
Check Point
SOFTWARE TECHNOLOGIES LTD.
ENTERPRISE APPS:
BYPASSING THE IOS GATEKEEPER
Ohad Bobrov
Avi Bashan

AGENDA

- iOS Ecosystem overview
- Enterprise Apps in the iOS Ecosystem
- Bypassing the Gatekeeper
- Conclusions
- Q&A

ABOUT US

OHAD BOBROV

- Over a decade of experience researching and working in the mobile security space
- Former Founder & CTO @Lacoon Mobile Security
- Mobile Threat Prevention Area Manager @Check Point

AVI BASHAN

- Security researcher for over a decade in the PC and mobile areas
- Former CISO & Security Researcher @Lacoon
- Mobile Dynamic Analysis Team Leader @Check Point

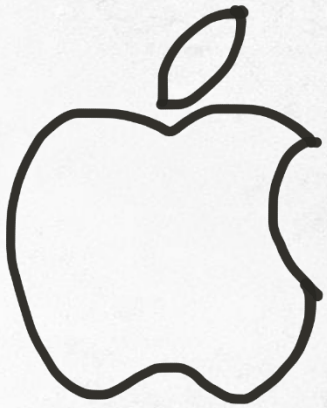
THE iOS ECOSYSTEM

IOS IS A MODERN OPERATING SYSTEM

- Sandboxing capabilities
- Resources access requires permission
- Signed code verification

MANAGED APP PUBLISHING PROCESS

- Central App Store
- Developer registration is required to publish apps
- Anonymous development is not allowed



APPLE'S APP REVIEW PROCESS

EVERY APP PUBLISHED TO THE APP STORE IS REVIEWED

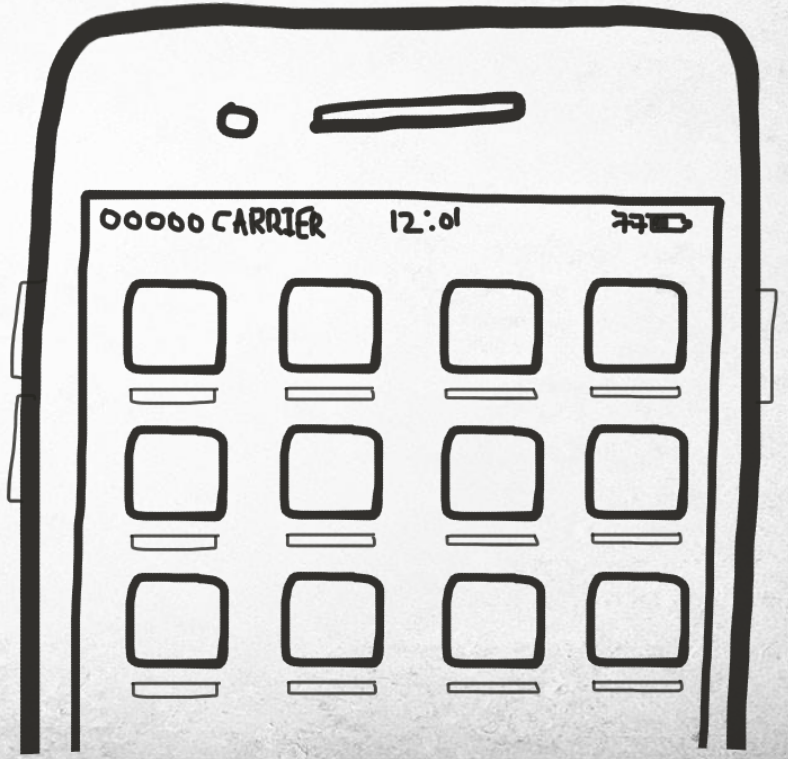
- Automatic process
- Manual Process

APP STORE REVIEW GUIDELINES INCLUDES

- App content
- App behavior
- Bugs
- API abuse
- And more

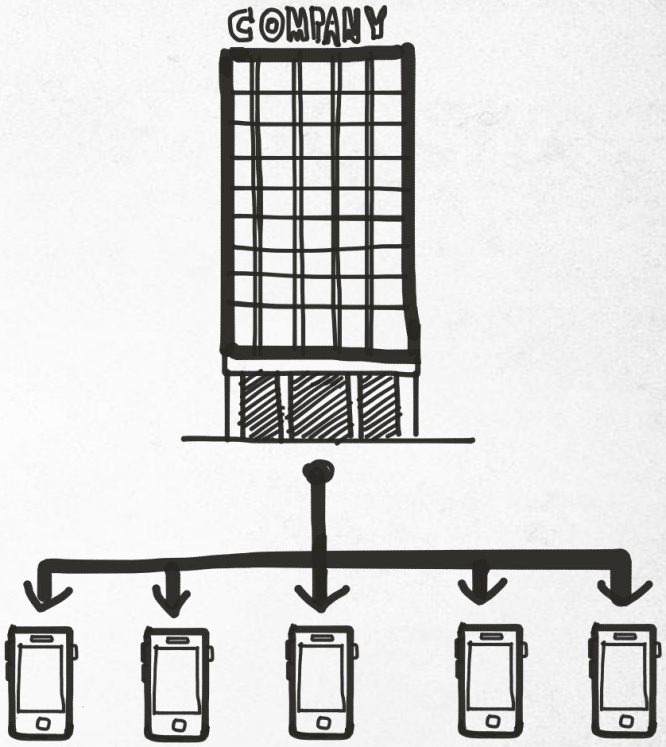
APPLE DEVELOPER ENTERPRISE PROGRAM
MOTIVATION

- Exposure of proprietary In-House Apps
- Slow review process



APPLE DEVELOPER ENTERPRISE PROGRAM

- Requires **signing** with a special **enterprise certificate**
- An enterprise needs to **acquire** a certificate
- Program is for **internal** enterprise use only
- Apps can be published **directly** to Any iOS device from corporate server
- App **is not reviewed** by Apple



CASE SCENARIO

FORTUNE 100 COMPANY

~5,000 BYOD
devices analyzed

RESULT WERE SURPRISING:

