



NowSecureTM



The incident response playbook: *For Android and iOS*



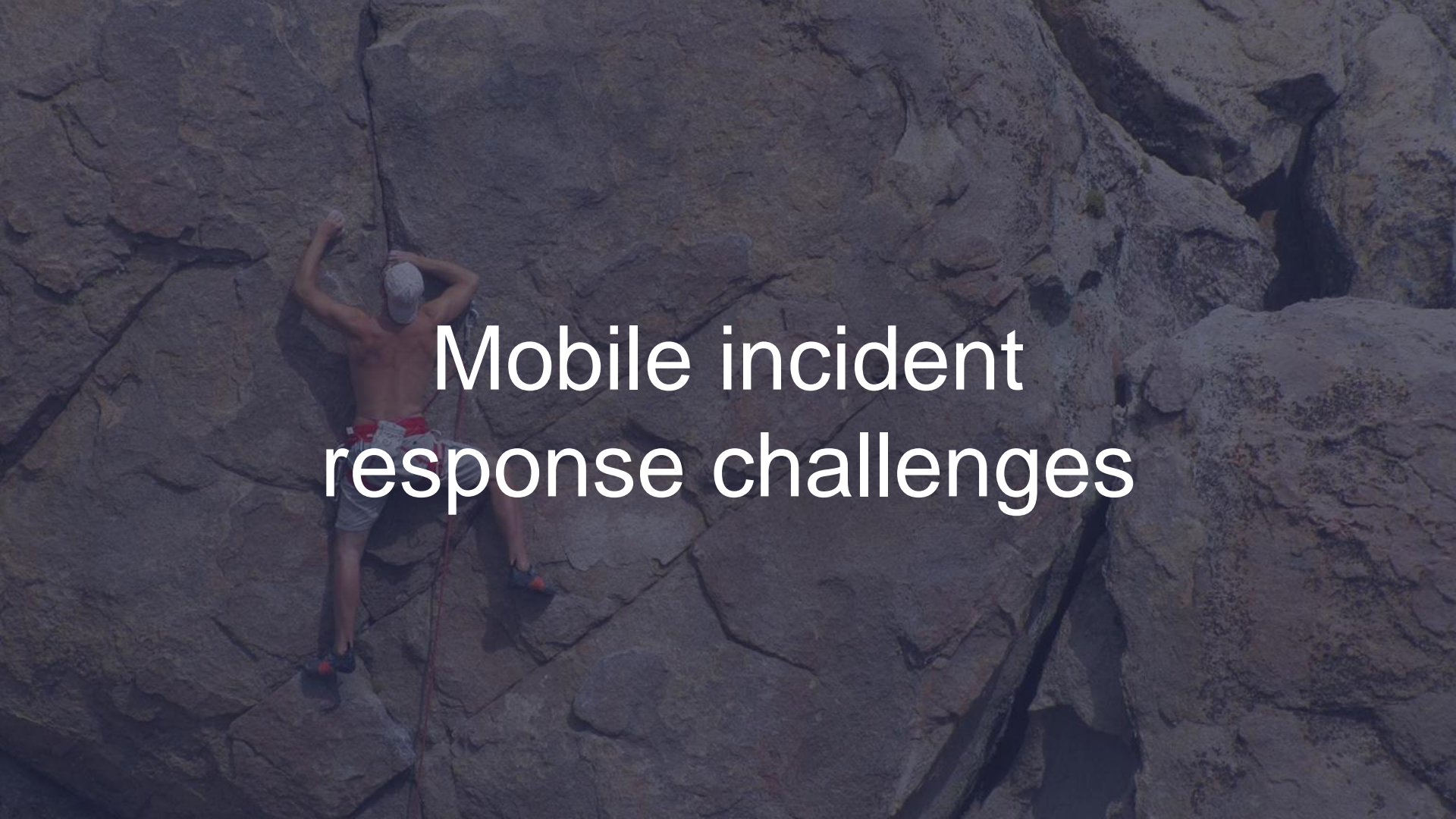
NowSecure™



Andrew Hoog

NowSecure CEO and Co-founder

- Computer scientist & mobile security researcher
- Author of three mobile security books
- Enjoyer of science fiction, running and red wine

A person is seen from behind, climbing a steep, textured rock face. They are wearing a white cap, a red harness, and light-colored shorts. A red rope is visible, extending from the climber down the rock face. The rock surface is rugged with various cracks and crevices. The overall scene is dimly lit, giving it a moody appearance.

