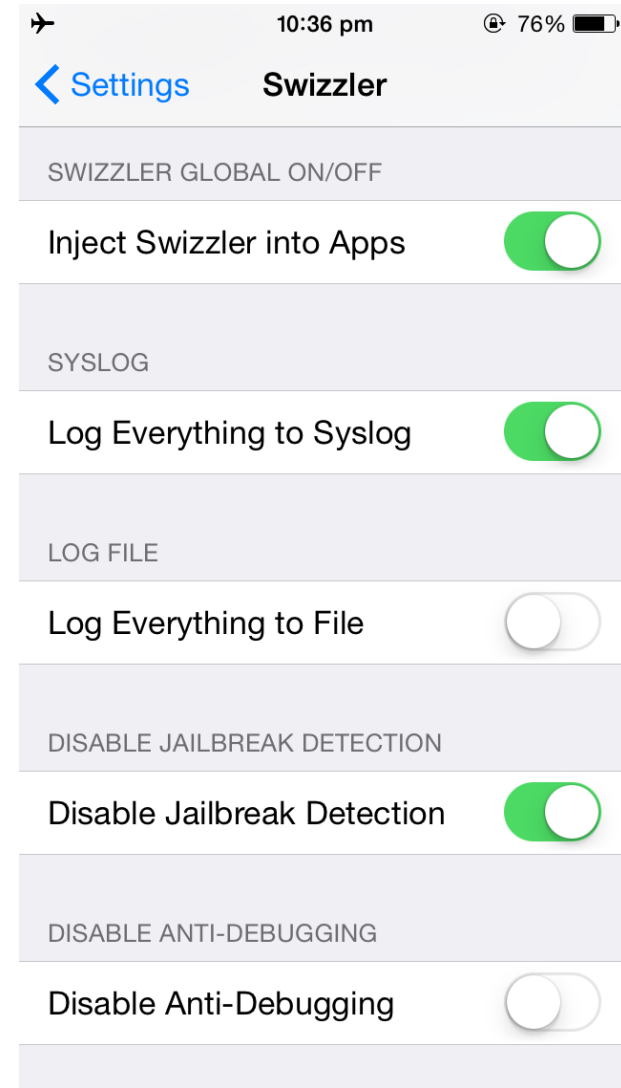
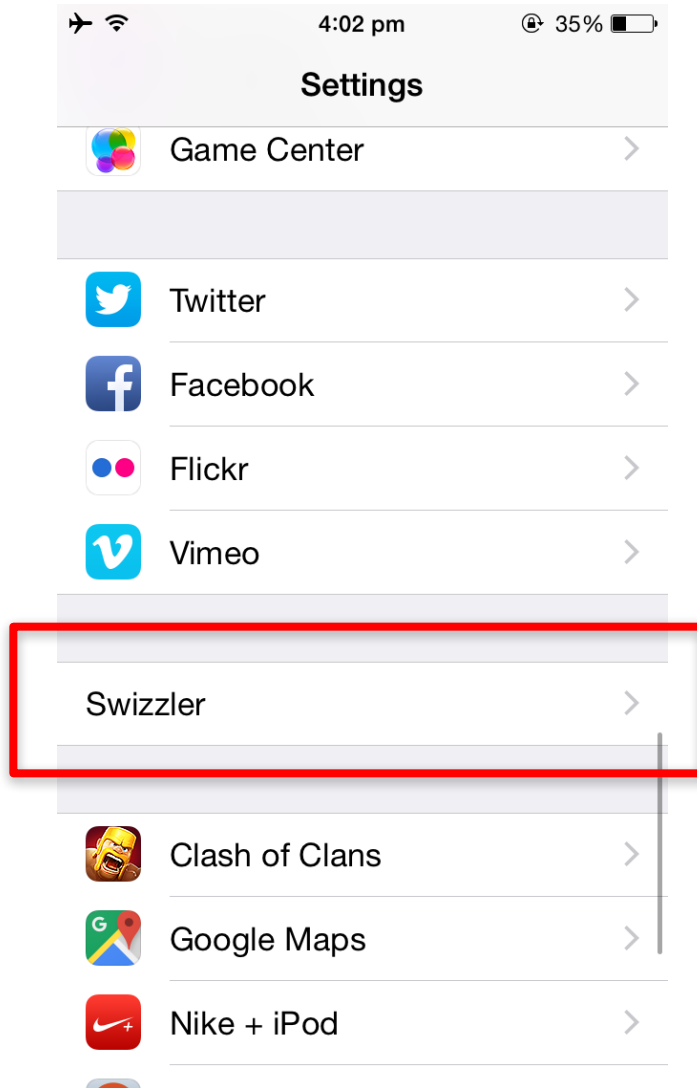
² <https://blog.fortinet.com/post/ios-malware-does-exist>

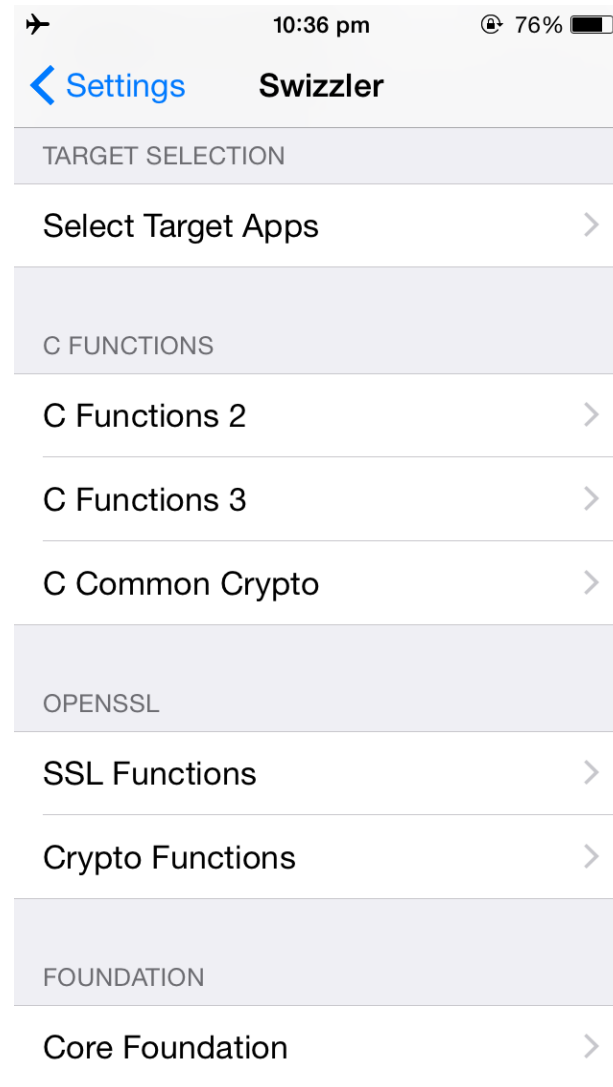
- Not normal pen testing...
 - Not just setting proxy and using Burp
- I'm not attacking the application
- Changing the environment in which the application runs.
- Not new. API Hooking and DLL Injections on Windows.
LD_PRELOAD on Linux. I'm just doing it on iOS.

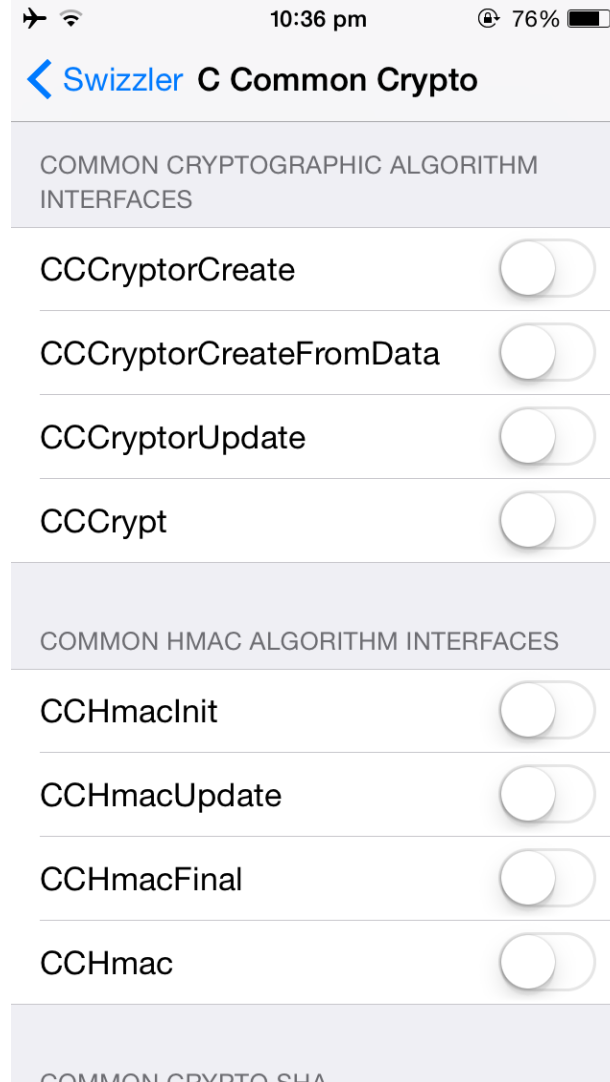
- How do I change the Environment?
- Built an App... More precisely a Dynamic Library (aka tweak)
 - DYLD_INSERT_LIBRARIES=Swizzler
- Loads itself before an application starts
 - Control all functionalities of an application