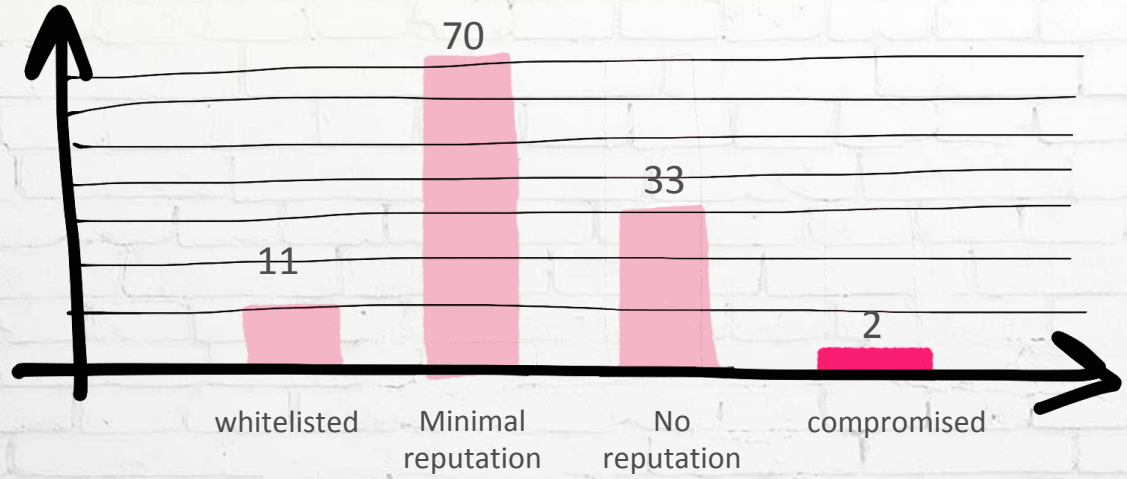
- 318 unique enterprise apps found
- 116 unique enterprise certificates were used

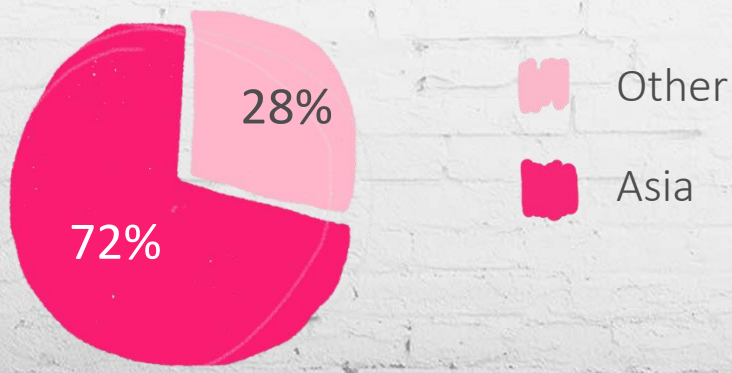
CASE SCENARIO - FORTUNE 100 COMPANY

GOAPP SRL	Mobvantage Marketing Ltd.
MCE SYS LTD	GF Securities Co., Ltd.
Miracle Intelligent Network Co., Ltd.	Qingdao Qingqi Industry Co., Ltd.
QIAO BANG LIMITED	FitnessKeeper, Inc.
National Public Radio, Inc.	Dentsu McGarry Bowen LLC
Operator, Inc.	eVigilo Ltd.
Phind Corp.	Shanghai Yike Automation Technology Co., Ltd.
Proving Ground, LLC.	Humin Inc
Dropbox, Inc.	Hundsun Technologies Inc.,
Quoord Systems Limited	Shenzhen Sunline Tech Co., Ltd.
Huatai Securities Co.,Ltd.	Shenzhen Baite Gifts Co., Ltd.
R/GA Media Group Inc.	Dongguan Chiting Trading Co., Ltd.
Readdle Inc.	Gameview sdn bhd
Reserve Media, Inc	Hangzhou HR Software Co., Ltd.
S.F. EXPRESS GROUP CO., LTD.	Fuzhou Yewen Advertising Co., Ltd.
Seasonal Spring LLC	Shanghai Soco Software Co., Ltd.
Shanghai Column Fashion Co., Ltd.	Shanghai 37 Degree Technology Co., Ltd.

Who can tell right from wrong?

NON APPSTORE CERTIFICATES





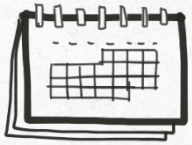
WHAT CAN ENTERPRISE APPS DO?

ABUSE PUBLIC APIs


Microphone

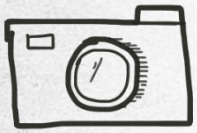

Location


Address Book


Calendar


Pictures

ABUSE PUBLIC APIs


Take Screenshot


List Apps

EXPLOIT


Jailbreak


Masque

What LIMITS the enterprise app developer from doing all of those actions?

