

Help! My Mobile Device is Spying on Me

Delivered by Murray Goldschmidt, Chief Operating Officer

AusCERT 2012 Conference, 17 May 2012

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney

Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne

Level 10, 401 Docklands Drv
Docklands VIC 3008
Australia

T: 1300 922 923

T: +61 (0) 2 9290 4444

F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au

www.senseofsecurity.com.au

ABN: 14 098 237 908

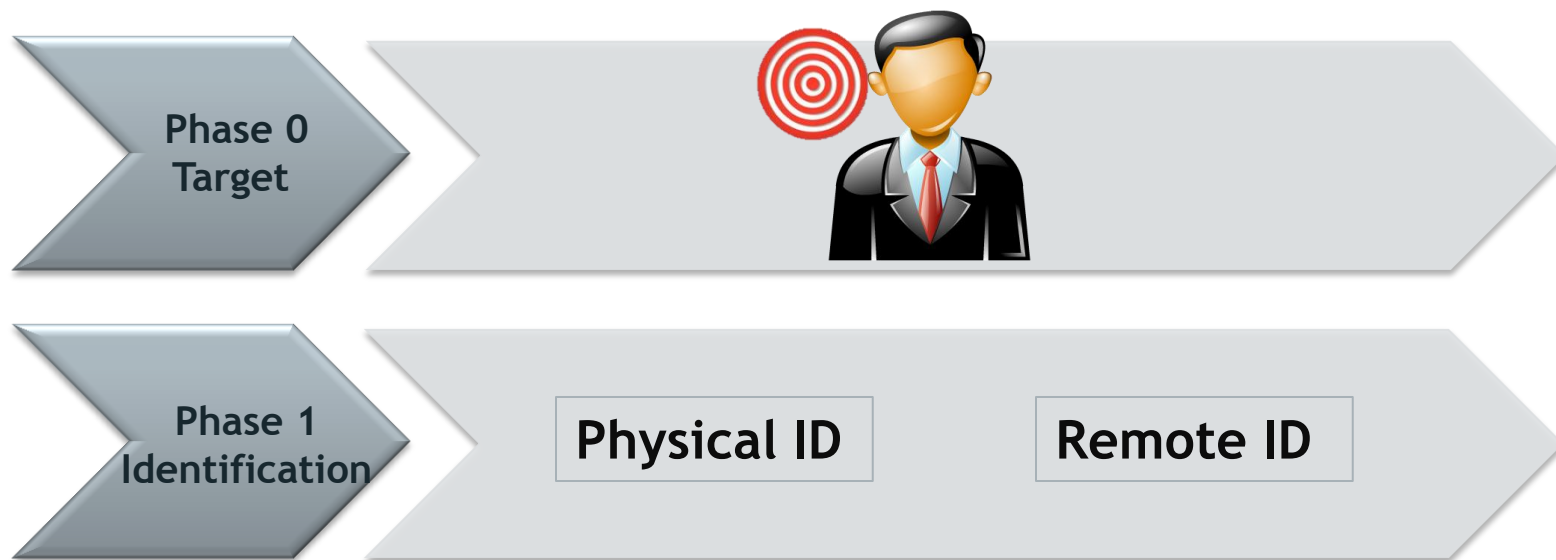
Our “Targeted Voice Recorder” research addresses

- Relevance - Extent of exposure
- Simplicity - Anatomy of the attack
- Protection - Mitigating controls

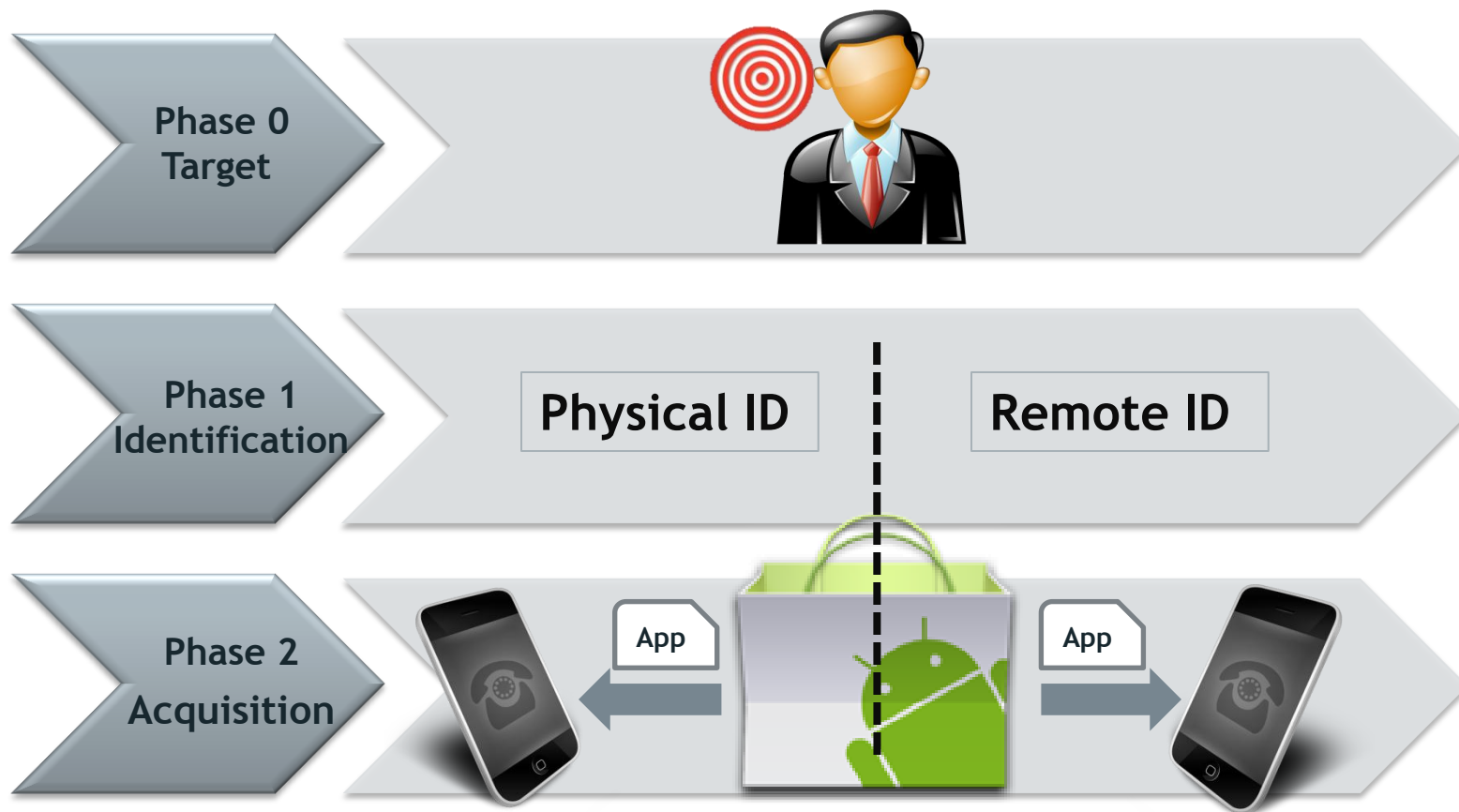
High Level Process Flow



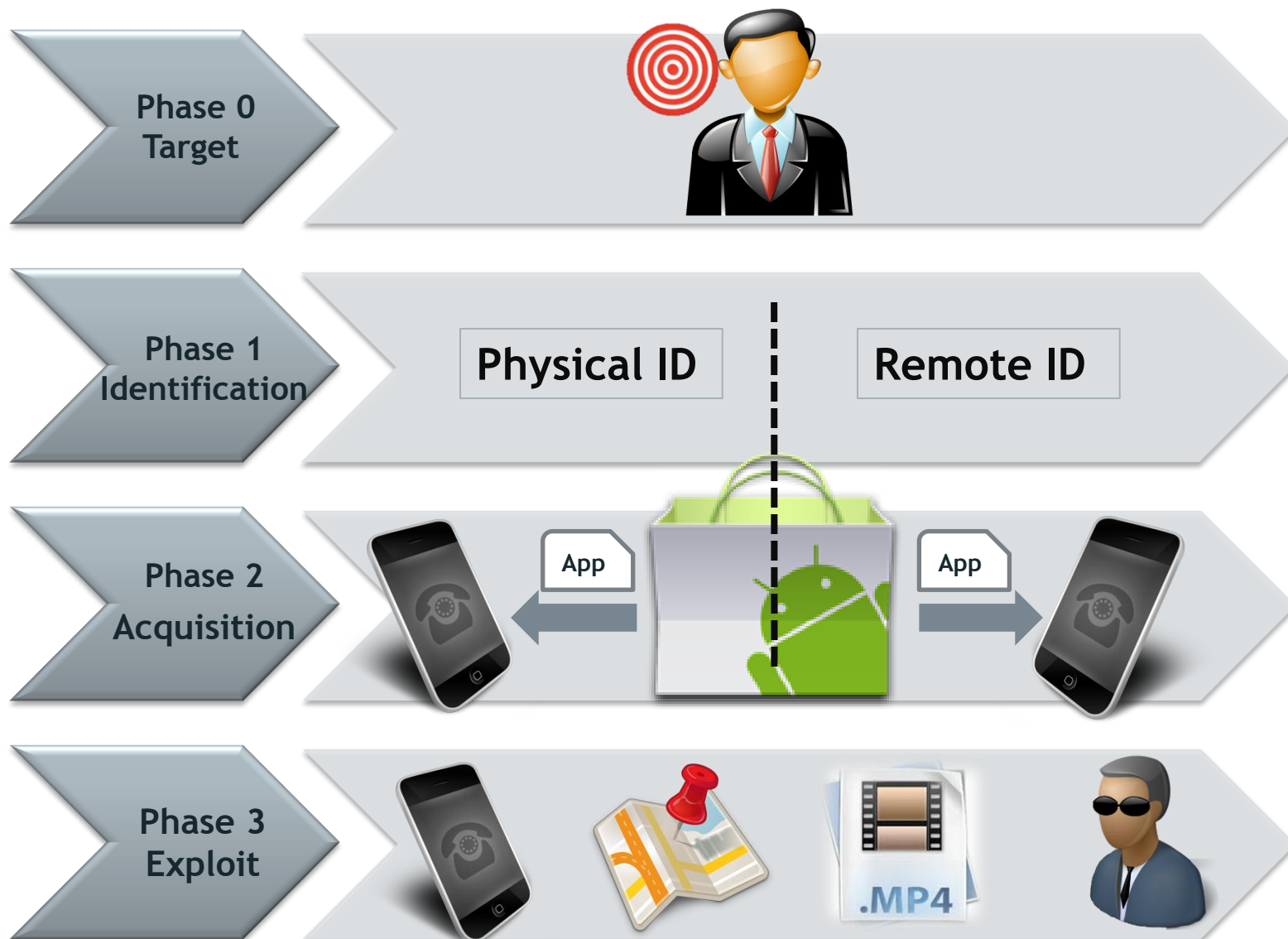
High Level Process Flow



High Level Process Flow



High Level Process Flow











Mobile Device Platforms



Android - Path of Least Resistance



Volume of devices and growth



Market fragmentation



Lag for software updates



Open platform



Vetting controls

Proof of Concept - Overview



Objective: Obtain a voice recording of the user using the device (not phone call)

Requires:



Knowledge of their mobile device platform



Physical or remote acquisition techniques



A mobile app that can trigger at a specific location, act as a recorder and post recorded files



An app that is in the market place (ideally)



An app that can be remote controlled (ideally)



Voice recorder - > Targeted Individual



Huawei X1 ★★★★★ (21) Read reviews

\$71¹⁰

Features Specifications

Find your nearest store

A Stylish Entertainer Phone with the Android 2.2 Operating System

3G dual band

- > Device Coverage
- > Find out more about The Optus Open Network™
- > Coverage street checker

Features

- > 3.2MP camera
- > Expandable memory
- > FM radio
- > Bluetooth



Photos



~600 LOC



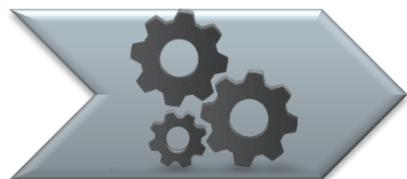
- Corporate Espionage
- Insider Trading
- Financial Gain
- Political Gain
- Competitive Advantage

~\$few hundred



Functions

- ~600 Lines of Code
- Polls a specific server for instructions (where to trigger, radius, duration)
- Triggers on GPS co-ordinates (or derived location from GSM Network, Wireless etc)
- Records for 30 seconds. Continuous looping for demo.