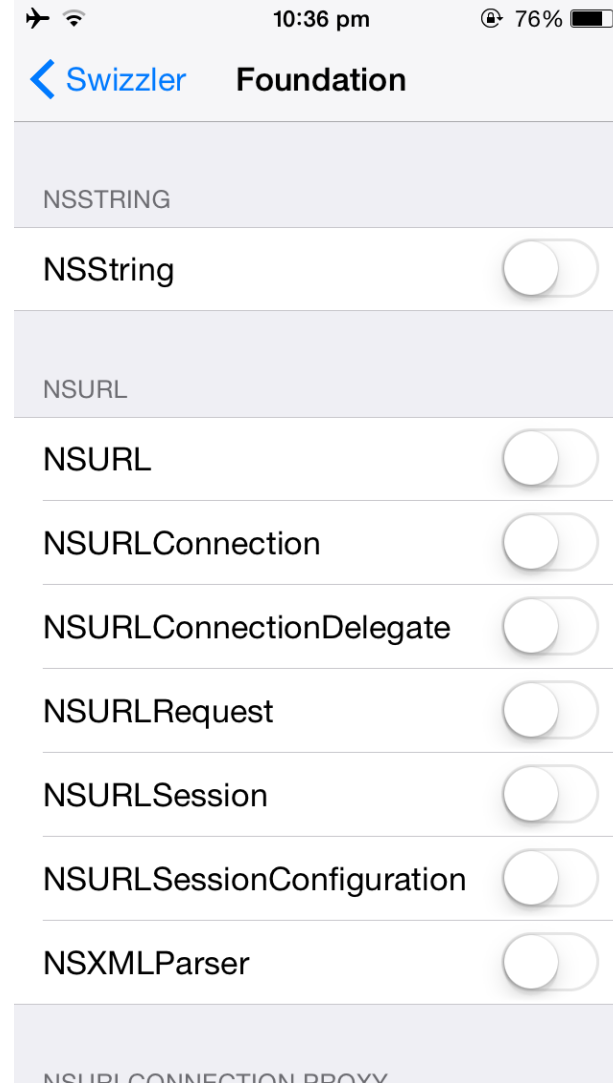
iOS Security Architecture



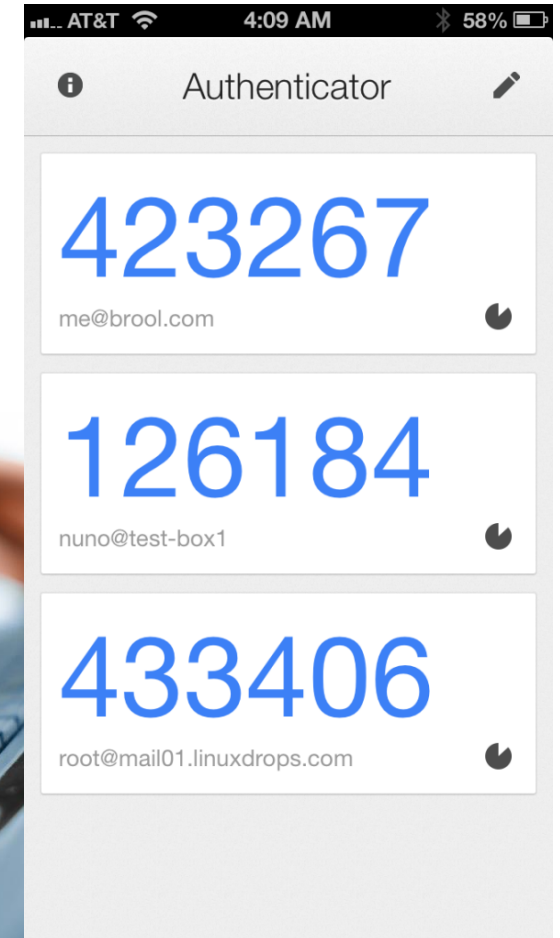
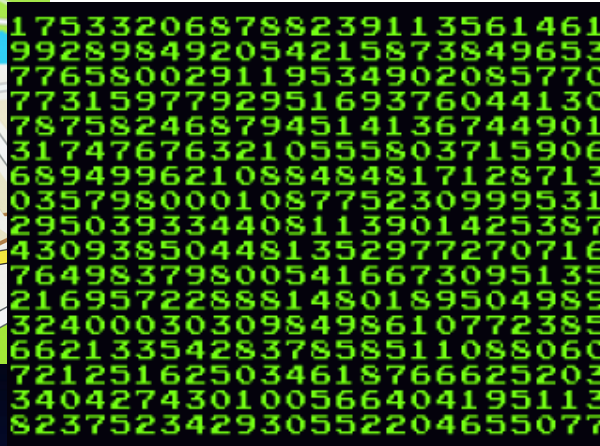
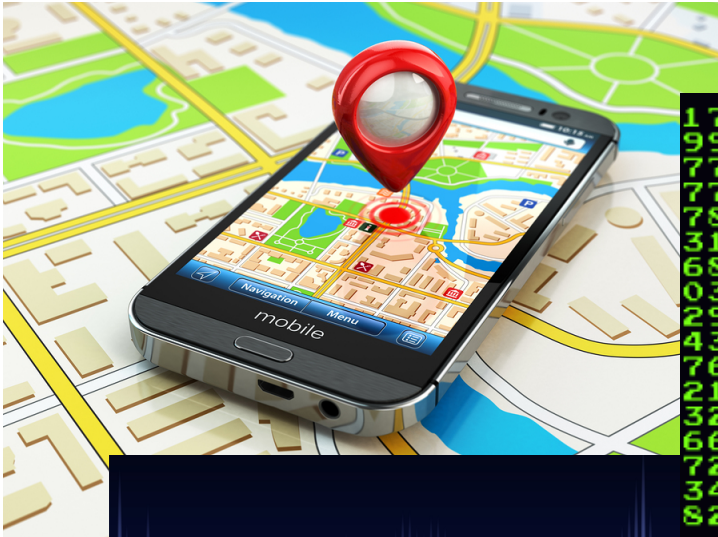








What else can you control?