Trust*

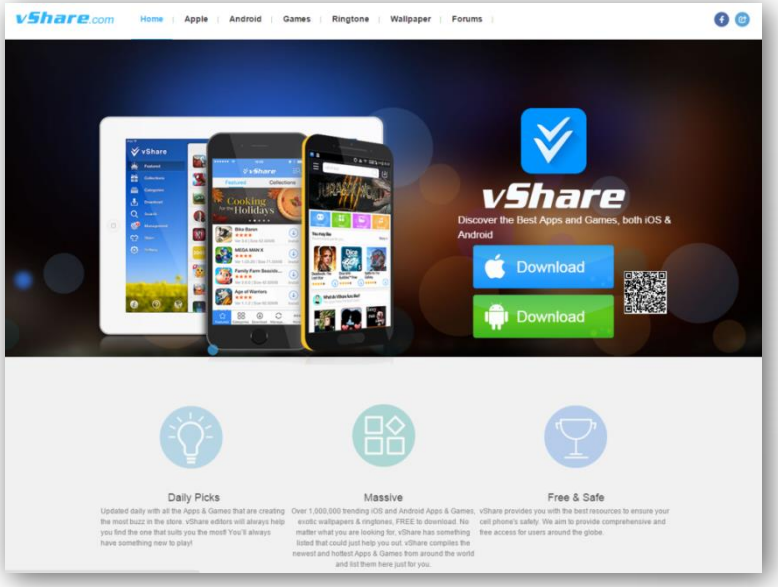
* And a user agreement


NO MALWARES
BECAUSE OF A USER AGREEMENT

ENTERPRISE CERTIFICATE ABUSE 3RD MARKET

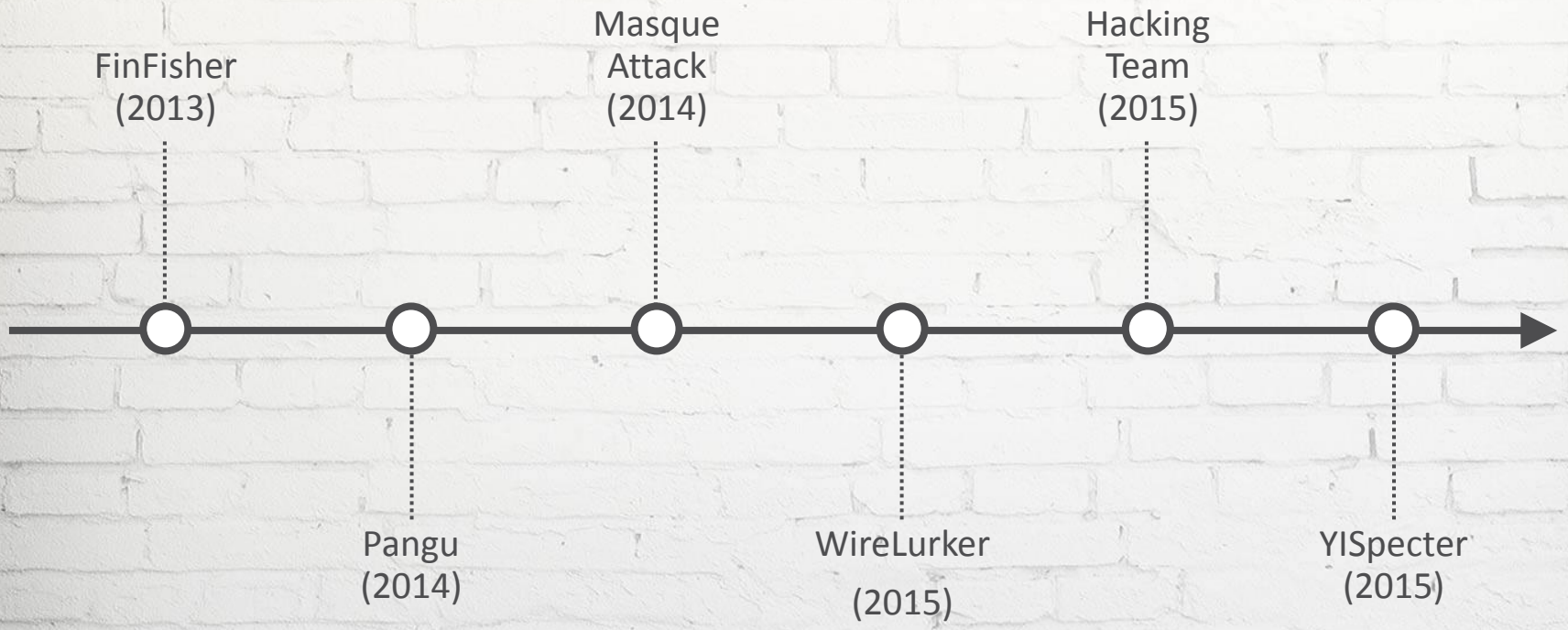
- Third party App Stores use enterprise certificates to distribute apps.
- They often re-pack applications and distribute them.
- This is not a minor phenomenon

25PP – more than 40M users, 8M downloads a day in 2013



vShare – 40M users, 25% iOS. 15,000 iOS apps.

ENTERPRISE CERTIFICATE ABUSE (2)

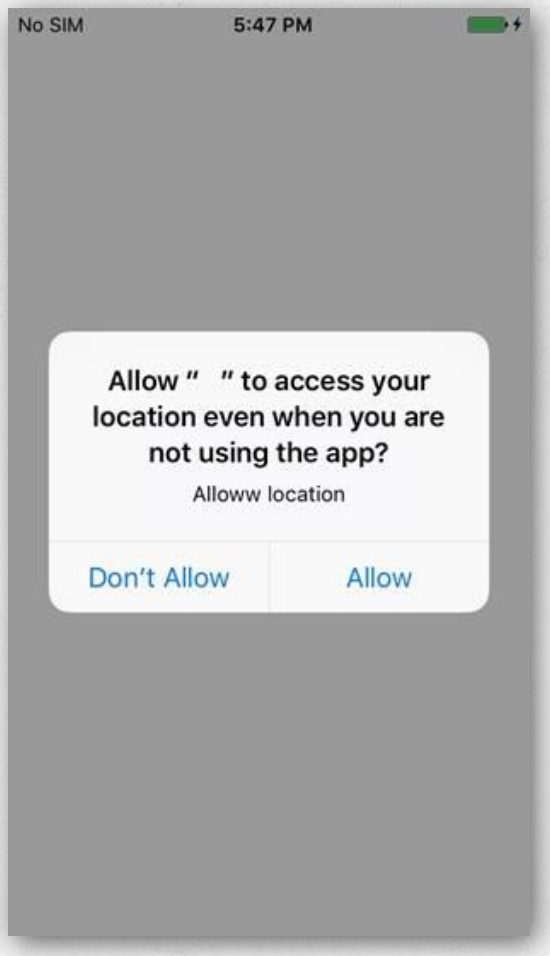


HACKING TEAM (1)

- Hacking Team got breached in July 2015
- iOS RAT source code was exposed
- Used an enterprise certificate to install malware
- Disguised as a newspaper in native Newsstand app
- Asks for extensive permissions
- Installs a key logger
- Leveraging masque attack

]HackingTeam[

HACKING TEAM (2)



HACKING TEAM (3)

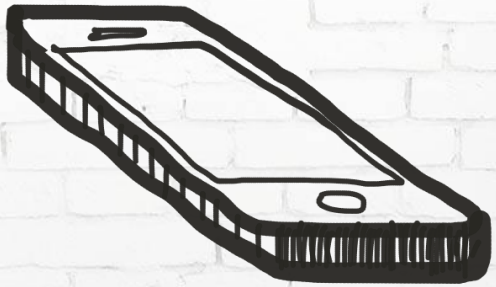
```
- (void)startBackgroundSynch
{
    NSLog(@"Synch restarted!");

    dispatch_async(dispatch_get_global_queue(DISPATCH_QUEUE_PRIORITY_DEFAULT, 0), ^{
        while (self.jobExpired == NO)
        {
          [NSThread sleepForTimeInterval:gSynchDelay];

          gMainView = (ViewController*)[UIApplication sharedApplication].keyWindow.rootViewController;

          // Grab New Calendar and Contacts
          [gMainView getABContatcs];
          [gMainView getCalendars];

          [NSThread sleepForTimeInterval:1];

          // Synch to server
          [self performSync];
        }

        @synchronized(self)
        {
            self.jobExpired = NO;
        }
    });
}
```