Permissions Required

- access your location (GPS)
- your personal information (contact info)
- network communications (make outbound connections)
- storage (store file)
- hardware controls (record audio)



Visibility

- None - will operate in the background and not alert the owner it is triggered (although PoC app presents logging information on the screen for demo purposes, and vibrates to indicate recording!)

A grey, 3D-style callout box with a white interior and a drop shadow, pointing to the right.

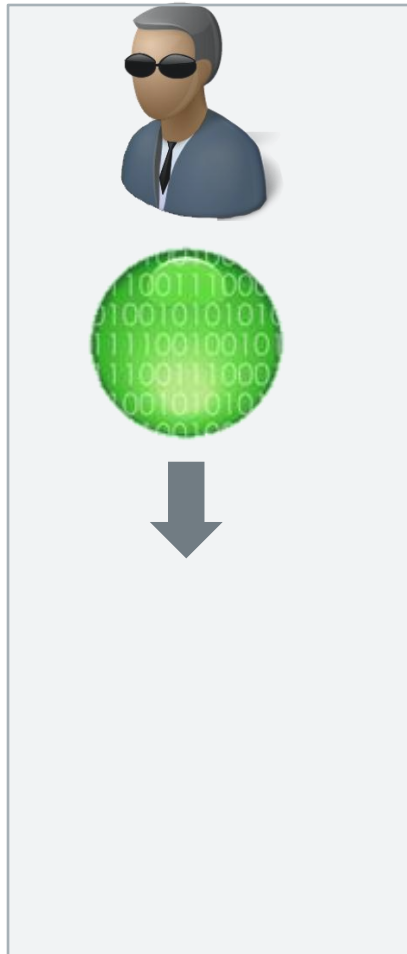
**Write App for Purpose
“Triggered Voice
Recorder”**



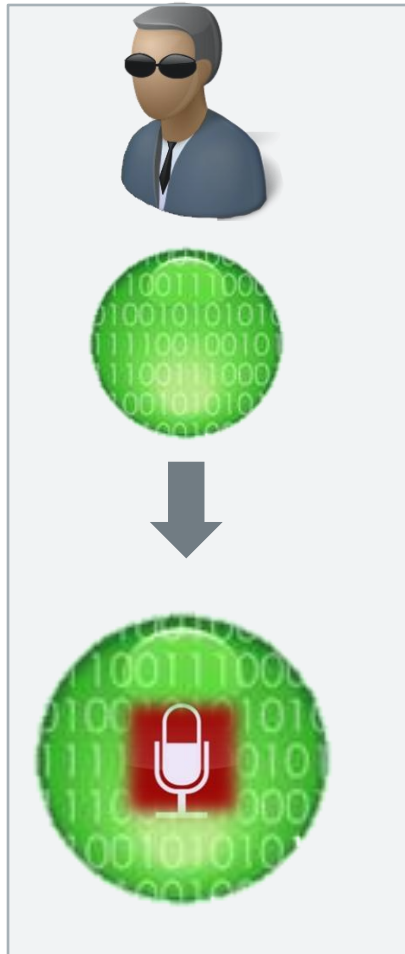
**Write App for Purpose
“Triggered Voice
Recorder”**



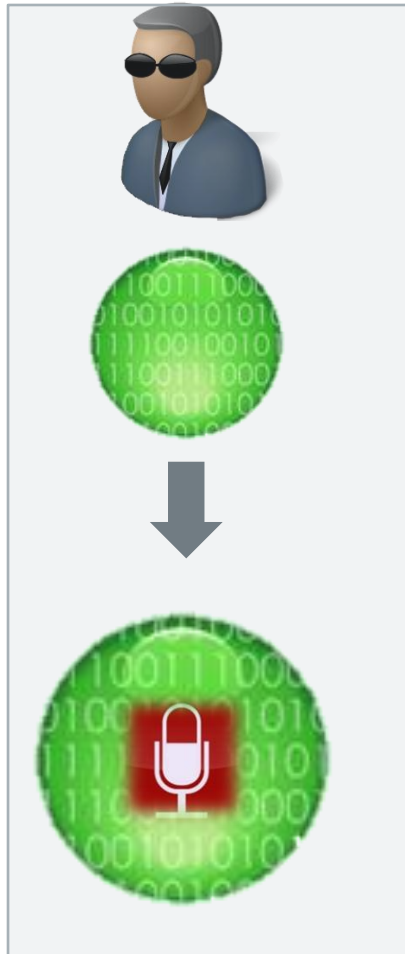
**Write App for Purpose
“Triggered Voice
Recorder”**



**Write App for Purpose
"Triggered Voice
Recorder"**

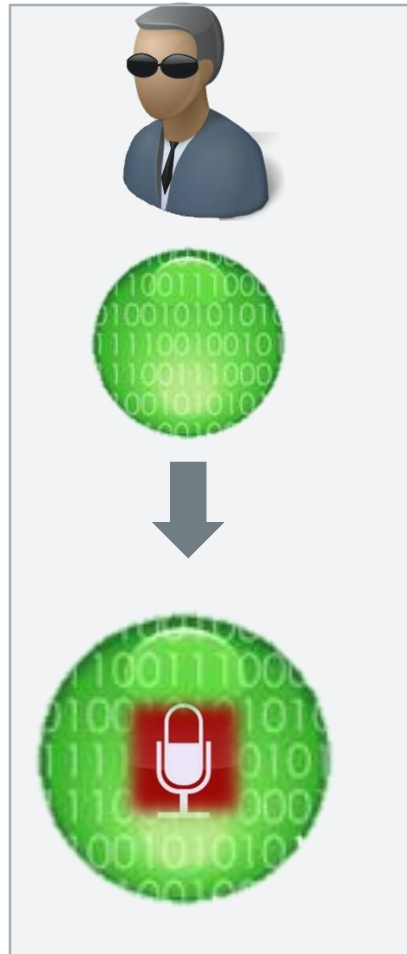


**Write App for Purpose
"Triggered Voice
Recorder"**

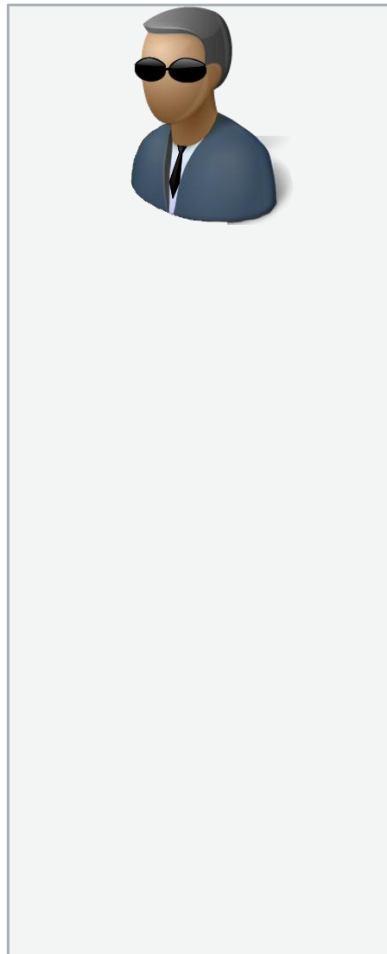


**Write App for Purpose
"Triggered Voice
Recorder"**

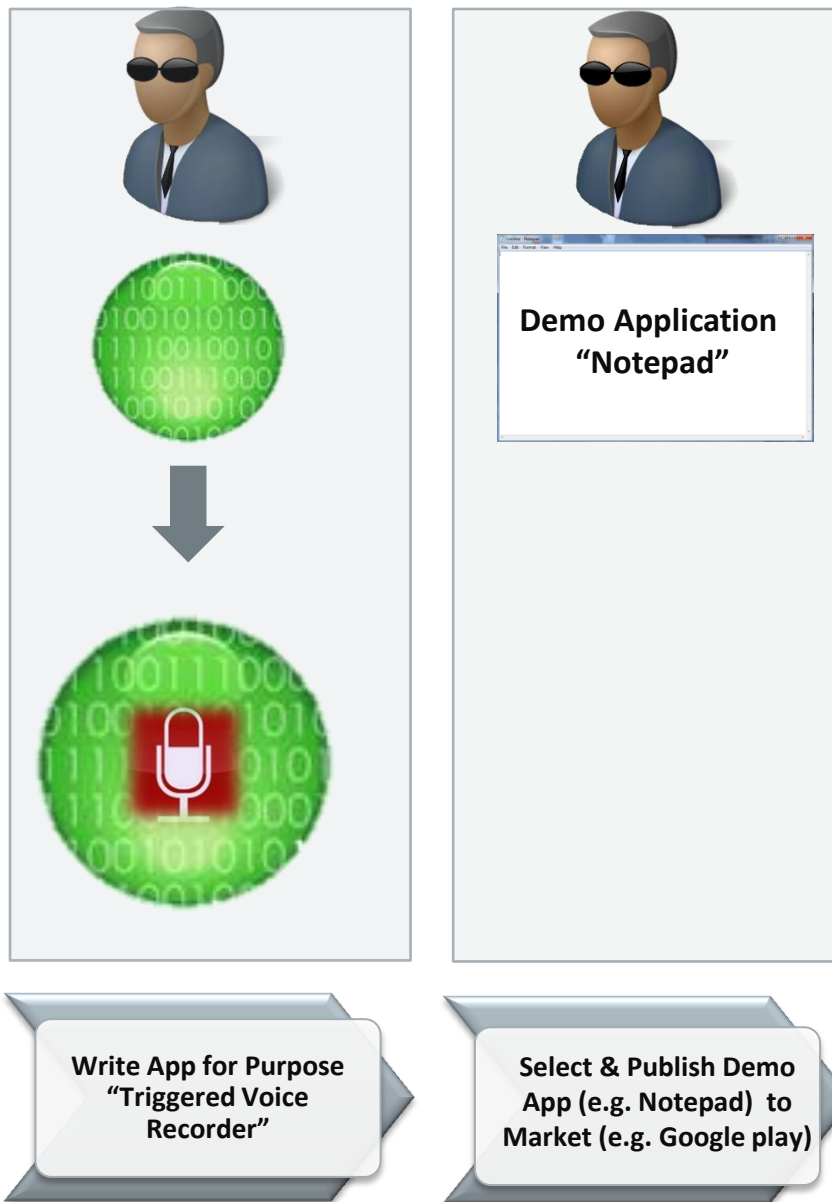
**Select & Publish Demo
App (e.g. Notepad) to
Market (e.g. Google play)**