Mobile incident response challenges

DFIR professionals vs. giants

Titans of industry, governments, organized crime

- Mobile defenders have few allies
- Apple and Google making strides to make iOS and Android more secure
- Restricted platforms amplify attackers' asymmetric advantage
- (Attackers know something their targets don't)

Broad attack surface

Resulting from large user base, dual-use devices, rapid development, and continuous connectivity

ATTACK SURFACE: THE PHONE



BROWSER

- Phishing
- Framing
- Clickjacking
- Man-in-the-Middle
- Buffer Overflow
- Data Caching



SYSTEM

- No Passcode/Weak Passcode
- iOS Jailbreak
- Android Rooting
- OS Data Caching
- Passwords & Data Accessible
- Carrier-Loaded Software
- No Encryption/Weak Encryption
- User-Initiated Code



PHONE/SMS

- Baseband Attacks
- SMishing



APPS

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Validation
- Config Manipulation
- Dynamic Runtime Injection
- Unintented Permissions
- Escalated Privileges



MALWARE

ATTACK SURFACE: THE NETWORK

- Wi-Fi (No Encryption/Weak Encryption)
- Rogue Access Point
- Pocket Sniffing
- Man-in-the-Middle (MITM)
- Session Hacking
- DNS Poisoning
- SSL Strip
- Fake SSL Certificate



ATTACK SURFACE: THE DATA SERVER

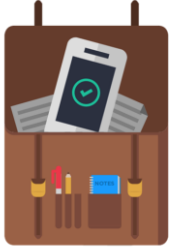
WEB SERVER

- Platform Vulnerabilities
- Server Misconfiguration
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Weak Input Validation
- Brute Force Attacks

DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

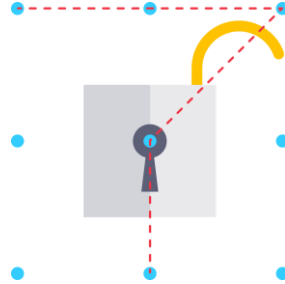
The challenges of mobile IR



DUAL-USE



**ALWAYS-ON
CONNECTIVITY**



**NO ADMIN
ACCESS**



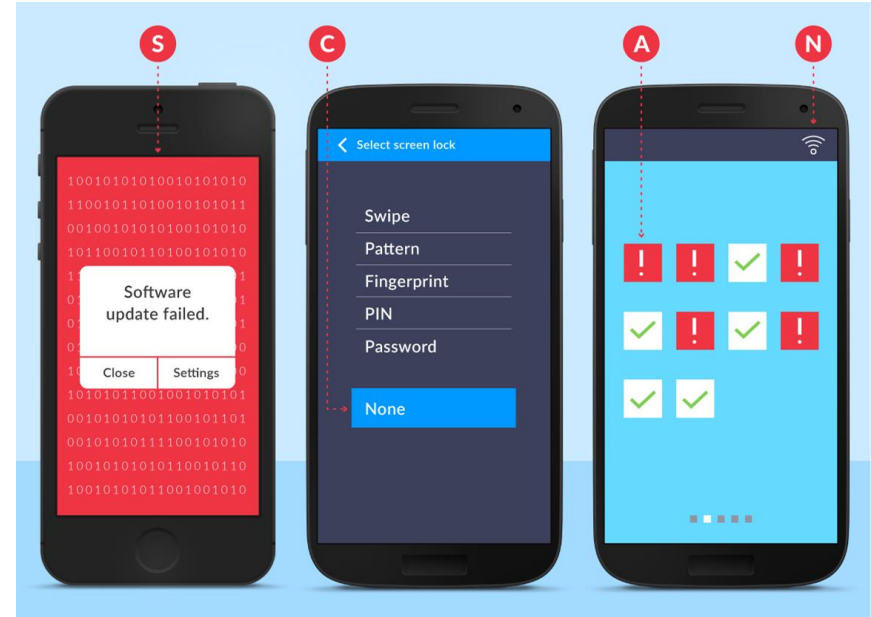
**DIFFERENT
TOOLS**

A dark red brick wall with a visible mortar pattern, serving as the background for the text.