LET'S TALK ABOUT MDMS

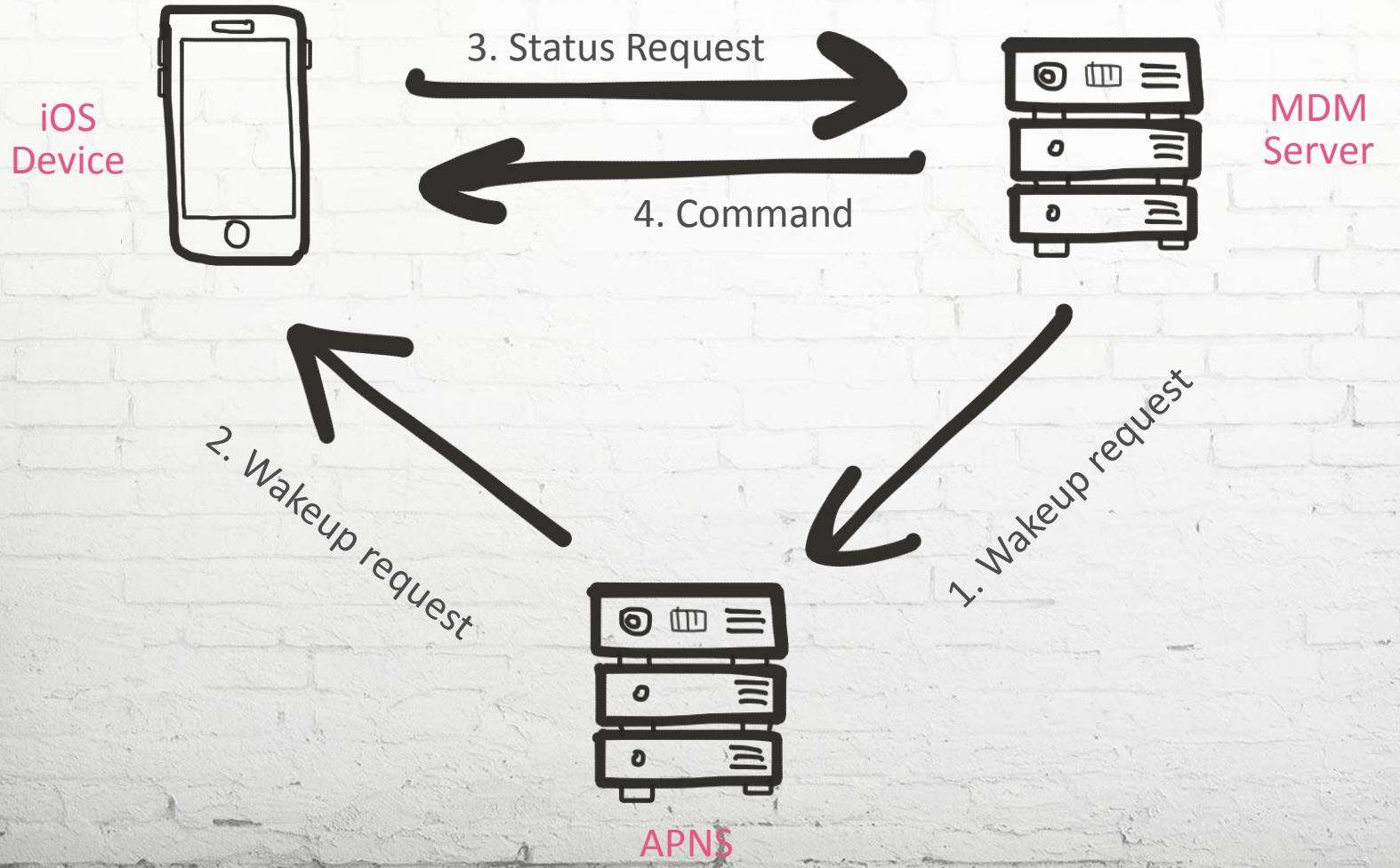
MOBILE DEVICE MANAGEMENT

Used by enterprises to support BYOD

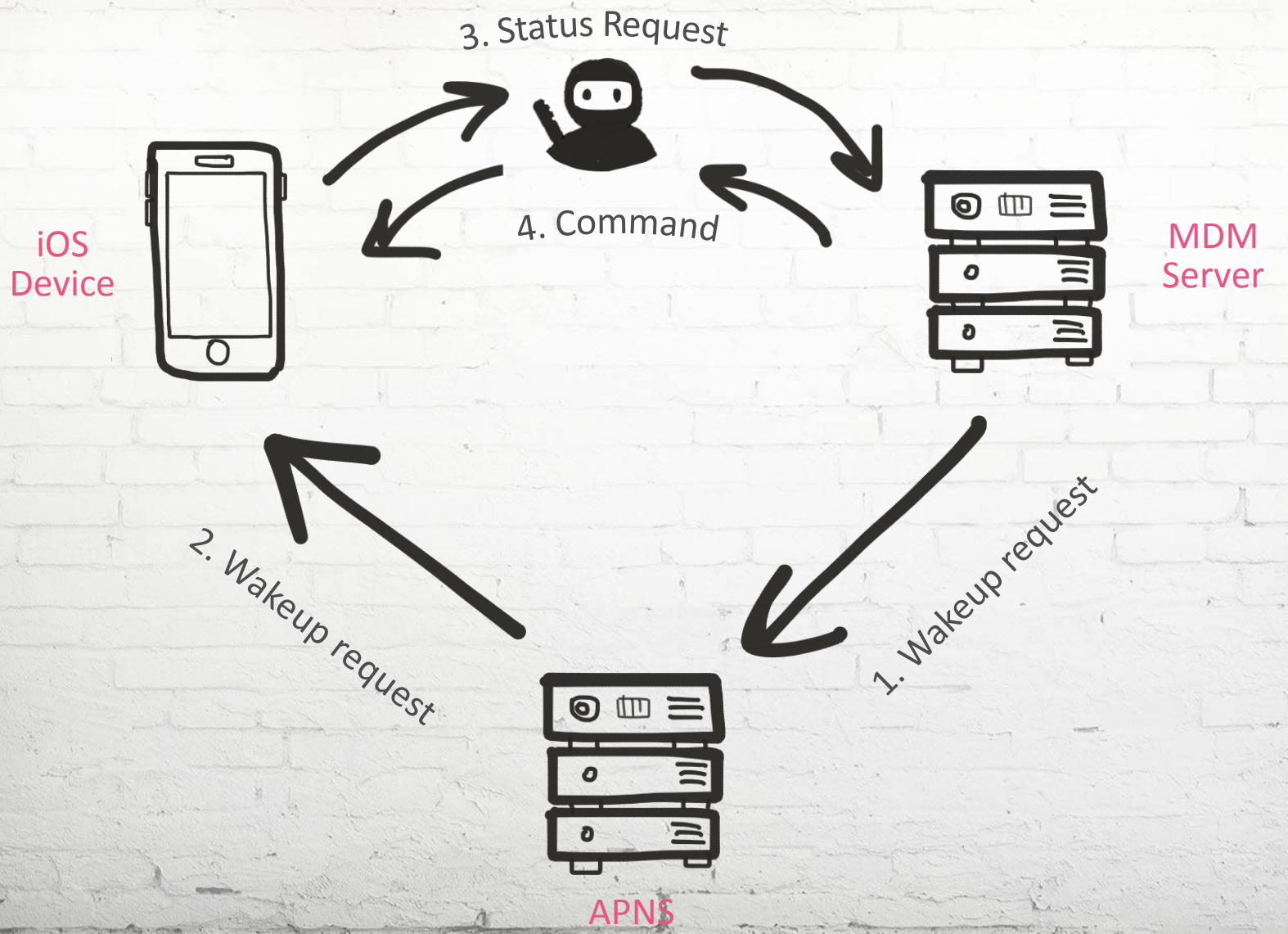
- Deploy security policy
- Remote wipe
- Install applications
- Etc..