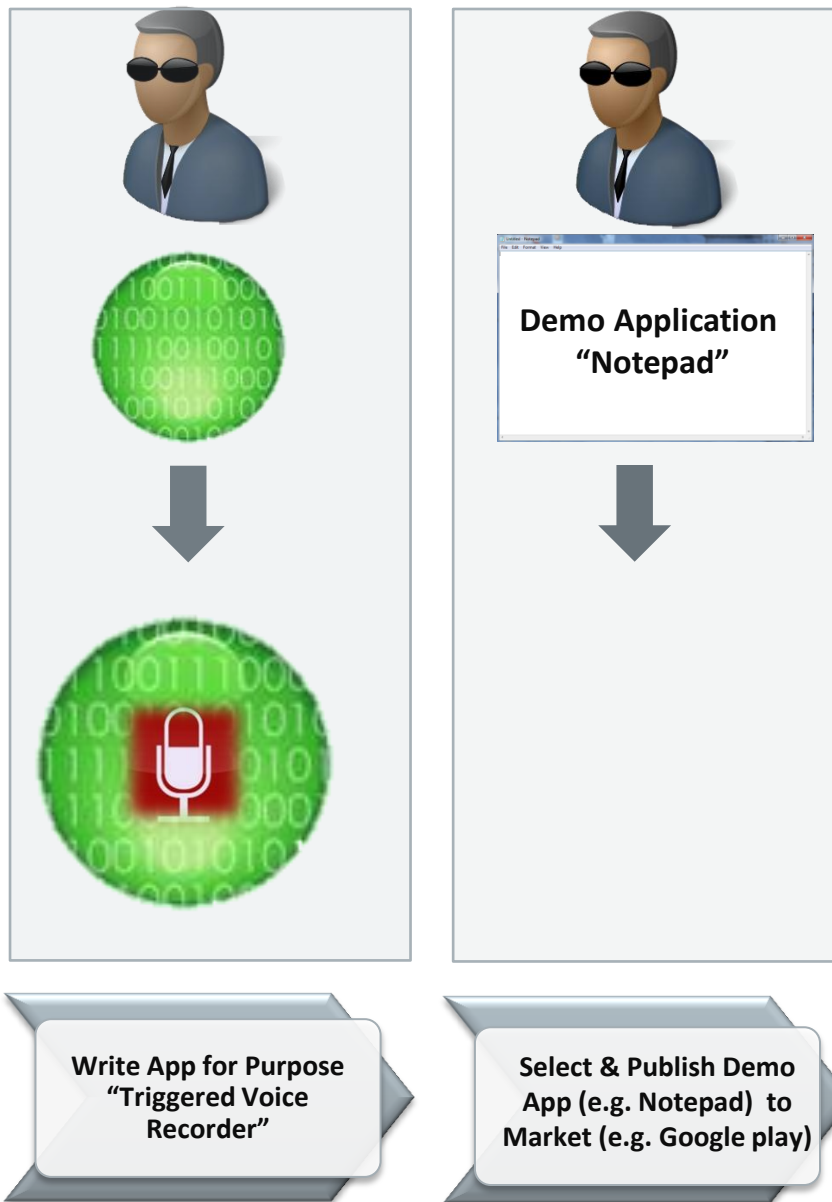


**Write App for Purpose
"Triggered Voice
Recorder"**

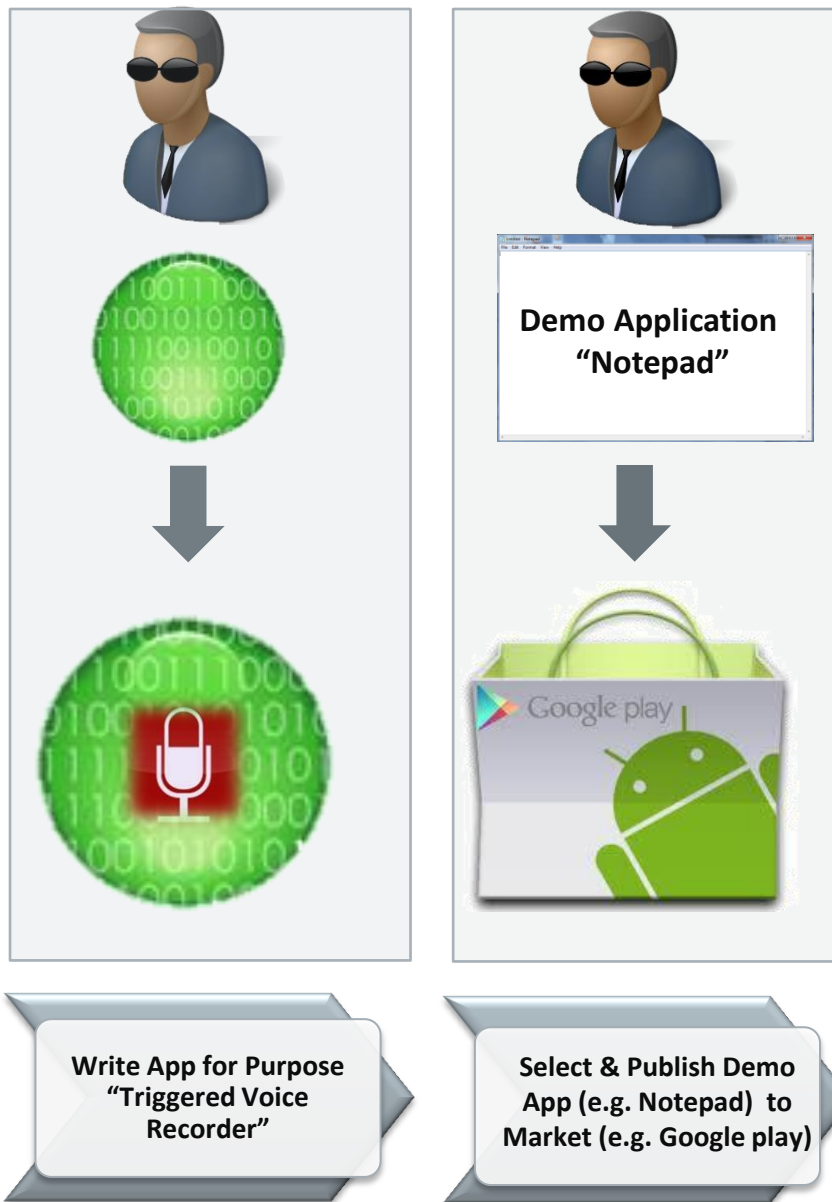


**Select & Publish Demo
App (e.g. Notepad) to
Market (e.g. Google play)**

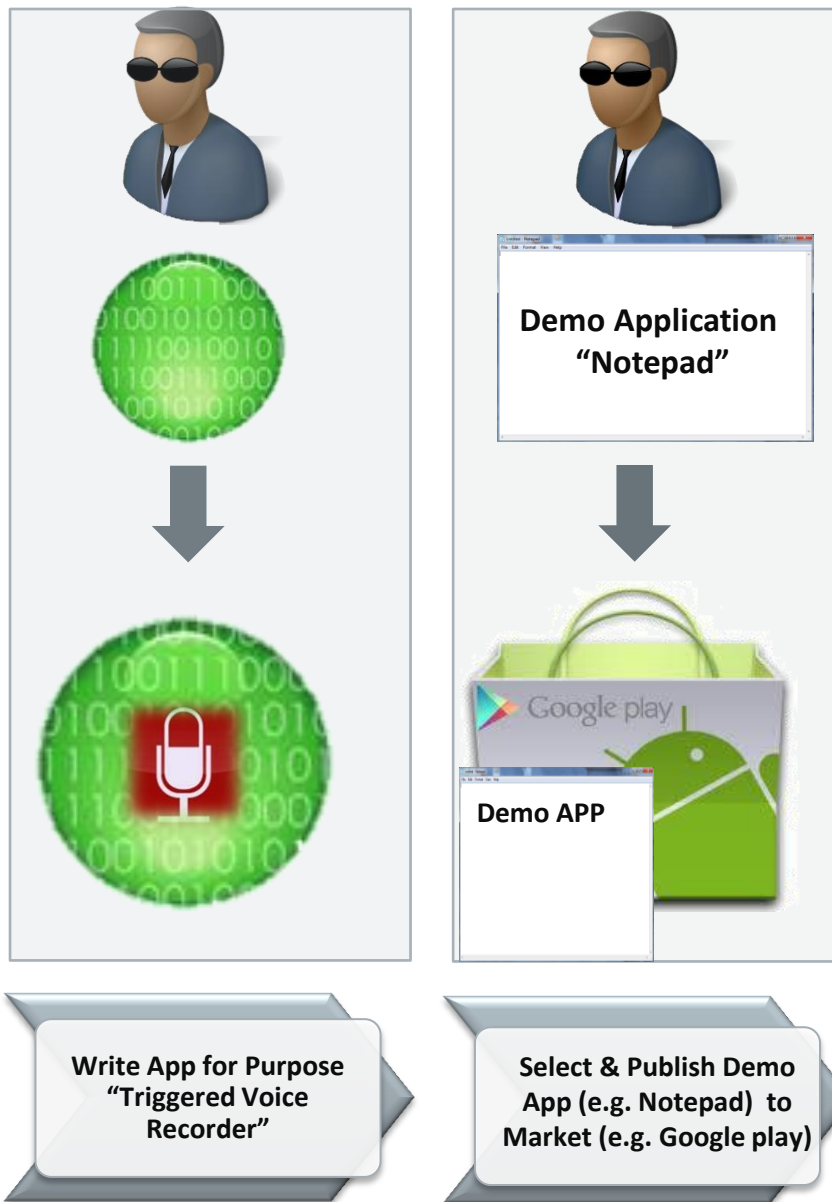


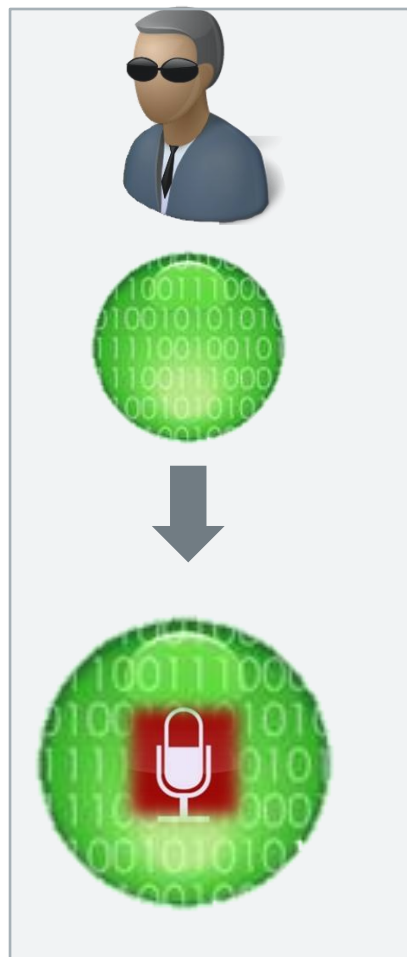


Anatomy of the Attack

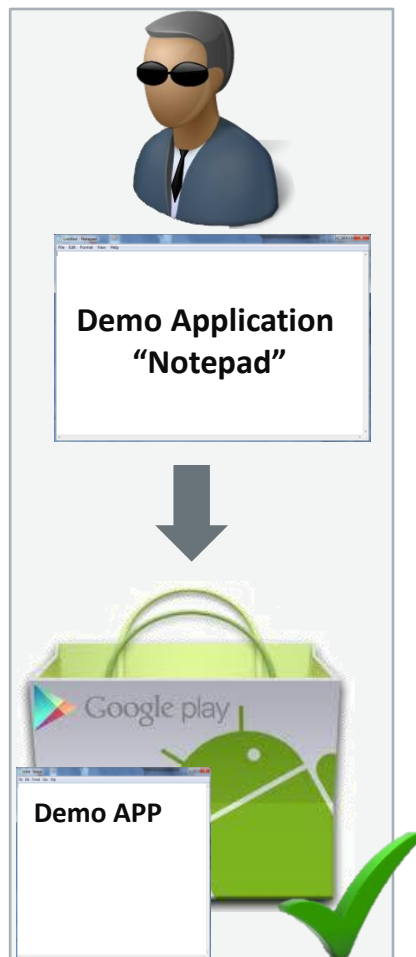


Anatomy of the Attack

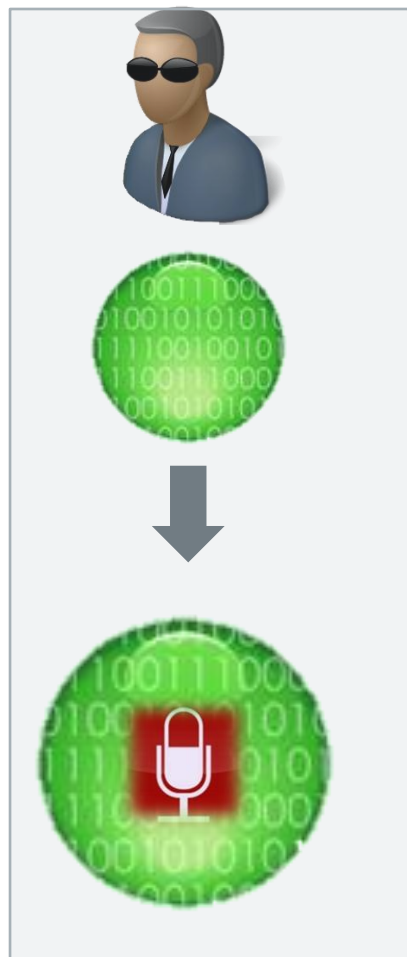




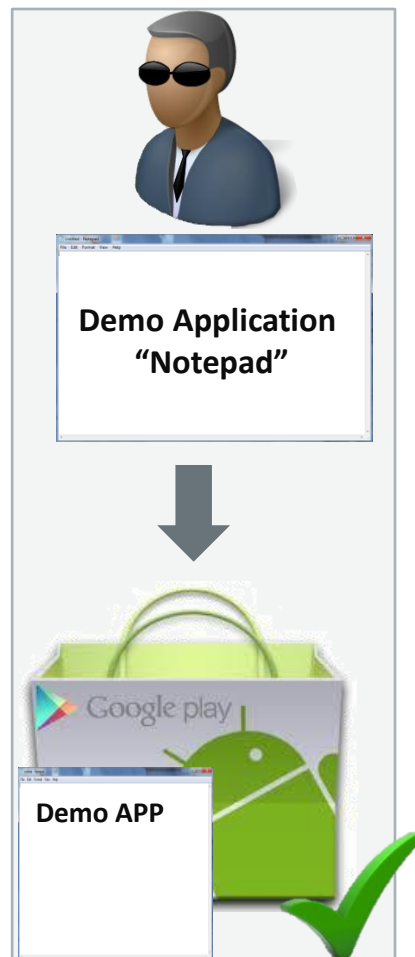
**Write App for Purpose
"Triggered Voice
Recorder"**



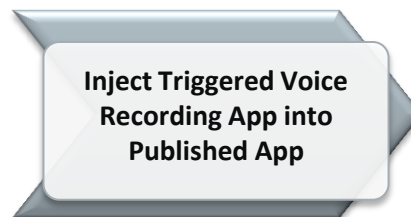
**Select & Publish Demo
App (e.g. Notepad) to
Market (e.g. Google play)**