Jailbreak

**Jailbreak
Detection**

Container

App DLP

Device PIN

**Container
Password**

App



Local & Network Attacks Against Good EMS





Local Attacks

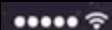


Jailbreak Detection


App
Wipe / Lock

Container
Password

Container
Encryption



9:41 am

100% 



Good Work



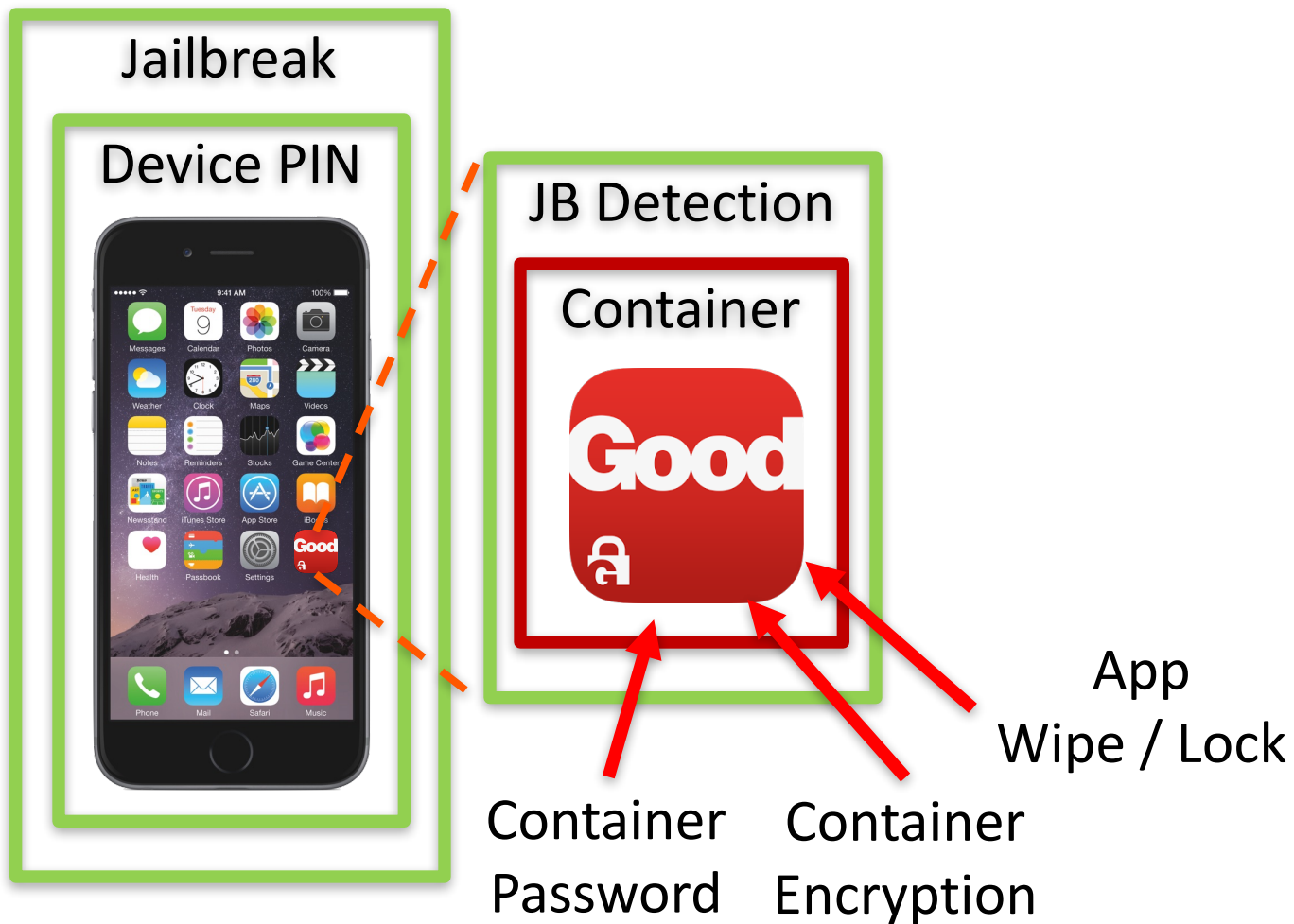
iFile



Settings



Safari



- ✓ Device PIN
- ✓ Jailbreak
- ✓ Jailbreak Detection
- ✗ Container Password
- ✗ Container Encryption
- ✗ App Wipe / Lock

Blacklist of Files

```
FILE *file = fopen("/Applications/Cydia.app",  
"r");  
if (file) {  
    fclose(file);  
    return JAILBROKEN;  
}
```

```
file = fopen("/usr/bin/ssh", "r");  
if (file) {  
    fclose(file);  
    return JAILBROKEN;  
}
```

```
FILE *replaced_fopen (const char *filename, const  
char *mode) {  
    if (blockPath(filename)) {  
        errno = ENOENT;  
        return NULL;  
    }  
}
```

```
bool blockPath(const char *fpath) {  
    ...  
    NSArray *denyPatterns = [[NSArray alloc]  
initWithObjects:    @"Cydia",    @"lib/apt",  
    @"/private/var/lib/apt",    @"/var/lib/apt",  
    @"/var/tmp/cydia.log",    @"/etc/apt/",  
    @"/var/cache/apt"  
    ....  
}
```

Prohibited Functions

```
int pid = fork();  
  
if(pid>=0)  
{  
    return JAILBROKEN;  
}
```

```
pid_t replaced_fork(void){  
    if (disableJBDetection()){  
        return -1;  
    }  
    pid_t ret = orig_fork();  
    return ret;  
}
```

- Jailbreak Detection Methods
 - Blacklist of files
 - Directories
 - Symbolic Links
 - Prohibited Commands
 - File System
 - URL Handles
 - Kernel Parameters & many more ...

Jailbreak / Policy Implementation

```
GT::GeneralUtilityClass::constructStringList (  
    GT::GeneralUtilityClass::tamper_detection_method_t,  
    std::vector<std::string, std::allocator<std::string> >  
)
```

```
loc_2ddaa8:  
    *(r5 + 0x150) = 0x1;  
    if ((statfs("/", sp + 0x8c0) != 0x0) || ((stack[1160] & 0x1) != 0x0)) goto loc_2ddace;
```

```
loc_2ddc48:  
    *(r5 + 0x150) = 0xb;  
    r0 = fork();  
    if (r0 != 0xffffffff) goto loc_2de498;
```


Jailbreak / Policy Implementation

- GD::GDSecureStorage::handleWrongPwd
- GD::GDSecureStorage::wipeDevice
- GD::PolicyProcessor::processLockAction
- GD::GDLibStartupLayer::checkPartialCompliance
- GD::PolicyComplianceChecker::checkComplianceUnlocked
- GD::PolicyComplianceChecker::checkComplianceLocked