Building blocks for your
mobile incident response plan

You need to start somewhere

- Identify assets:
 - Devices
 - Operating systems
 - Installed apps
- SCAN Principle
 - System
 - Configuration
 - Apps
 - Network
- Historical data is crucial to response



Your mobile IR “jump bag”

Install and configure your tools and know how to use them



**CONTINUAL
ANALYSIS TOOLS**



**ACQUISITION
TOOLS**



**FORENSIC
ANALYSIS TOOLS
(& more)**

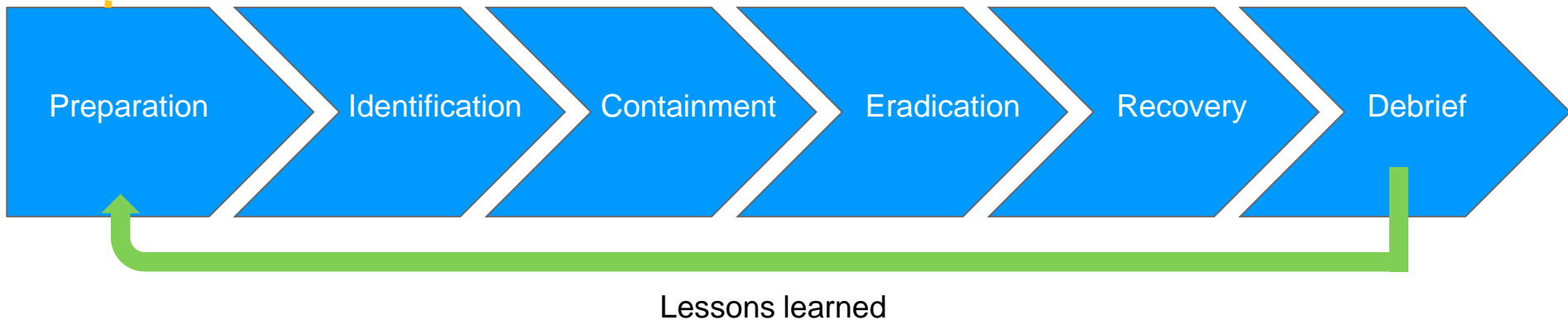
See a detailed list at

<https://www.nowsecure.com/resources/mobile-incident-response/en/tools/index.html>

Phases of incident response

Playbooks are an output of the preparation phase

➤ Playbooks



Great reference: Mason Pokladnik's ["Checklist for incident response capability"](#)

Types of mobile incidents

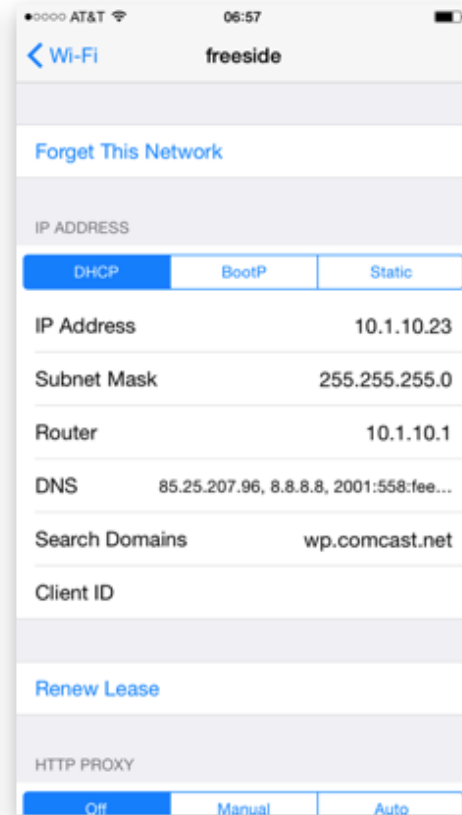
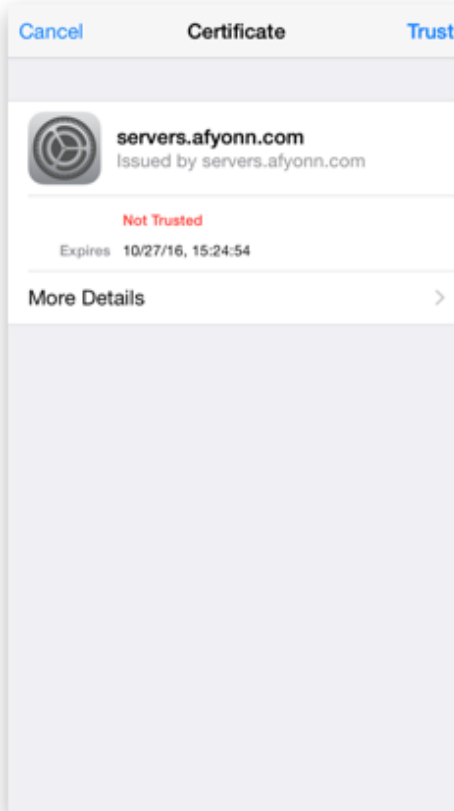
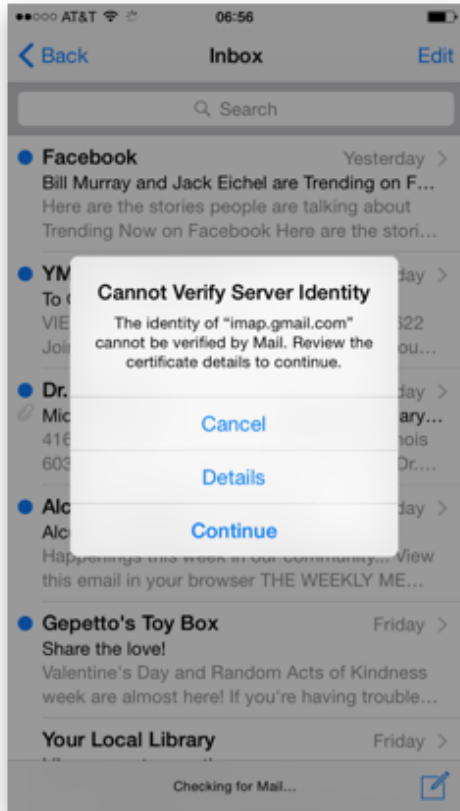
<i>Incident Type</i>	<i>Prevalence</i>	<i>Max Impact</i>	<i>Risk</i>
INTERNAL INVESTIGATION	HIGH	MEDIUM	HIGH
INSIDER ATTACK	MEDIUM	HIGH	HIGH
LOST OR STOLEN DEVICE	HIGH	LOW	MEDIUM
VULNERABLE OR LEAKY APP	MEDIUM	MEDIUM	MEDIUM
MALICIOUS IMPOSTER APP	LOW	HIGH	MEDIUM
DATA BREACH	LOW	HIGH	MEDIUM
DEVICE ACTING SUSPICIOUSLY	MEDIUM	LOW	LOW
MALWARE ON DEVICE	LOW	MEDIUM	LOW