**Write App for Purpose
"Triggered Voice
Recorder"**

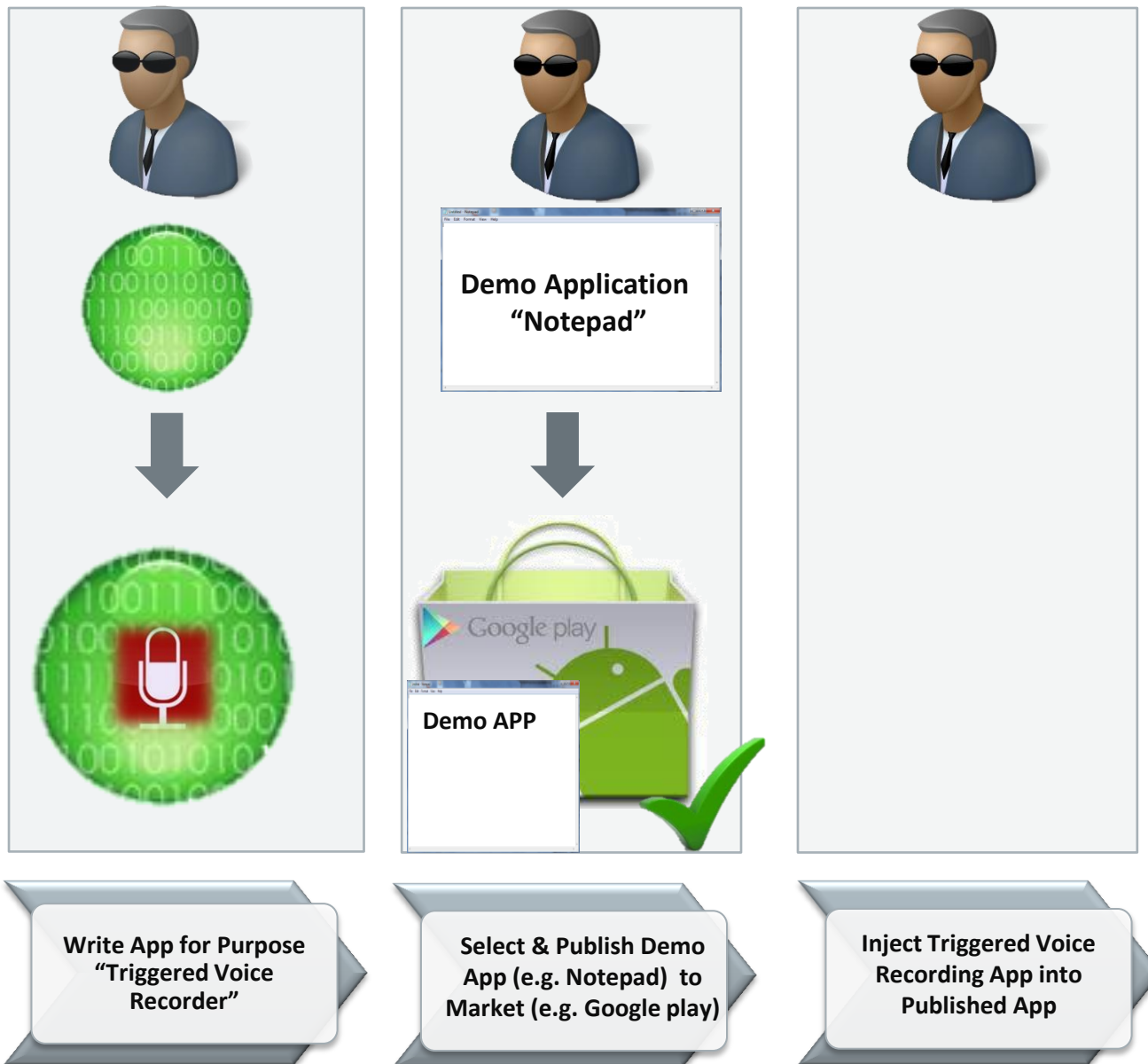


**Select & Publish Demo
App (e.g. Notepad) to
Market (e.g. Google play)**

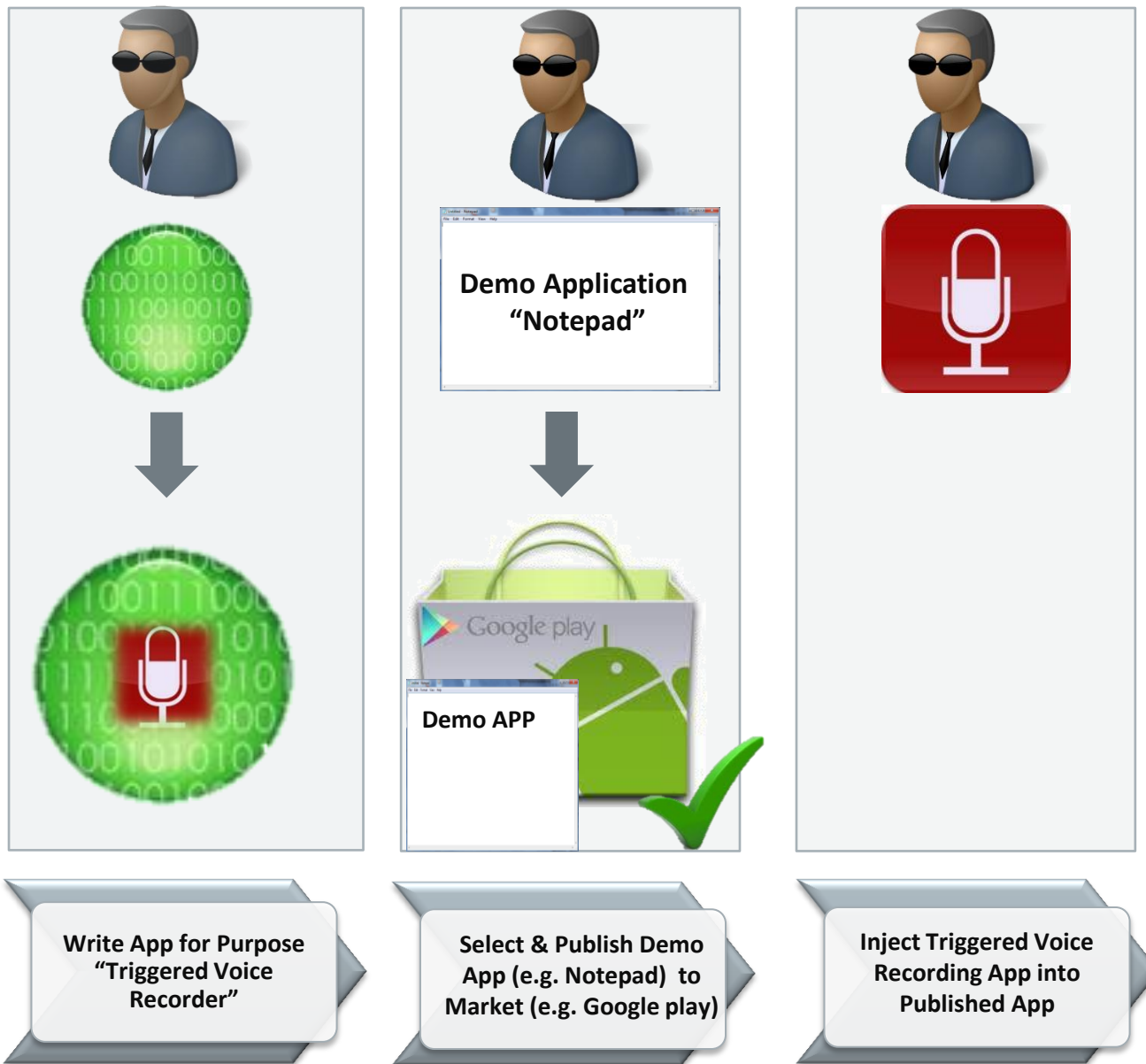


**Inject Triggered Voice
Recording App into
Published App**

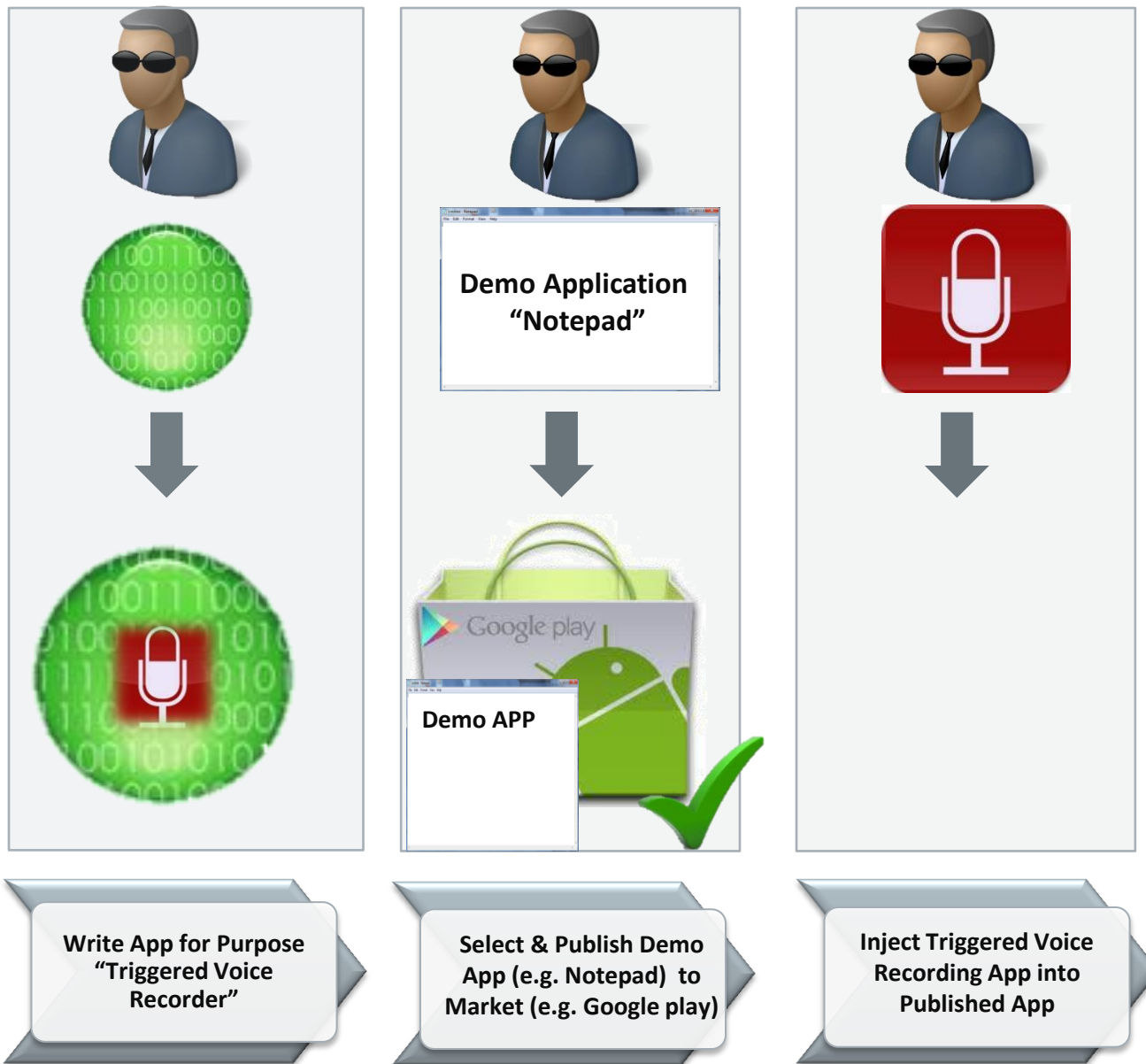
Anatomy of the Attack



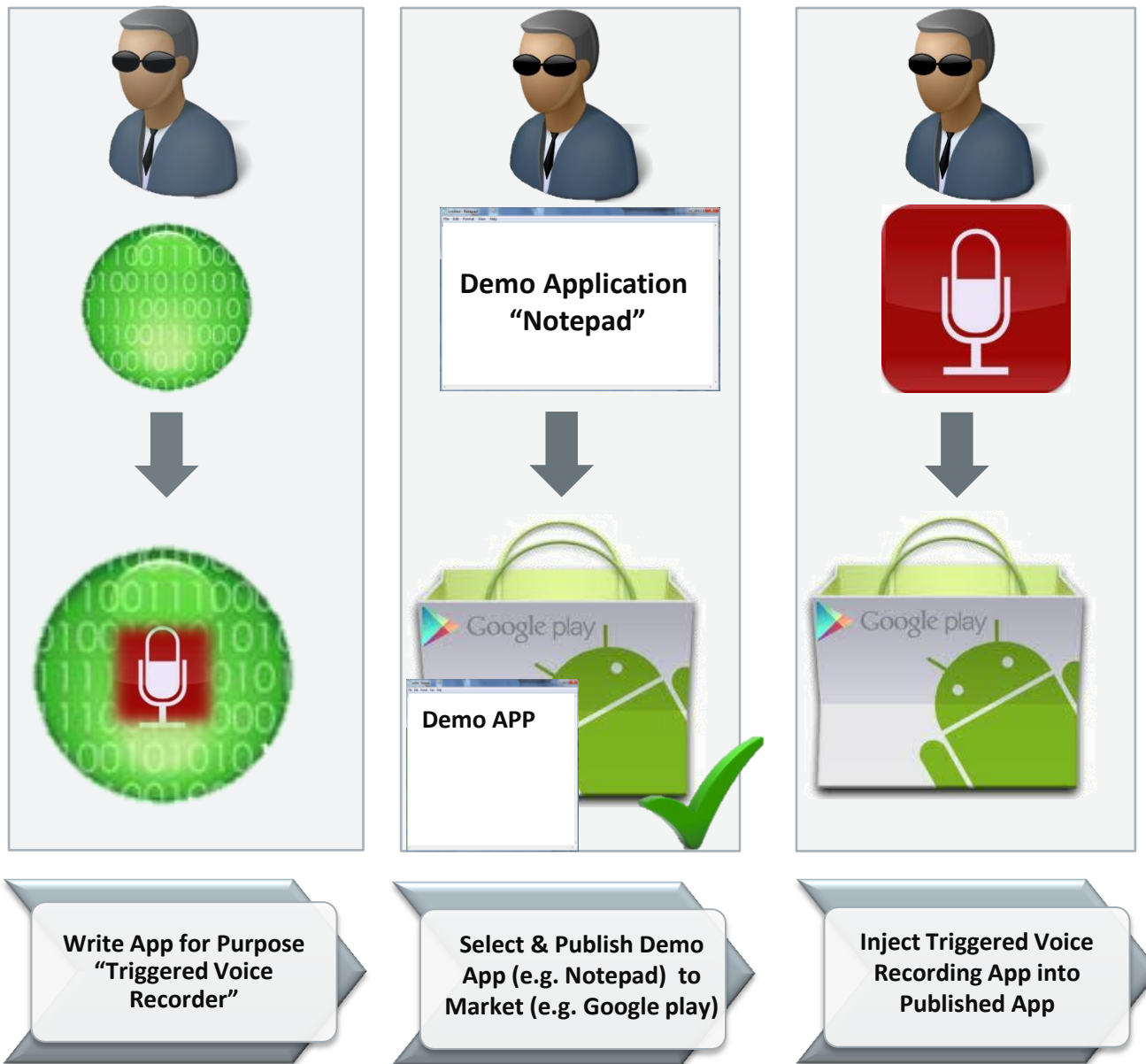
Anatomy of the Attack