Container
Password

Container
Encryption

App
Wipe / Lock

Password Bruteforce



9:41 am

100%



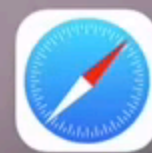
Good Work



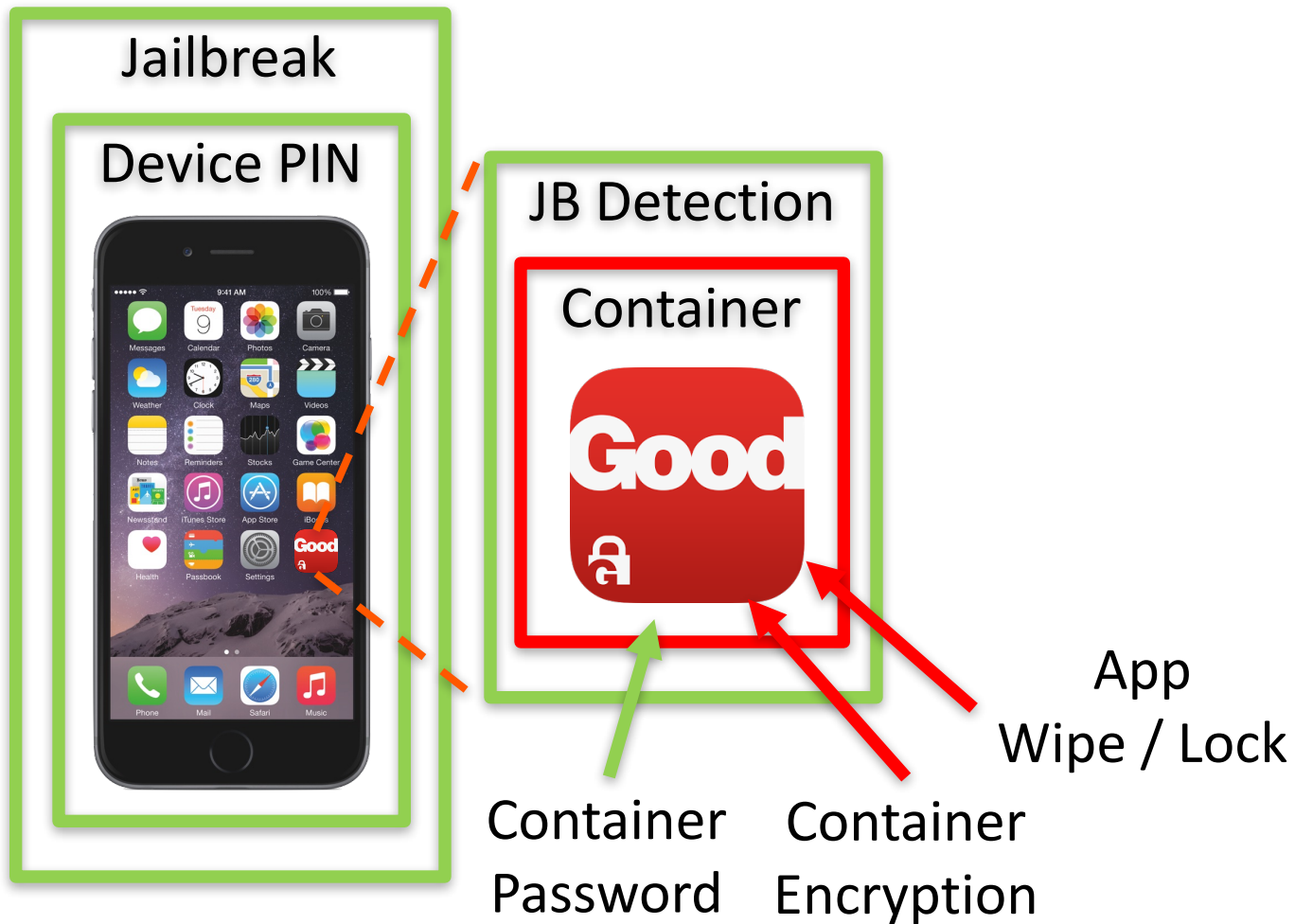
iFile



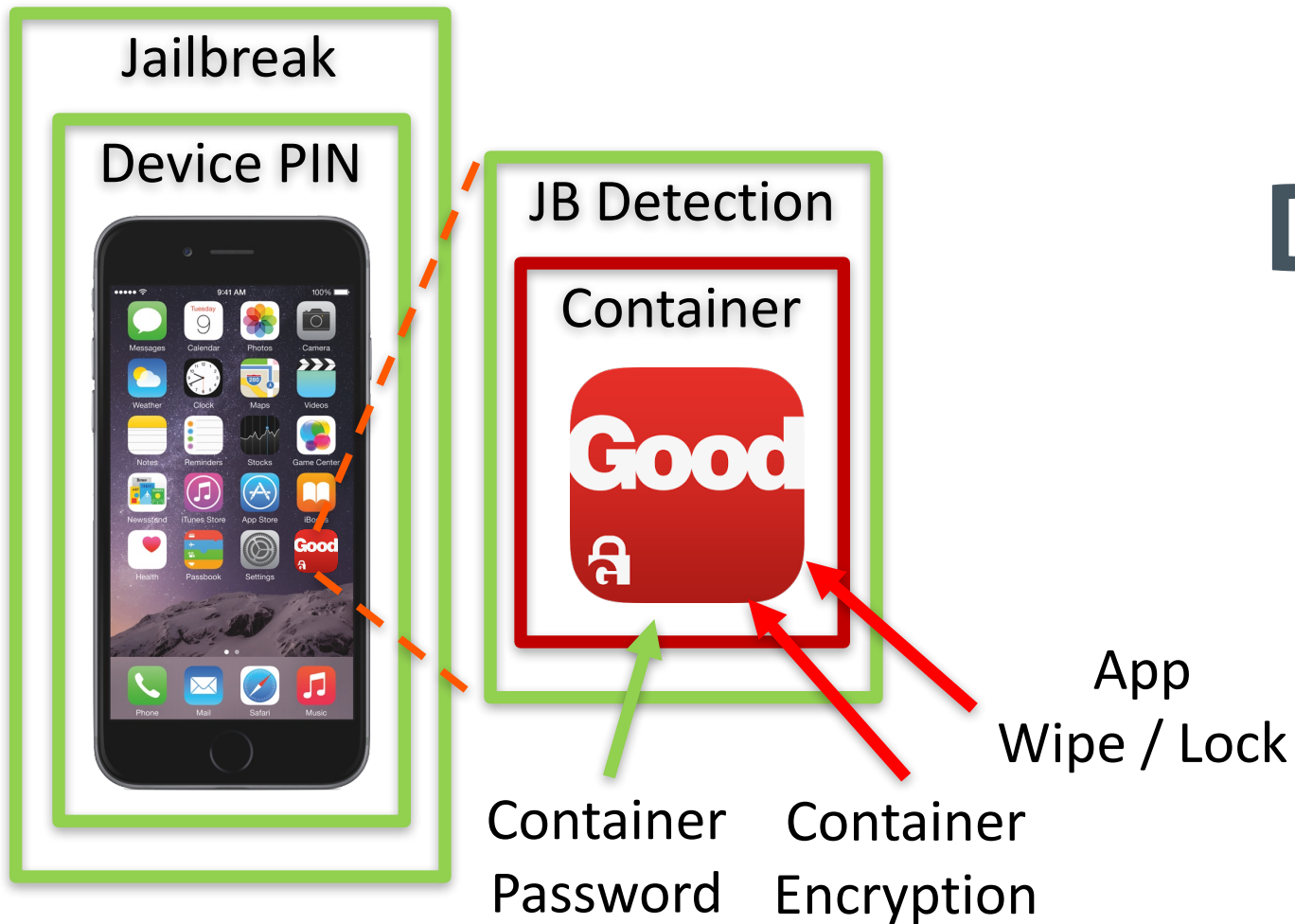
Settings



Safari

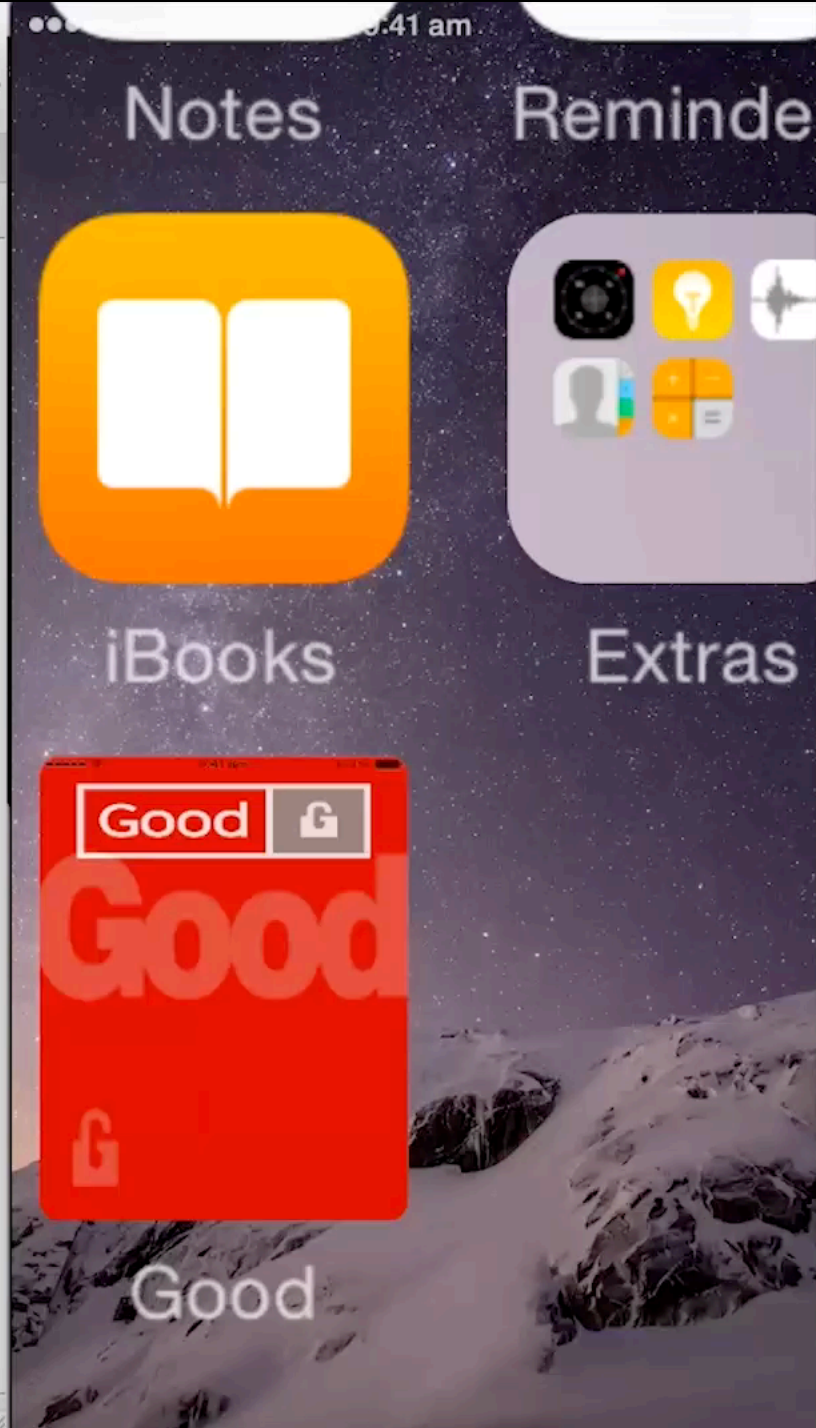


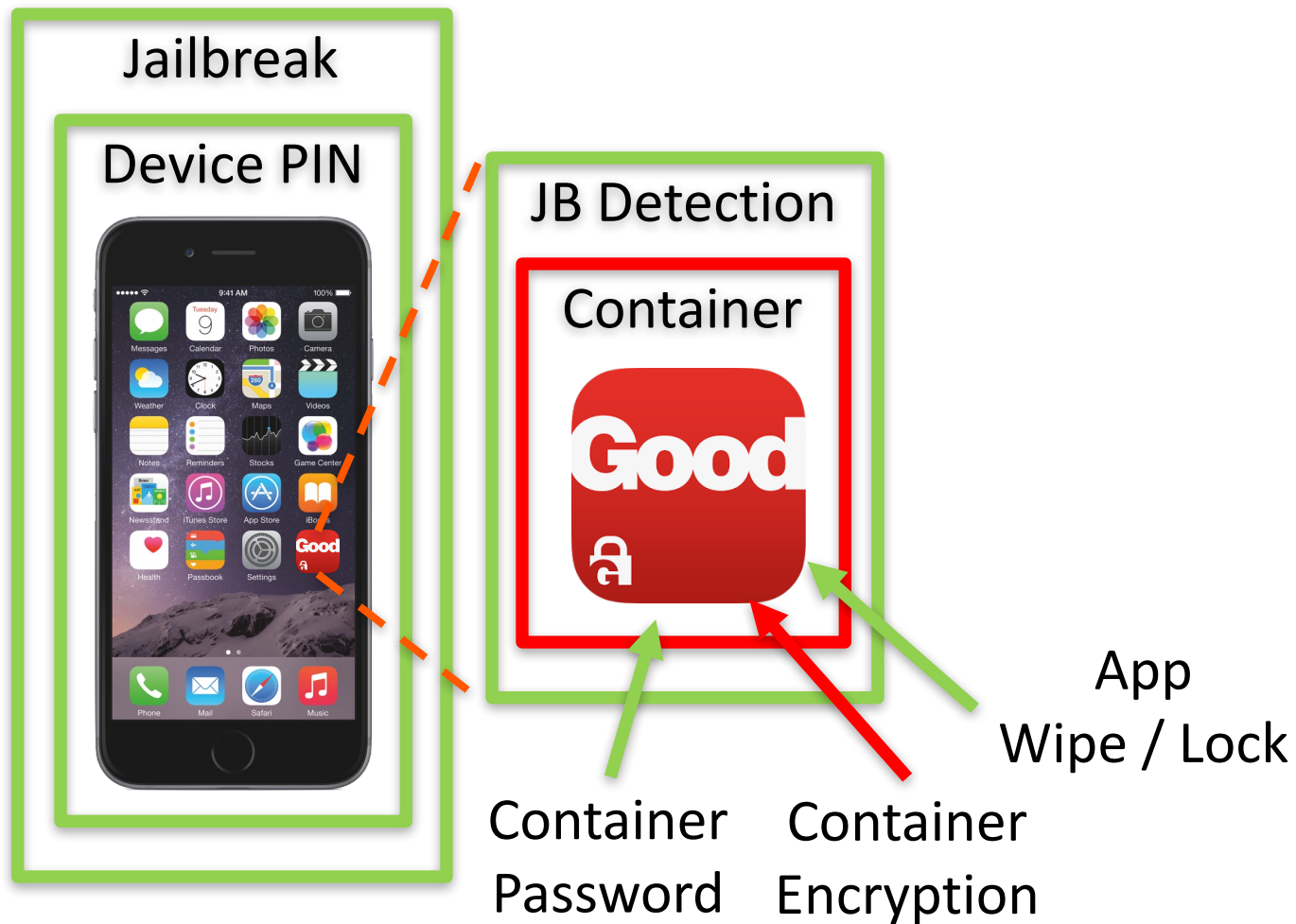
- ✓ Device PIN
- ✓ Jailbreak
- ✓ Jailbreak Detection
- ✓ Container Password
- ✗ Container Encryption
- ✗ App Wipe / Lock



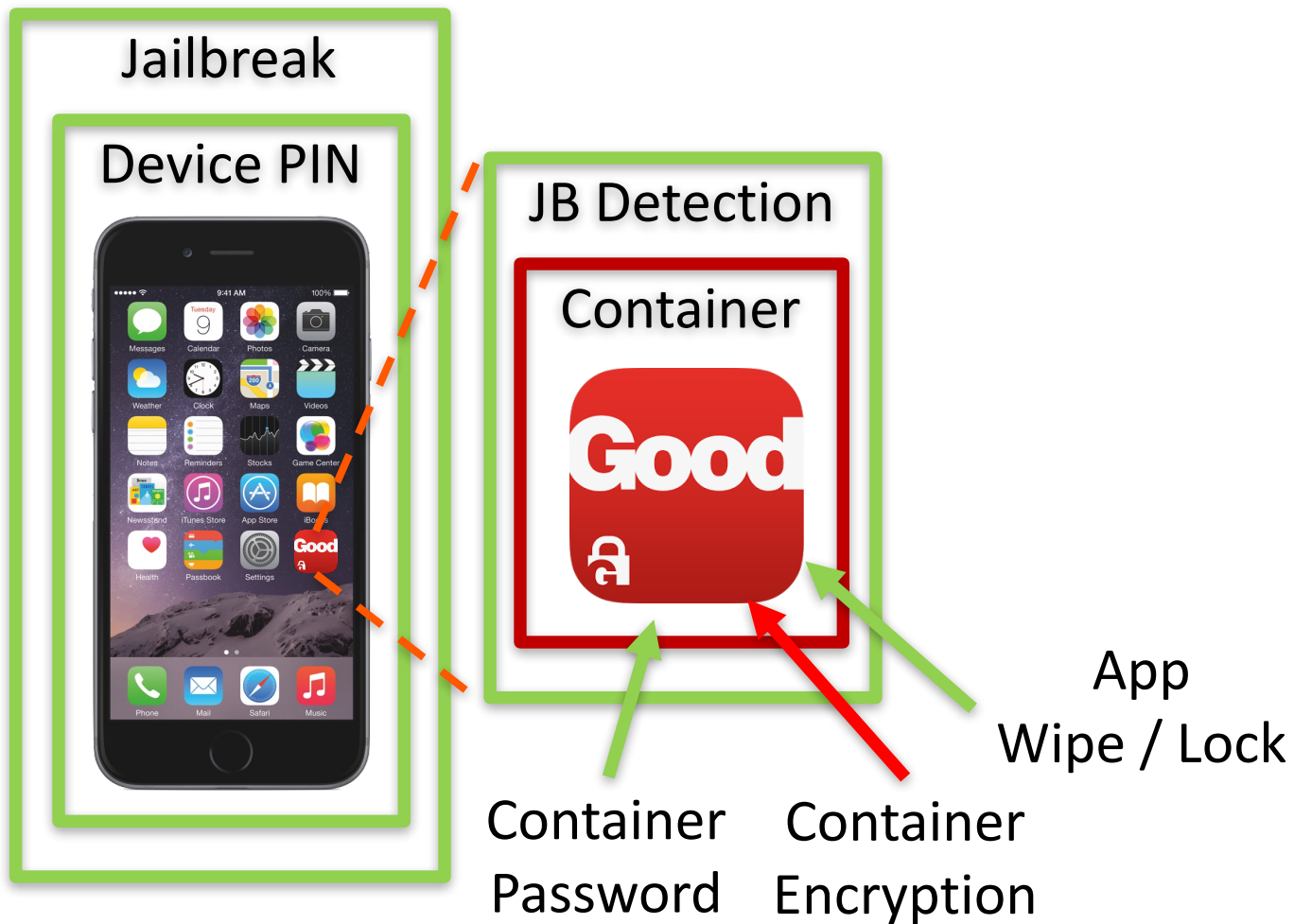
Disable App Lock & Device Wipe


```
Host Directory Quick Connection Disconnect Scroll Back as Window Clear Scroll Buffer Show Stream Capture Paste Download Upload Send Textfile
127.0.0.1:2222
About these Buttons Send "exit<enter>" Call Host from Host Directory Run Sample Script
Jun 9 10:57:06 iPhone kernel[0]: xpcproxy[1987] Container: /private/var/mobile/Containers/Data/Application/DCE8A4E0-B944-49F1-8267-1A22347EFDE4 (sandbox)