Mobile incident response playbook

It all began on Saturday, February 13






Here's the data you might get from an end user








Step 1 — Identification

 IDENTIFY	<ul style="list-style-type: none">● Device Indicators of Compromise (IoCs)<ul style="list-style-type: none">○ Battery drain○ Unusual network traffic○ Certificate errors○ Unusual log messages○ Crash reports● App reputation monitoring<ul style="list-style-type: none">○ Unauthorized use of brand○ Apps connecting to your transactional servers● User reported
 CONTAIN	
 ERADICATE	
 RECOVER	
 DEBRIEF	






Step 2 — Containment

 IDENTIFY	Once you have identified and logged an incident <ul style="list-style-type: none">• Gain access to device, if possible• Capture device, OS, and app baseline• Determine if network analysis is appropriate• Isolate the device<ul style="list-style-type: none">○ Airplane mode○ Faraday bag○ Etc.• Perform full forensic acquisition
 CONTAIN	
 ERADICATE	
 RECOVER	
 DEBRIEF	






Step 3 — Eradication

 IDENTIFY	<ul style="list-style-type: none">• Analyze attack artifacts• Determine if threat can be removed• Identify all impacted (if malware on app store)• Remove threat or wipe corporate data
 CONTAIN	
 ERADICATE	
 RECOVER	
 DEBRIEF	

Step 4 — Recovery

 IDENTIFY	<p>Mobile recovery typically involves</p> <ul style="list-style-type: none">• Re-provision mobile devices• Ensure attacker didn't move laterally• Monitor accounts and systems connected to mobile device and impacted user(s)• Effectiveness of social engineering attacks is greatly increased
 CONTAIN	
 ERADICATE	
 RECOVER	
 DEBRIEF	

Step 5 — Debriefing

 IDENTIFY	<ul style="list-style-type: none">● Team debrief:<ul style="list-style-type: none">○ What worked, what can be improved○ Policies & procedures changes, user education● Determine IOCs<ul style="list-style-type: none">○ Attribution○ Share threat intel data● Inoculate against future attacks<ul style="list-style-type: none">○ Static signatures generally ineffective○ Focus on anomaly detection○ Shared insights and cross-referenceable data
 CONTAIN	
 ERADICATE	
 RECOVER	
 DEBRIEF	



Don't panic

Andrew Hoog // CEO & Co-founder

NowSecure
ahoog@nowsecure.com
+1.312.878.1100
@ahoog42