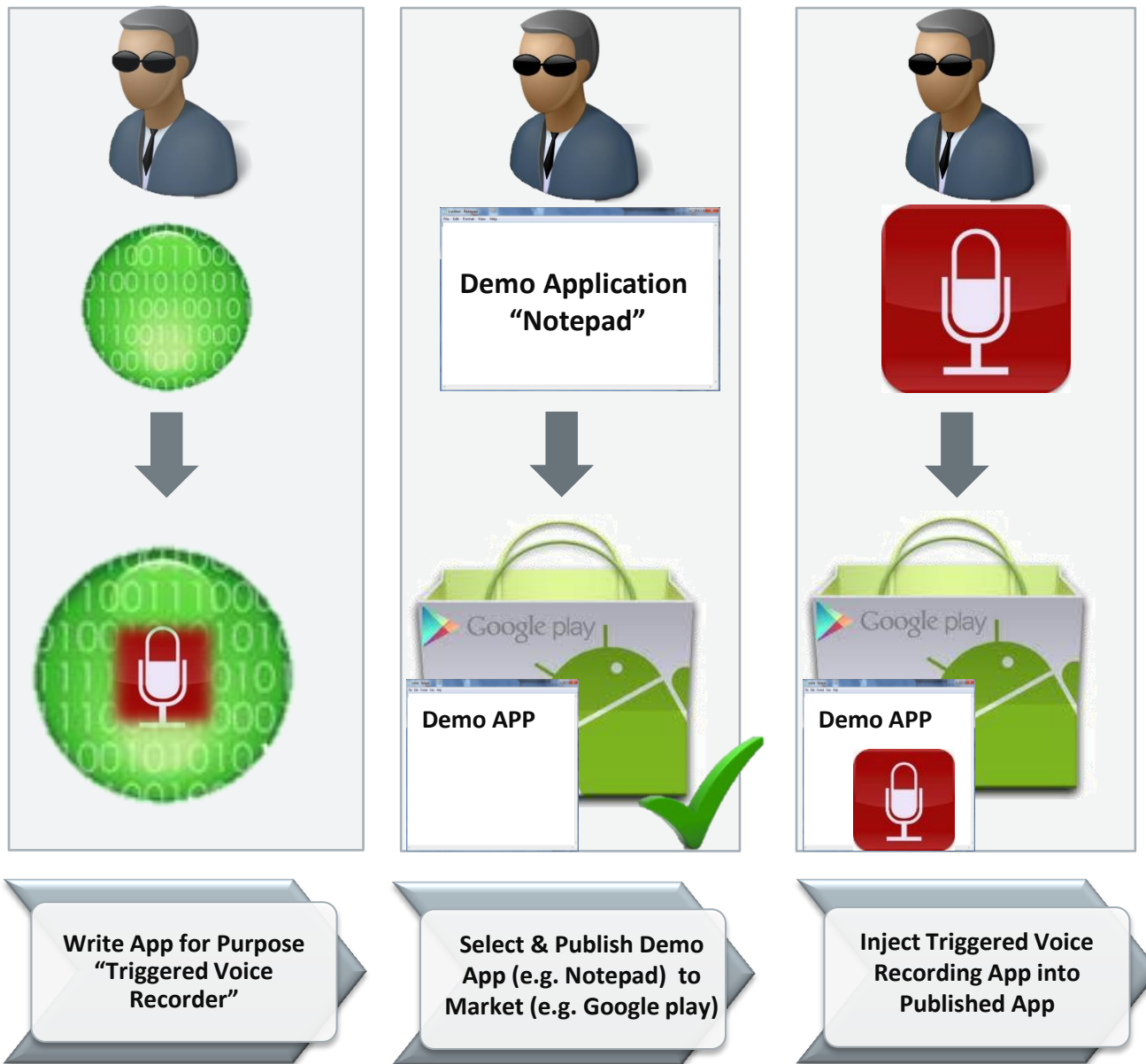
Anatomy of the Attack



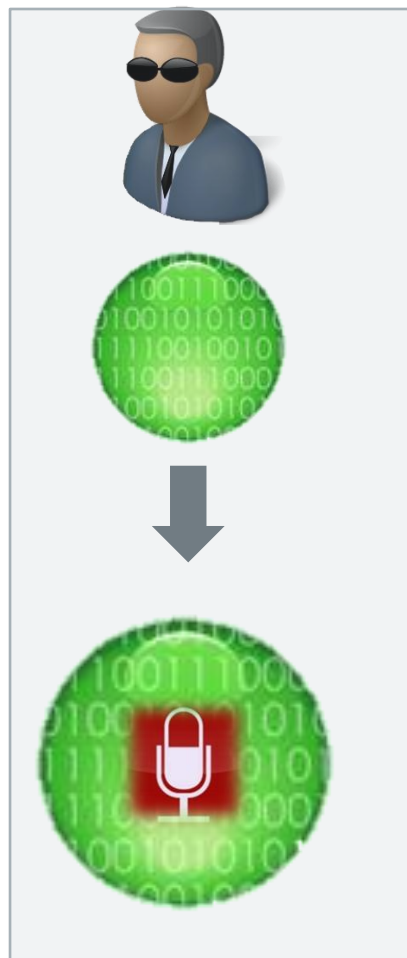
Anatomy of the Attack



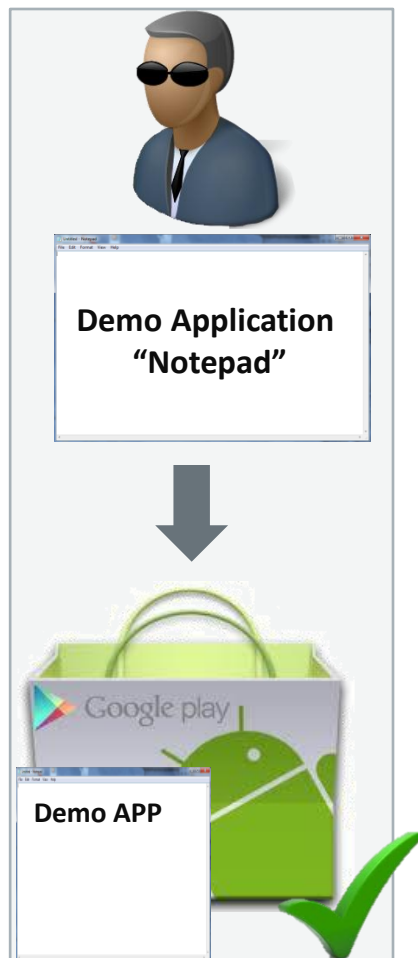
Anatomy of the Attack



Anatomy of the Attack



**Write App for Purpose
"Triggered Voice
Recorder"**



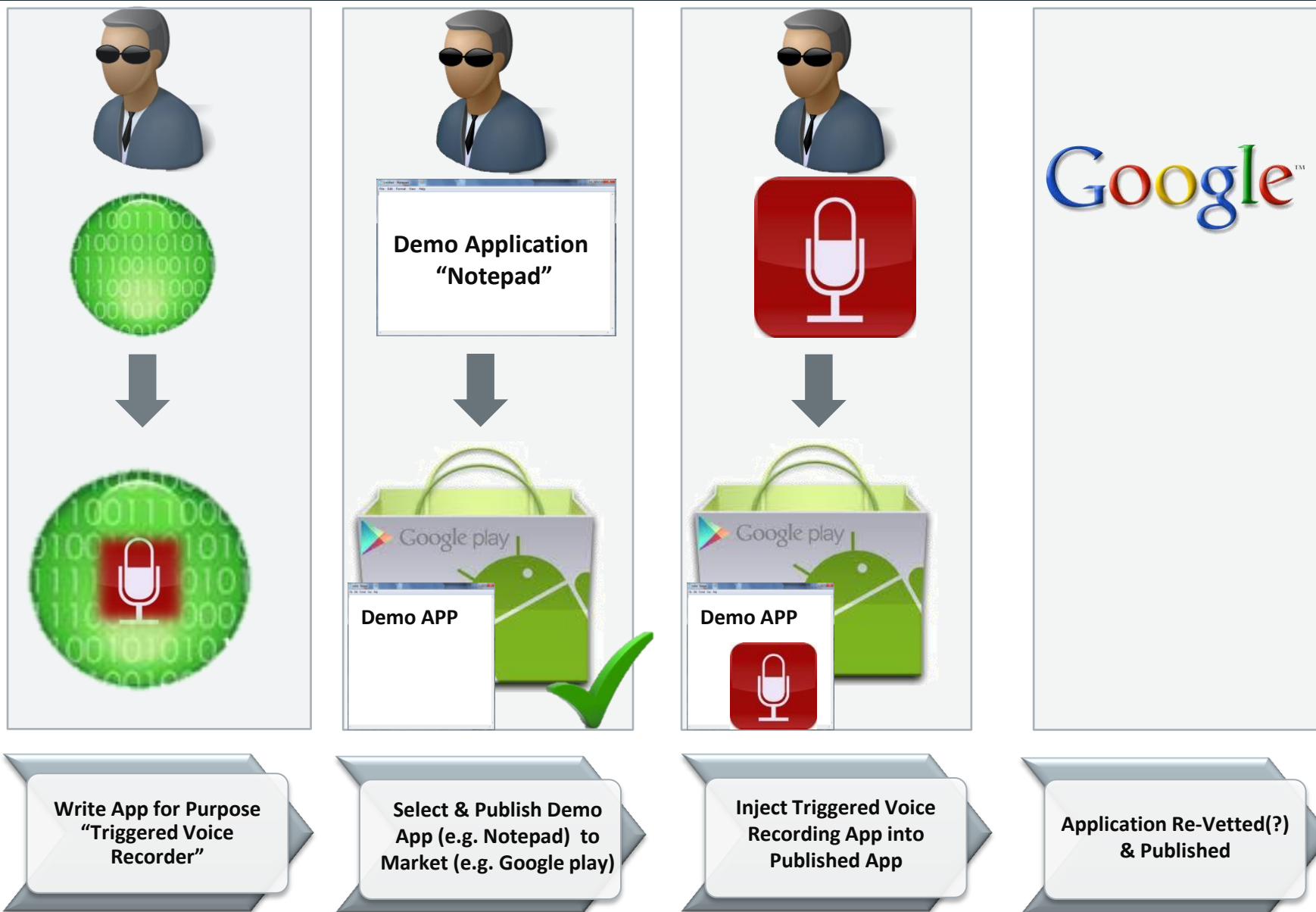
**Select & Publish Demo
App (e.g. Notepad) to
Market (e.g. Google play)**



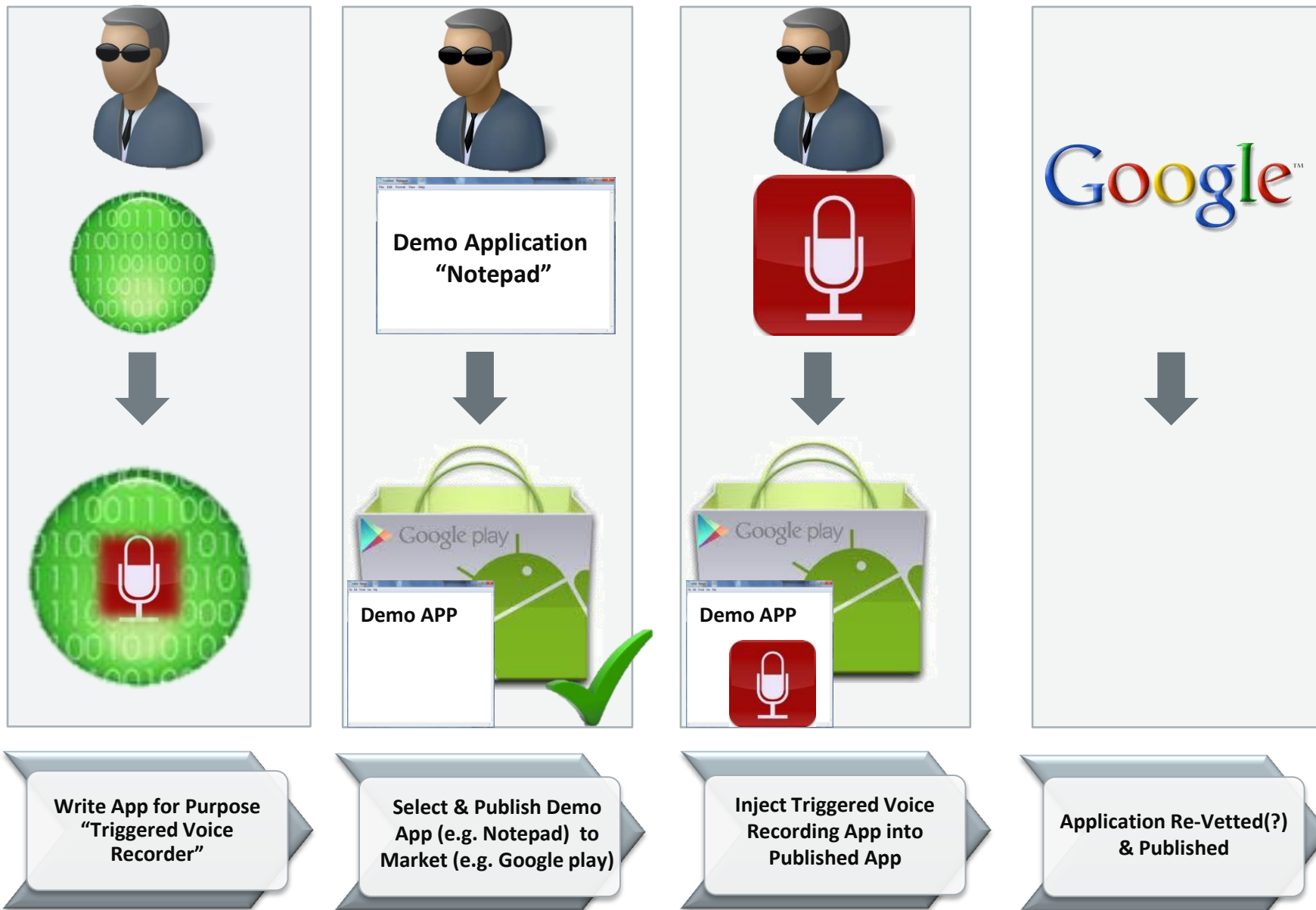