Jun 9 10:57:06 iPhone locationd[105]: Gesture EnabledForTopClient: 0, EnabledInDaemonSettings: 0
Jun 9 10:57:07 iPhone Good[1987]: MS:Notice: Injecting: com.good.gmmiphone [Good] (1140.10)
Jun 9 10:57:07 iPhone Good[1987]: MS:Notice: Loading: /Library/MobileSubstrate/DynamicLibraries/ihack.dylib
Jun 9 10:57:07 iPhone Good[1987]: objc[1987]: Class GCDAsyncReadPacket is implemented in both /private/var/mobile/Containers/Bundle/Application/5B296DF0-B711-4096-BFAB-C19DD20B4D36/Good.app/Good and /Library/MobileSubstrate/DynamicLibraries/ihack.dylib. One of the two will be used. Which one is undefined.
Jun 9 10:57:07 iPhone Good[1987]: objc[1987]: Class GCDAsyncWritePacket is implemented in both /private/var/mobile/Containers/Bundle/Application/5B296DF0-B711-4096-BFAB-C19DD20B4D36/Good.app/Good and /Library/MobileSubstrate/DynamicLibraries/ihack.dylib. One of the two will be used. Which one is undefined.
Jun 9 10:57:07 iPhone Good[1987]: objc[1987]: Class GCDAsyncSpecialPacket is implemented in both /private/var/mobile/Containers/Bundle/Application/5B296DF0-B711-4096-BFAB-C19DD20B4D36/Good.app/Good and /Library/MobileSubstrate/DynamicLibraries/ihack.dylib. One of the two will be used. Which one is undefined.
Jun 9 10:57:07 iPhone Good[1987]: objc[1987]: Class GCDAsyncSocket is implemented in both /private/var/mobile/Containers/Bundle/Application/5B296DF0-B711-4096-BFAB-C19DD20B4D36/Good.app/Good and /Library/MobileSubstrate/DynamicLibraries/ihack.dylib. One of the two will be used. Which one is undefined.
Jun 9 10:57:07 iPhone Good[1987]: #####
Jun 9 10:57:07 iPhone Good[1987]:
Jun 9 10:57:07 iPhone Good[1987]:  _ _ _ _ _ ( ) _ _ _ _ _ / / _ _ _ _ _
Jun 9 10:57:07 iPhone Good[1987]:  \ \ / / / / / / / / / / / / / / / / \ \ / /
Jun 9 10:57:07 iPhone Good[1987]:  _ / / / / / / / / / / / / / / / / \ \ / /
Jun 9 10:57:07 iPhone Good[1987]: #####
Jun 9 10:57:07 iPhone Good[1987]: ##### Entry Point #####
Jun 9 10:57:07 iPhone Good[1987]: HTTPServer: Started HTTP server on port 80
```