MOBILE DEVICE MANAGEMENT (2)



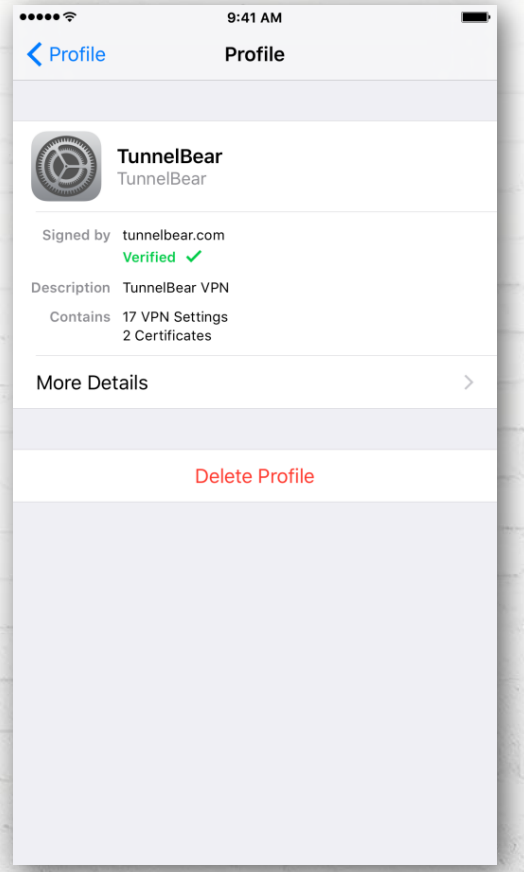
MOBILE DEVICE MANAGEMENT (2)



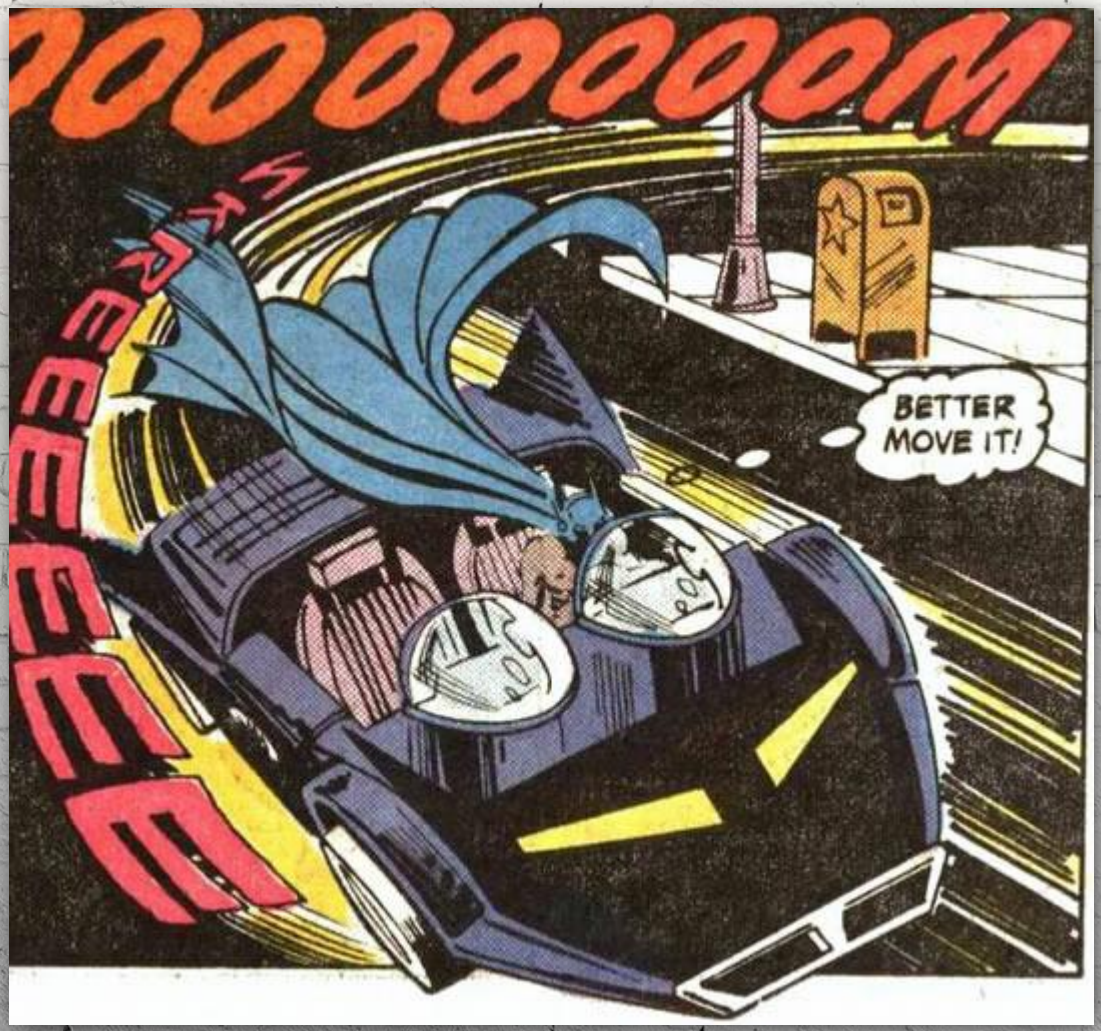
MiTM MDM

Install an iOS configuration profile:

- Can be used to route traffic through VPN/Proxy
- Can install root CA certificates
- Easy to deploy through phishing attacks



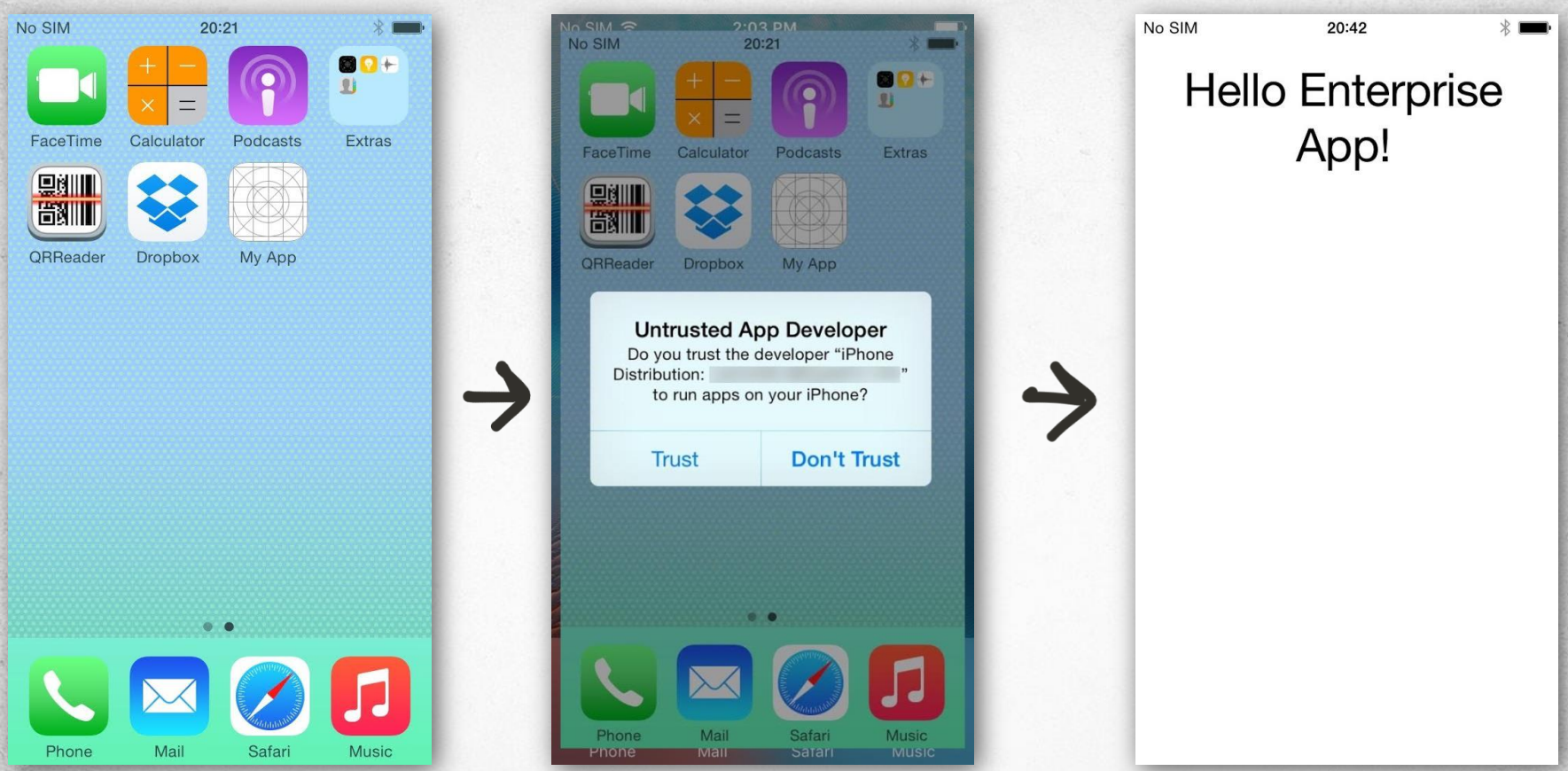
GOING BACK TO ENTERPRISE APPS



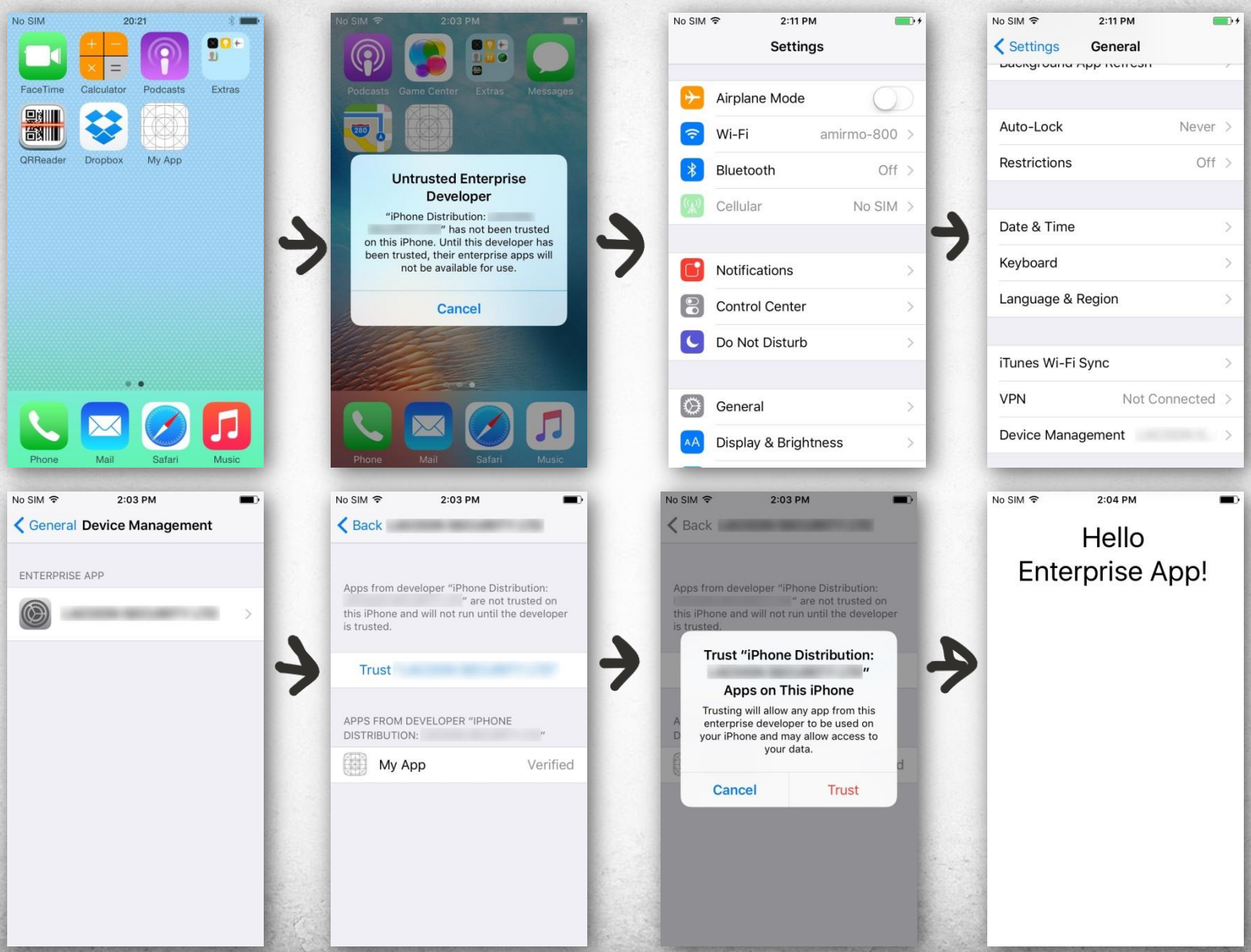
SECURITY FEATURES INTRODUCED IN iOS 9

- Apple understood the problem which lies in enterprise apps
- However, Enterprise apps cannot be eliminated