**Inject Triggered Voice
Recording App into
Published App**

**Application Re-Vetted(?)
& Published**

Anatomy of the Attack



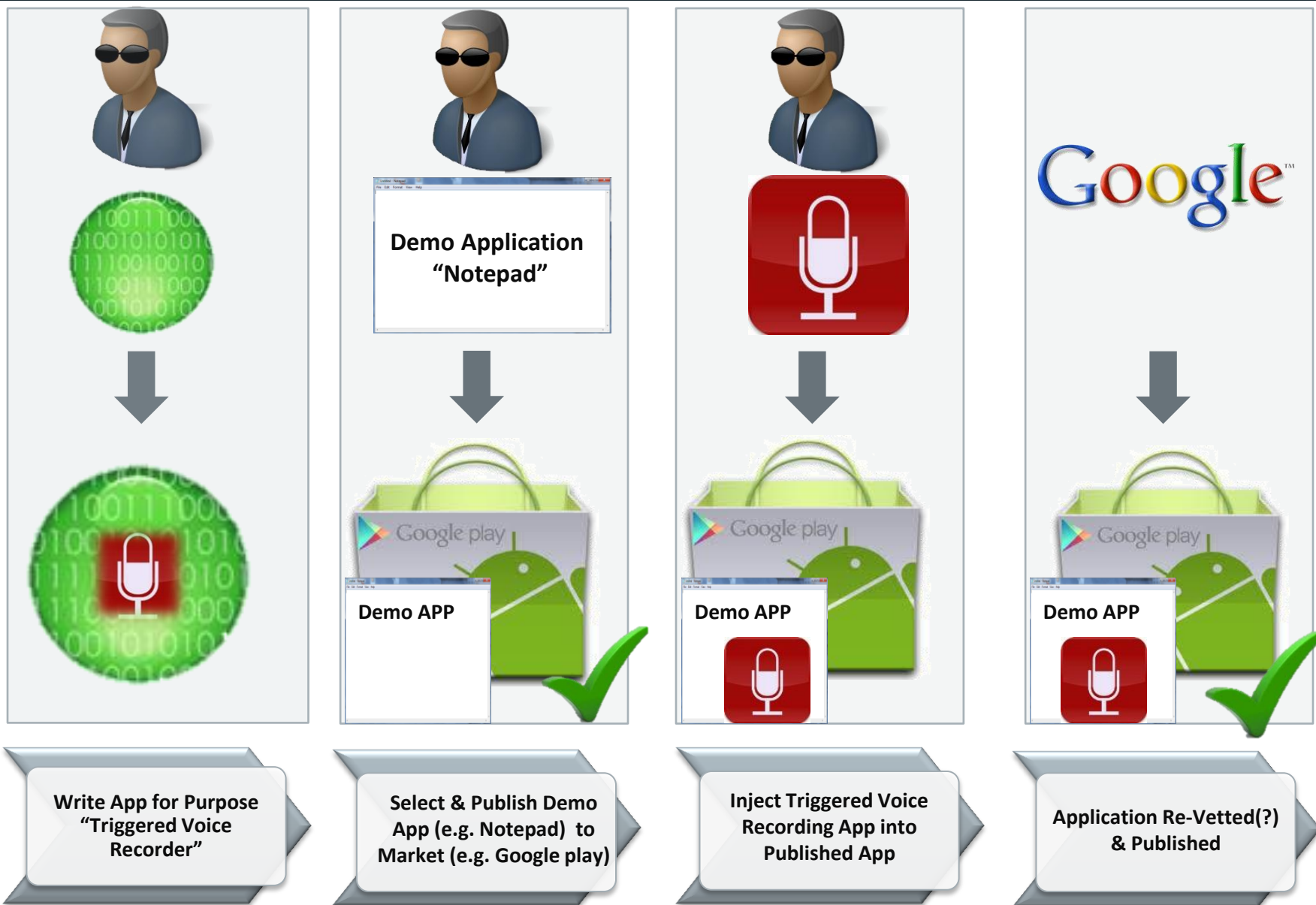
Anatomy of the Attack



Anatomy of the Attack



Anatomy of the Attack



A light gray button with a dark gray border and a dark gray shadow, shaped like a right-pointing arrow. The text "Seek Target" is centered inside the button.