- ✓ Device PIN
- ✓ Jailbreak
- ✓ Jailbreak Detection
- ✓ Container Password
- ✗ Container Encryption
- ✓ App Wipe / Lock



Containerization

Host Directory Quick Connection Disconnect Scroll Back as Window Clear Scroll Buffer Show Stream Capture Paste Download Upload Send Textfile Start RE

127.0.0.1:2222 (Standard.zoc)

127.0.0.1:2222

About these Buttons Send "exit<enter>" Call Host from Host Directory Run Sample Script

Secure Shell Xterm Zmodem [x] ZOC1506_127.0.0.1_22220109.log

Settings Swizzler

Disable Anti-Debugging

TARGET SELECTION

Select Target Apps

C FUNCTIONS

C Functions 2

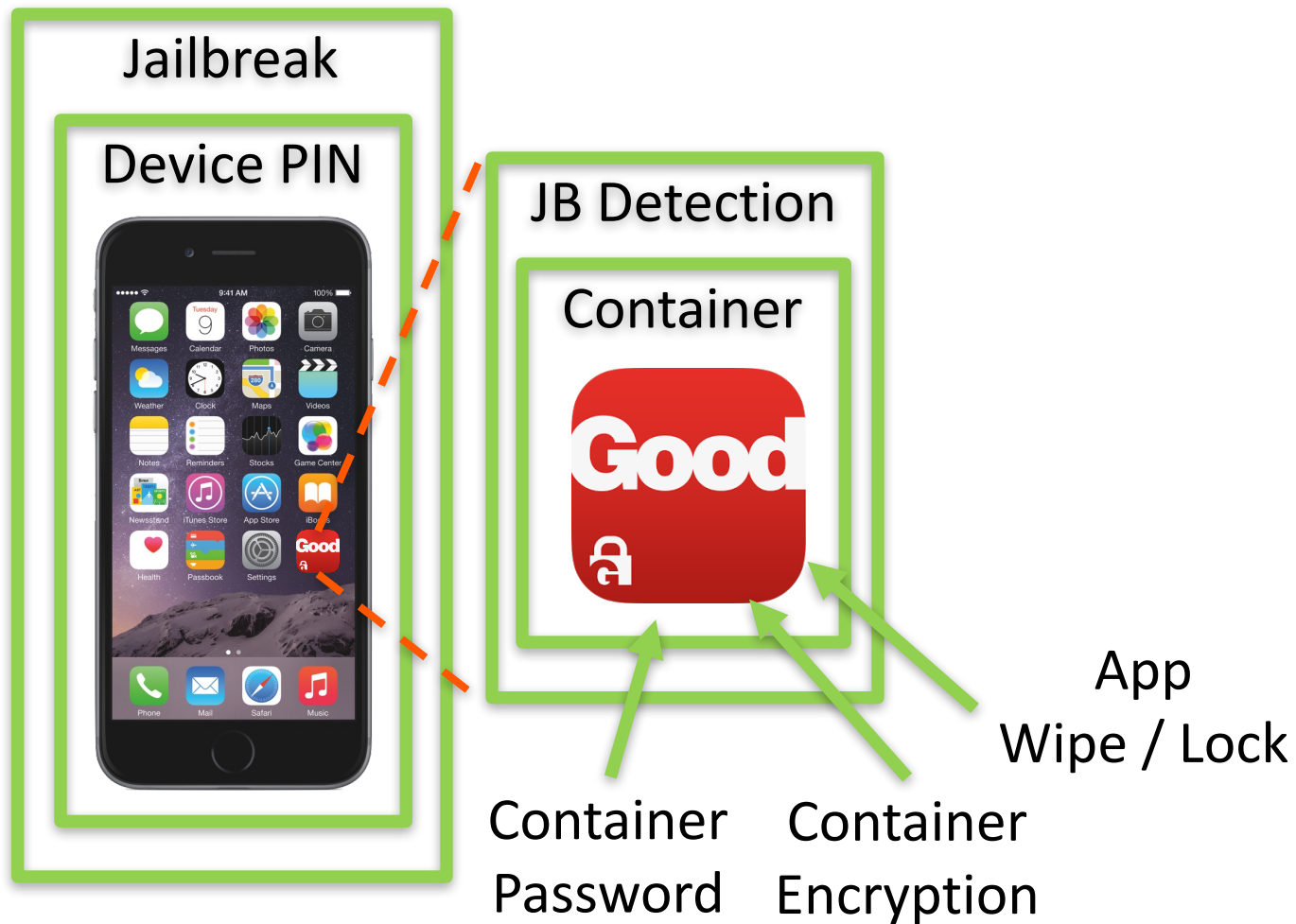
C Functions 3

C Common Crypto

OPENSSL

OpenSSL Functions

CORE FOUNDATION

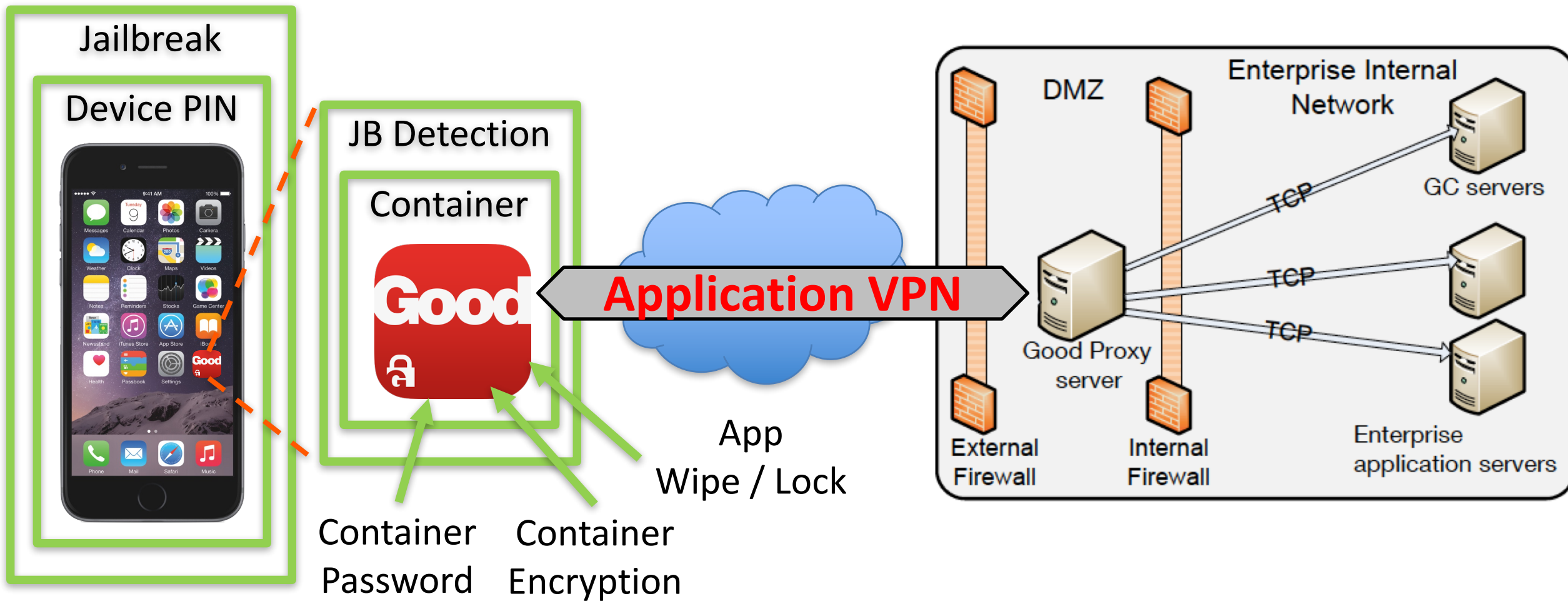


- ✓ Device PIN
- ✓ Jailbreak
- ✓ Jailbreak Detection
- ✓ Container Password
- ✓ Container Encryption
- ✓ App Wipe / Lock

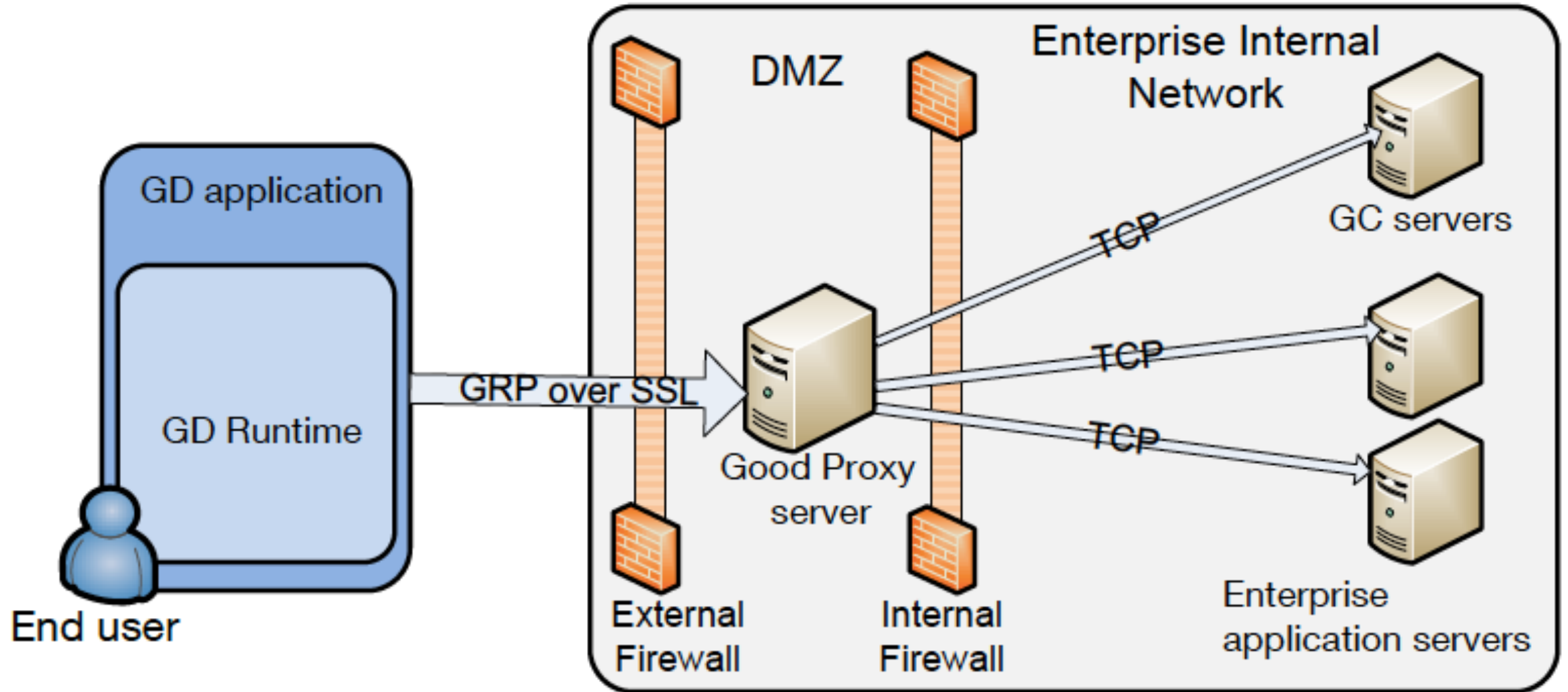
vincent: /Users/vincent/Desktop/iostesting/Good