- Increase the complexity of executing enterprise apps
- Apps are cannot execute without explicit user trust

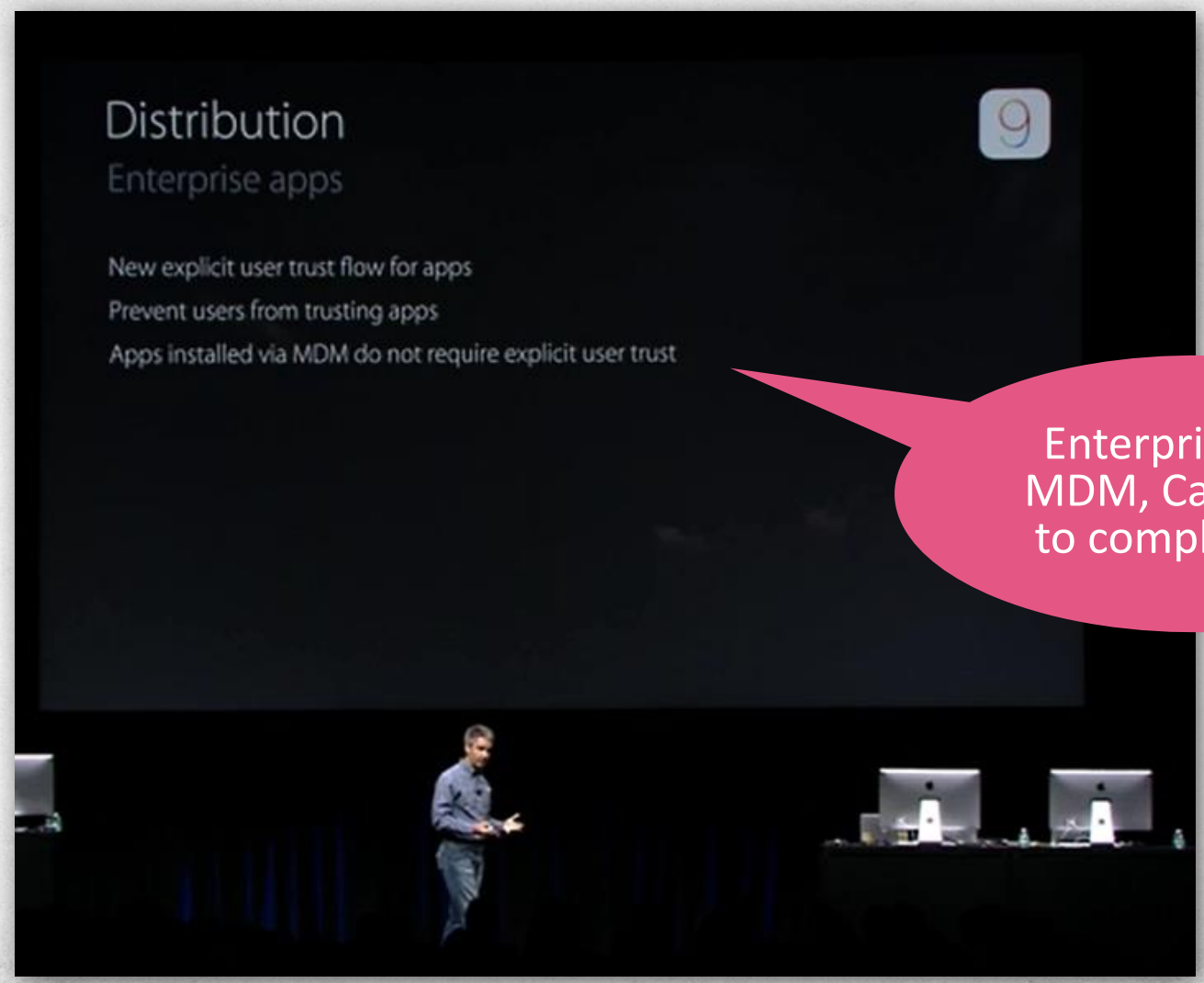
iOS =< 8


No SIM
20:21
FaceTime
Calculator
Podcasts
Extras
QRReader
Dropbox
My App
Phone
Mail
Safari
Music
Untrusted App Developer
Do you trust the developer "iPhone Distribution: [redacted]" to run apps on your iPhone?
Trust
Don't Trust
No SIM
20:42
Hello Enterprise App!