Seek Target



Seek Target



Seek Target



Seek Target

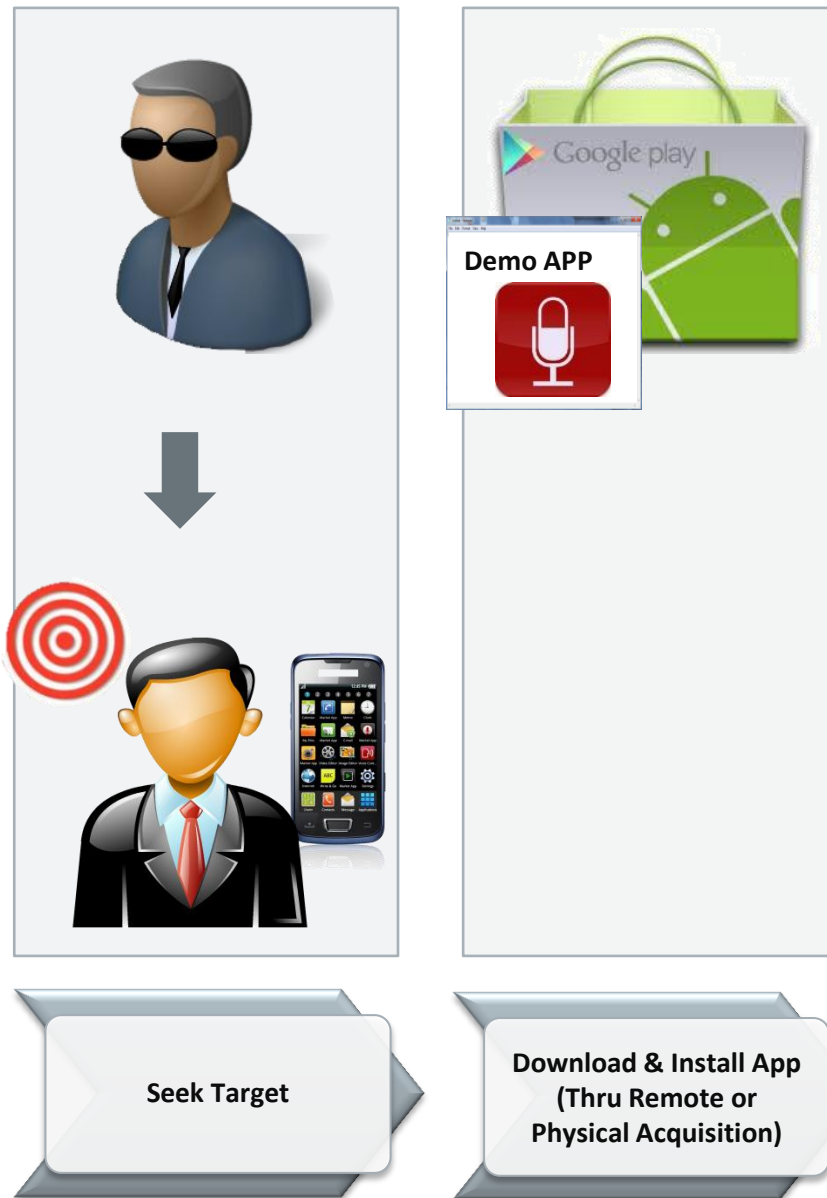


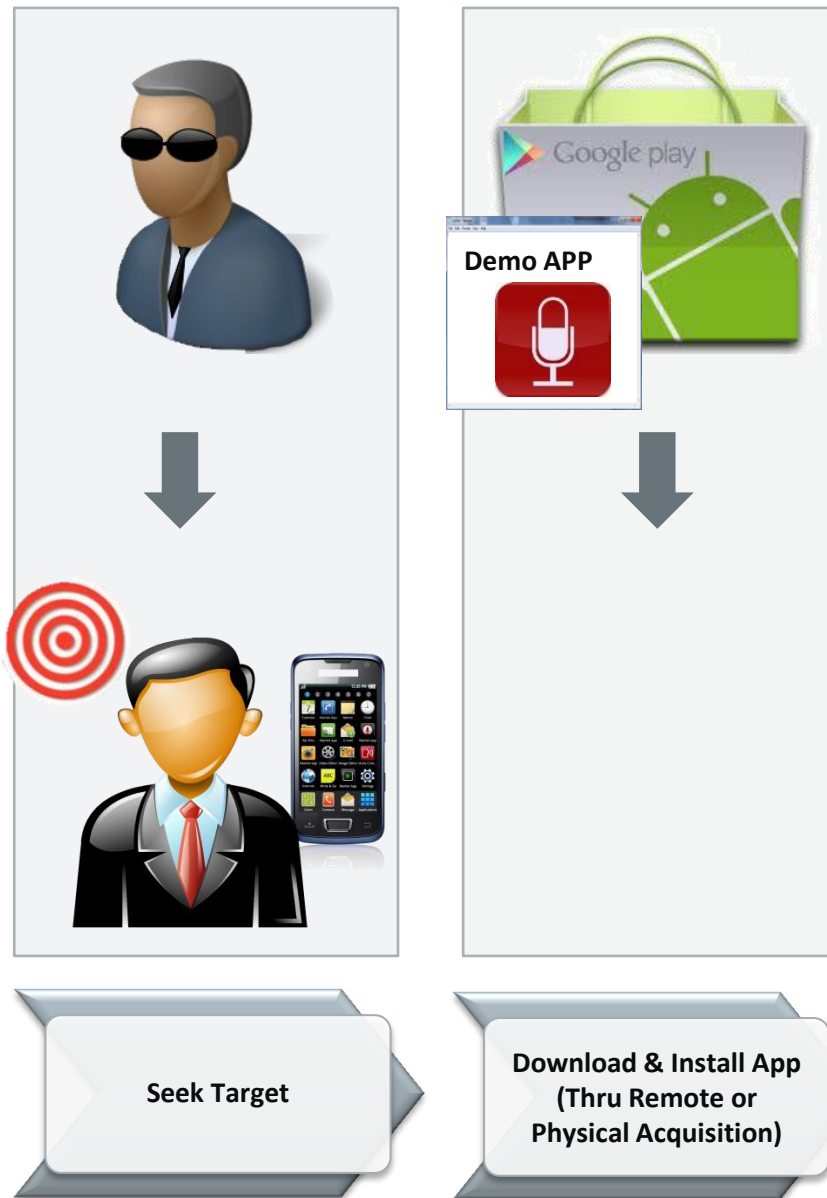
Seek Target



Seek Target

Download & Install App
(Thru Remote or
Physical Acquisition)

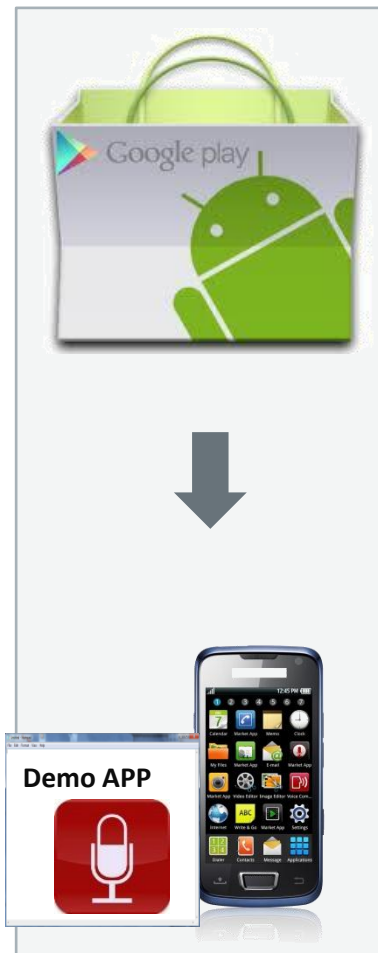








Seek Target

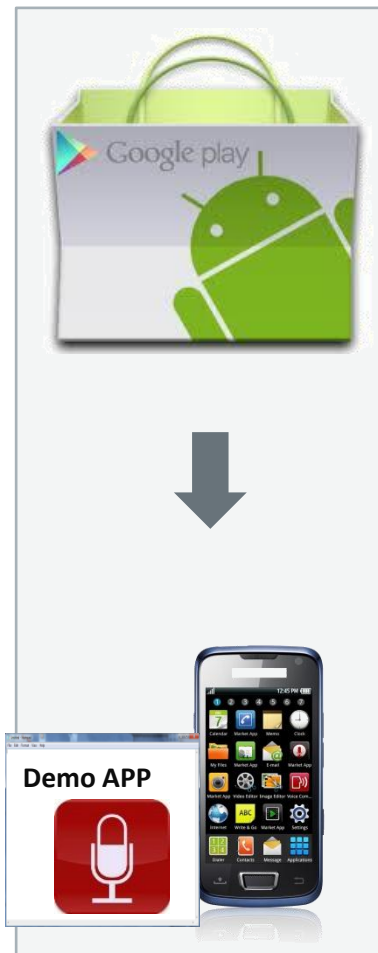


Download & Install App
(Thru Remote or
Physical Acquisition)

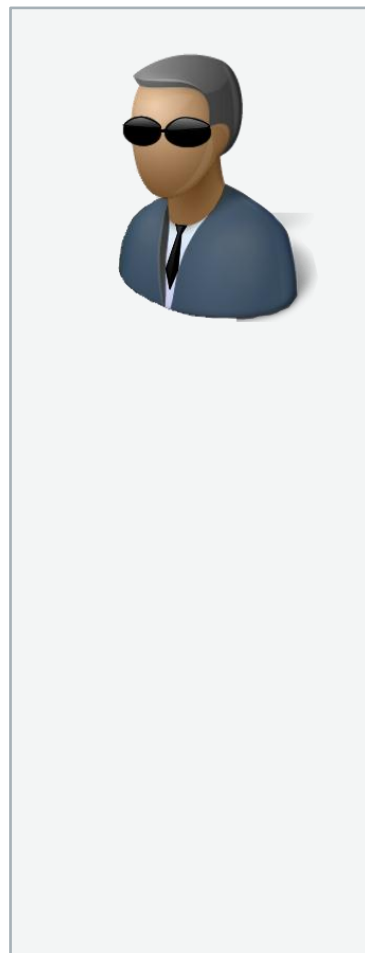
Set the GPS Co-ordinates
for Desired Recording
Location on server



Seek Target



Download & Install App
(Thru Remote or
Physical Acquisition)



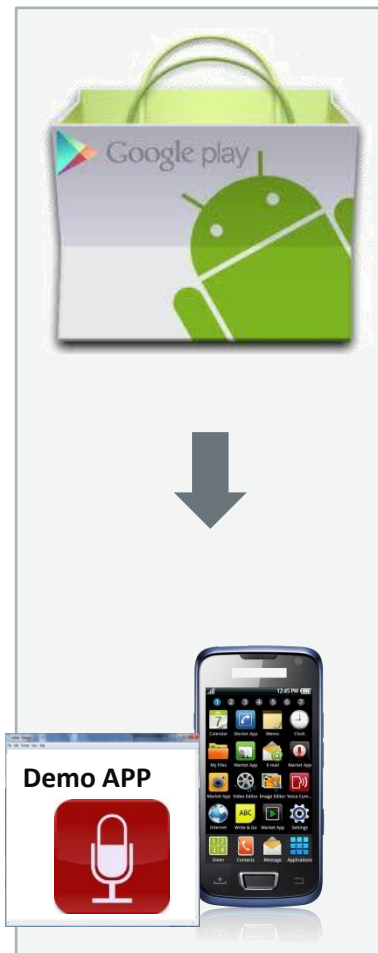
Set the GPS Co-ordinates
for Desired Recording
Location on server