>>>

Network Attacks

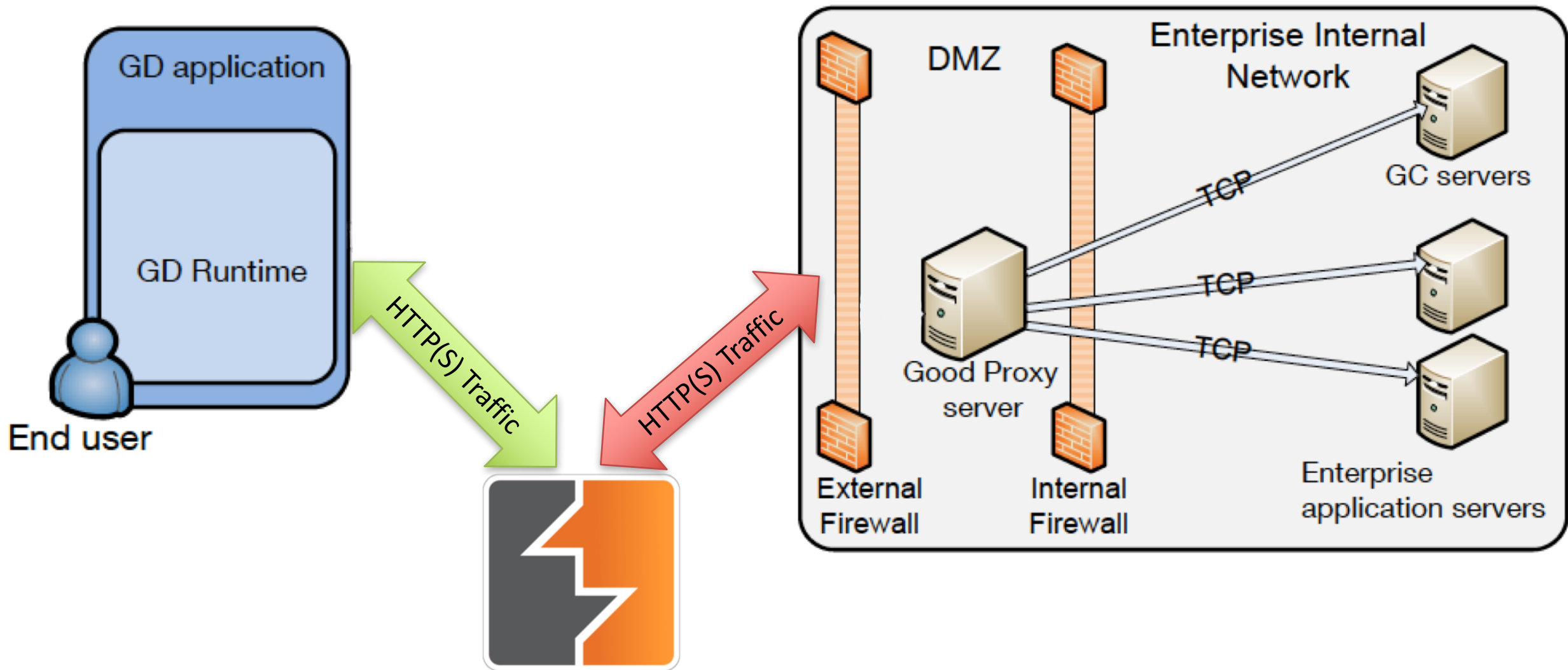


Application VPN

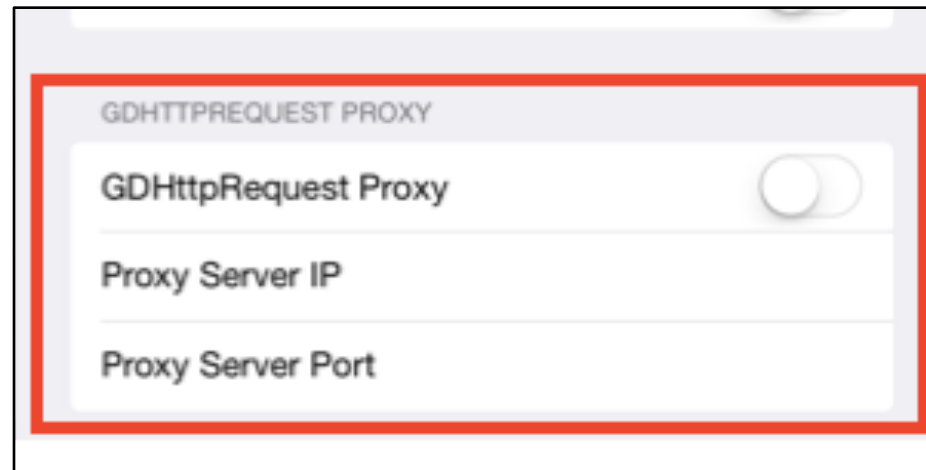


Two methods of communication with the enterprise application server,

1. GDHttpRequest
2. Native URL Loading (NSURL, NSMutableURL, etc.)

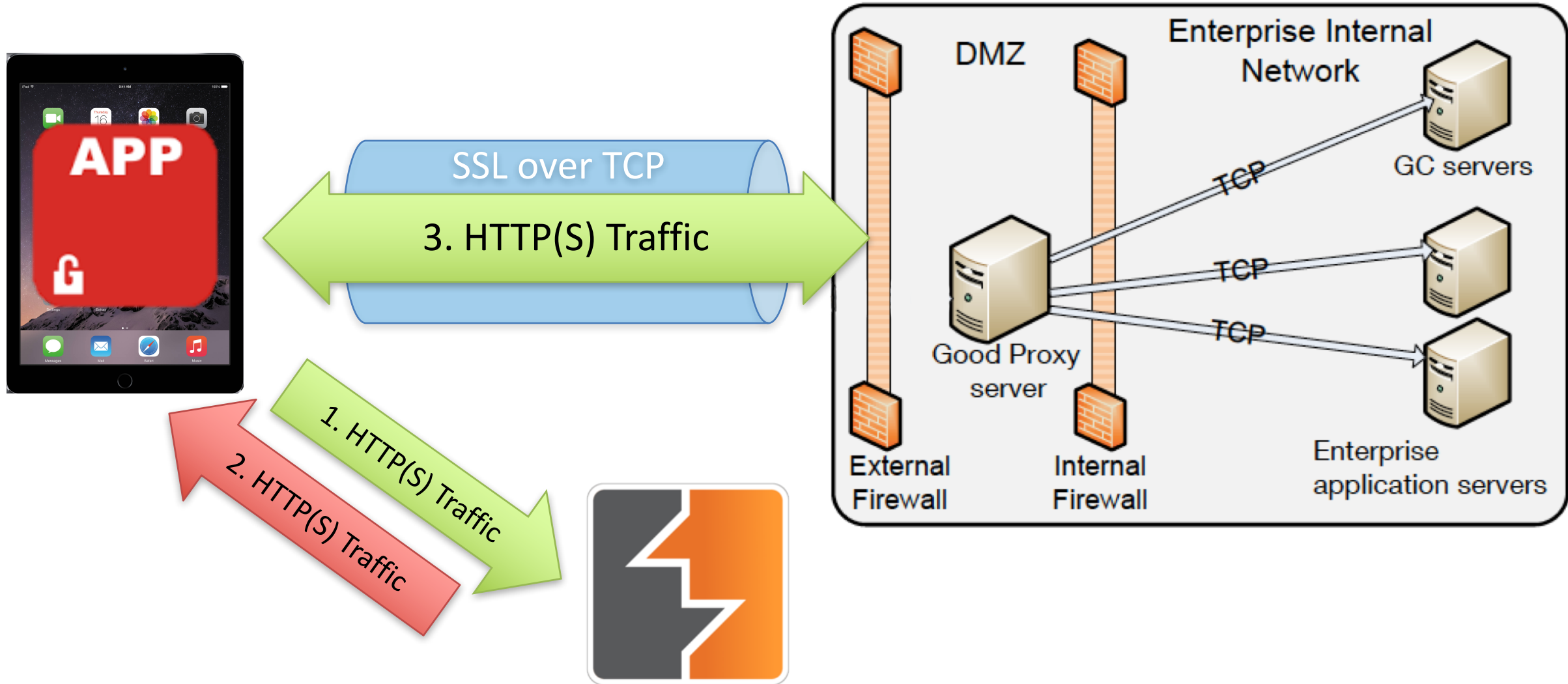


- Part of the GD SDK
 - `#import <GDNETiOS.h>`
- Easy to enable proxy
 - `[GDHttpRequest enableHttpProxy:ip withPort:port];`
 - `[GDHttpRequest disablePeerVerification];`



- Enabled via GDURLLoadingSystem Class
 - `[GDURLLoadingSystem enableSecureCommunication]`
- Enabled by default
- Proxying traffic is harder
- Doesn't obey iOS network proxy settings
- Swizzle `[NSURLConnection initWithRequest]`

Hooking the Network



QuickTime Player File Edit View Window Help

Burp Suite Professional v1.6.39 - licensed to Vantage Point S

Burp Intruder Repeater Window Help

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Ale

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status
---	------	--------	-----	--------	--------	--------

9:41 am 18% Wed 7:49 pm 100%

Good Access gd_test

iFile Settings Safari

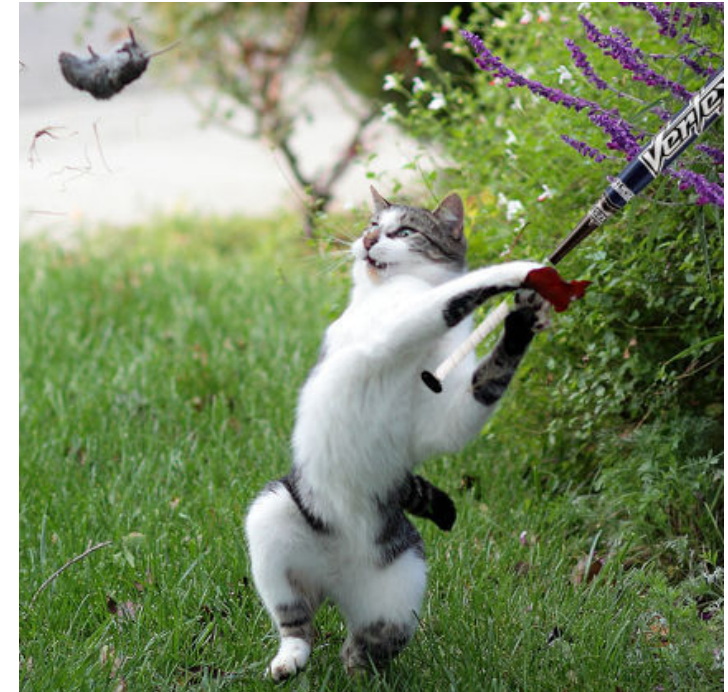
Mac OS X dock with various application icons including Finder, Spotlight, Safari, Mail, and others.

Does everything suck?

- Local device access is important, but remote attacks possible.
 - <https://www.youtube.com/watch?v=STIHO2XOOiM>
- Employee Education.
 - Be careful of USB chargers. BadUSB.
- Intranet == Internet
- Additional security checks on apps

Take Aways!

- Think outside the box to break the box!
- BYOD Policy helps to a certain extent, but such attacks will always be possible.
- Do not blindly trust what the vendors sell you.
- <https://github.com/vtky/Swizzler>



Thank You!



vincent.vtky@outlook.com



<https://www.linkedin.com/in/vincenttky>



@vincent_tky