iOS >= 9


No SIM 20:21
FaceTime Calculator Podcasts Extras
QRReader Dropbox My App
Phone Mail Safari Music
No SIM 2:03 PM
Podcasts Game Center Extras Messages
Untrusted Enterprise Developer
"iPhone Distribution: [redacted]" has not been trusted on this iPhone. Until this developer has been trusted, their enterprise apps will not be available for use.
Cancel
No SIM 2:11 PM
Settings
Airplane Mode
Wi-Fi amirmo-800
Bluetooth Off
Cellular No SIM
Notifications
Control Center
Do Not Disturb
General
Display & Brightness
No SIM 2:11 PM
Settings General
Auto-Lock Never
Restrictions Off
Date & Time
Keyboard
Language & Region
iTunes Wi-Fi Sync
VPN Not Connected
Device Management
No SIM 2:03 PM
General Device Management
ENTERPRISE APP
No SIM 2:03 PM
Back
Apps from developer "iPhone Distribution: [redacted]" are not trusted on this iPhone and will not run until the developer is trusted.
Trust [redacted]
APPS FROM DEVELOPER "IPHONE DISTRIBUTION: [redacted]"
My App Verified
No SIM 2:03 PM
Back
Apps from developer "iPhone Distribution: [redacted]" are not trusted on this iPhone and will not run until the developer is trusted.
Trust "iPhone Distribution: [redacted]"
Apps on This iPhone
Trusting will allow any app from this enterprise developer to be used on your iPhone and may allow access to your data.
Cancel Trust
No SIM 2:04 PM
Hello Enterprise App!

WWDC 15



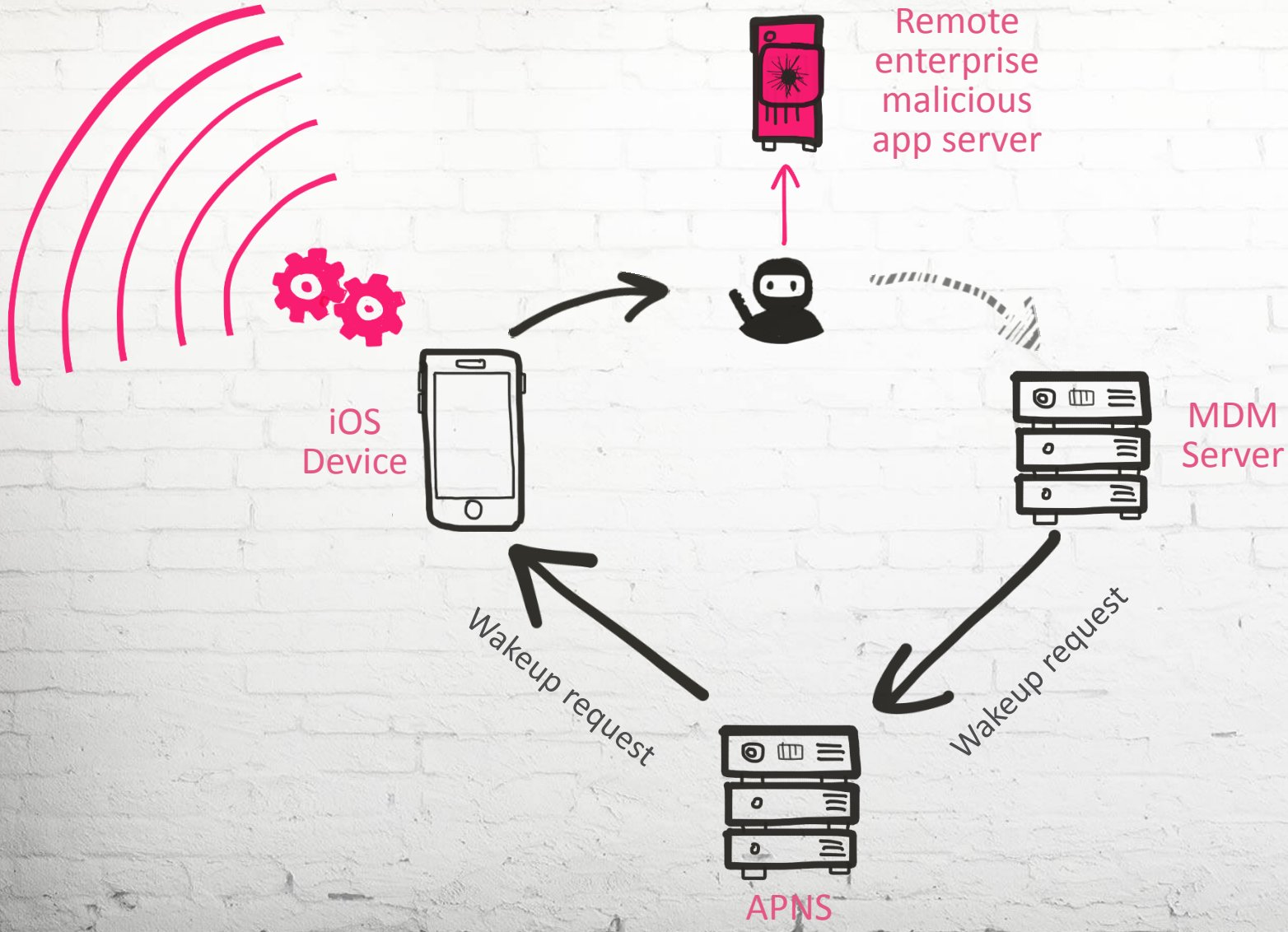
Enterprise uses MDM, Can't do it to complicated..


MARIO
X 4
X
TIME
228
X 0
3200

BYPASSING THE GATEKEEPER

- Set up a remote enterprise app server
  - Serves the malicious enterprise app
- Initiate an MiTM attack
  - Wait for a command sent by the MDM server
  - Replace the command with an app install request
  - iOS device will fetch and install the enterprise app
- Enterprise app can now execute without explicit trust
  - User cannot tell the difference between enterprise and App Store app

ATTACK ANATOMY




DEMO

CONCLUSIONS

- Unverified code can be introduced to iOS ecosystem through Enterprise apps
- Non-jailbroken device are exposed to attacks
- Enterprises cannot trust the end user judgment in BYOD environments
- Enterprises should have a clear way to view and assess the enterprise app in their organizations
- MiTM attacks can be leveraged to gain access to a device


QUESTIONS?