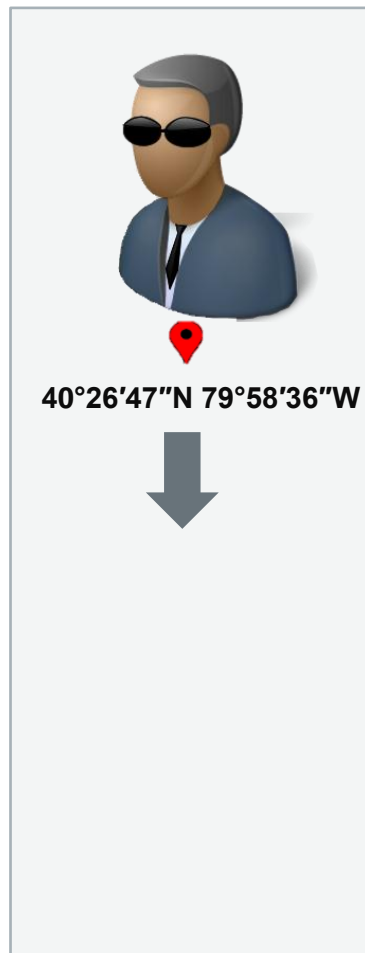
Anatomy of the Attack



Seek Target



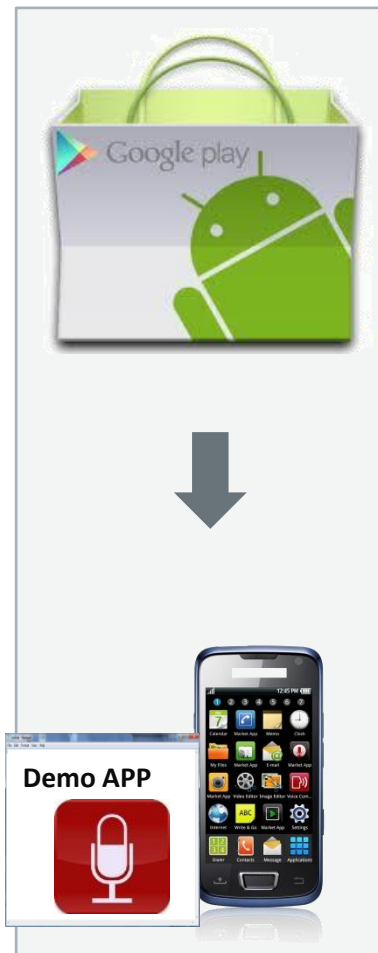
Download & Install App
(Thru Remote or
Physical Acquisition)



Set the GPS Co-ordinates
for Desired Recording
Location on server



Seek Target



Download & Install App
(Thru Remote or
Physical Acquisition)

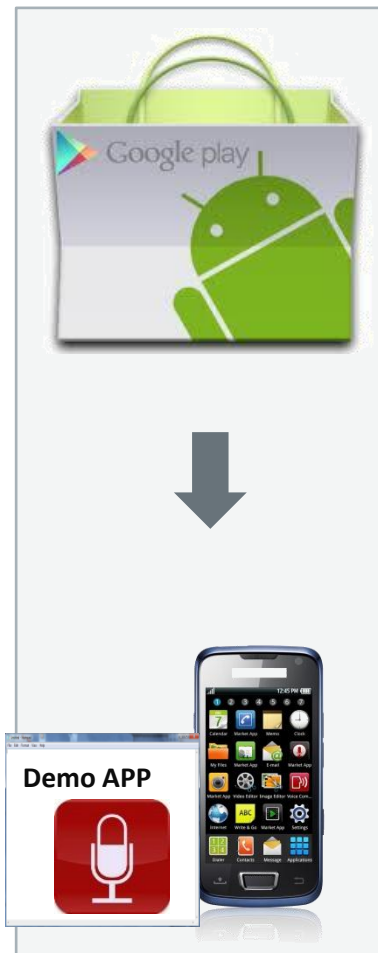


Set the GPS Co-ordinates
for Desired Recording
Location on server

Anatomy of the Attack



Seek Target



Download & Install App
(Thru Remote or
Physical Acquisition)



Set the GPS Co-ordinates
for Desired Recording
Location on server

Anatomy of the Attack





Anatomy of the Attack



Anatomy of the Attack




Anatomy of the Attack



Anatomy of the Attack

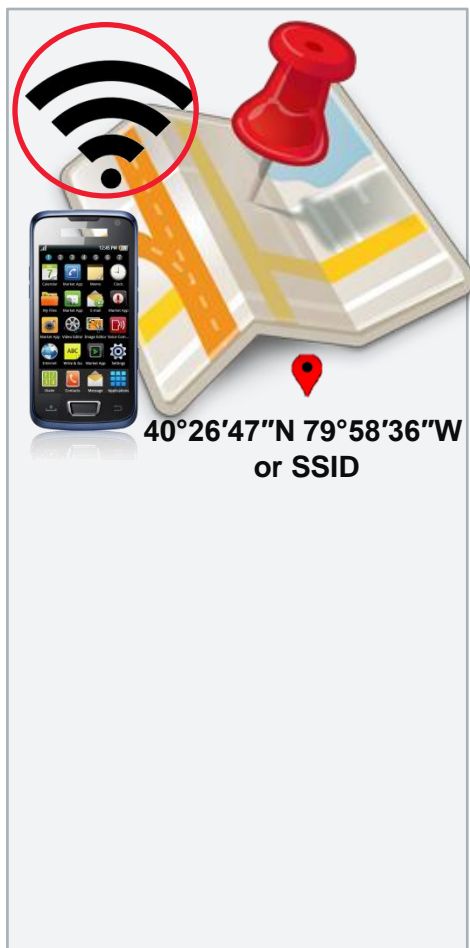


A grey, 3D-style callout box with a white center containing the text "Recording Device Activated at Prescribed Location".

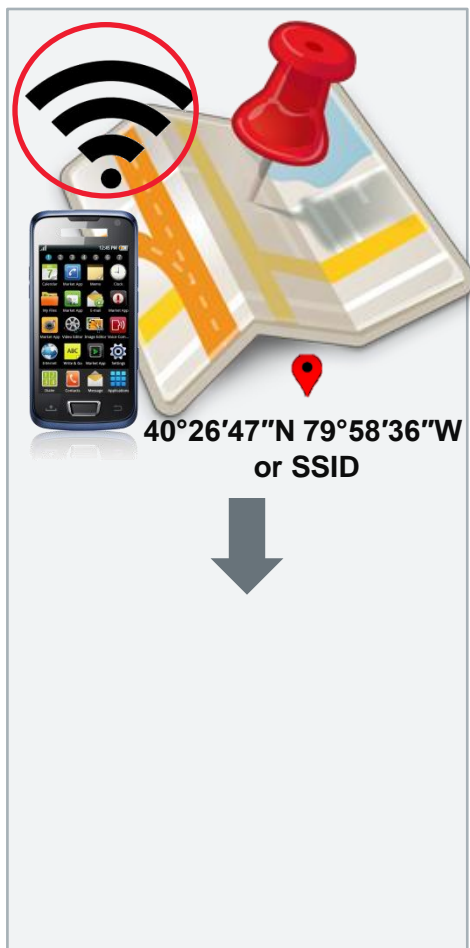
**Recording Device
Activated at Prescribed
Location**



**Recording Device
Activated at Prescribed
Location**



**Recording Device
Activated at Prescribed
Location**



**Recording Device
Activated at Prescribed
Location**



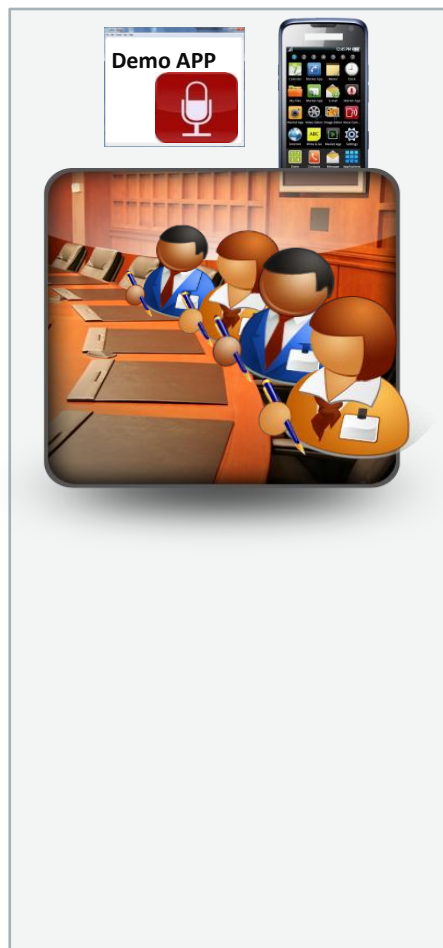


**Recording Device
Activated at Prescribed
Location**

Recording



**Recording Device
Activated at Prescribed
Location**

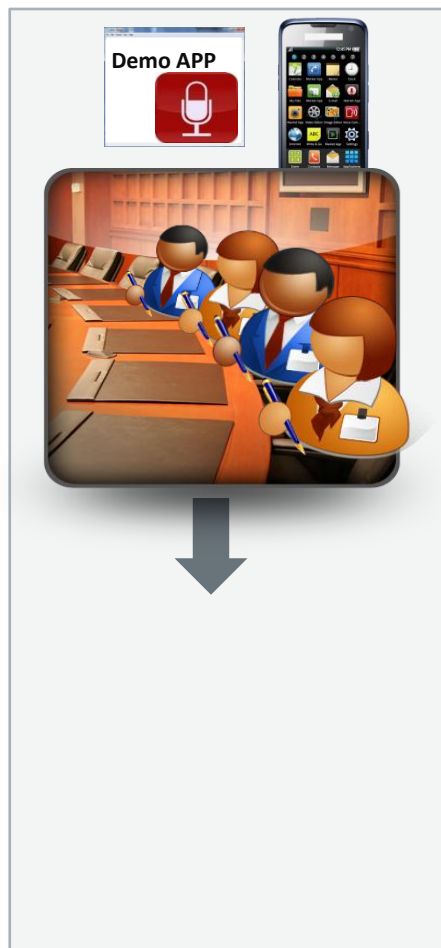


Recording

Anatomy of the Attack



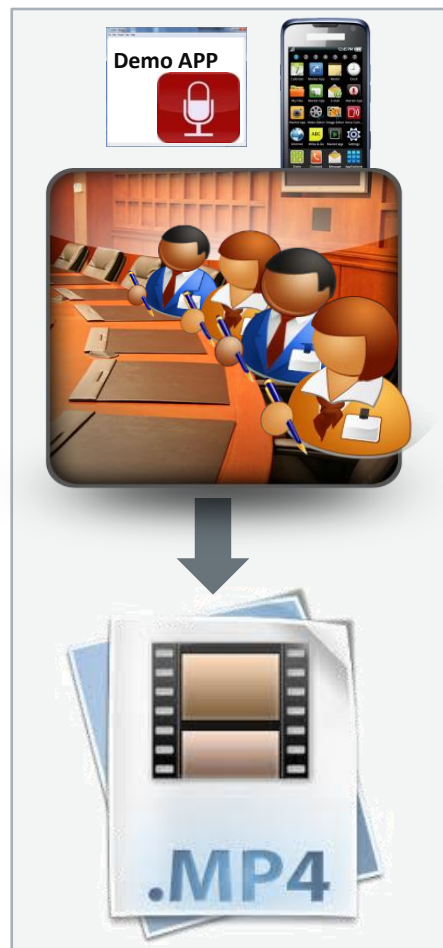
**Recording Device
Activated at Prescribed
Location**



Recording



**Recording Device
Activated at Prescribed
Location**



Recording



**Recording Device
Activated at Prescribed
Location**



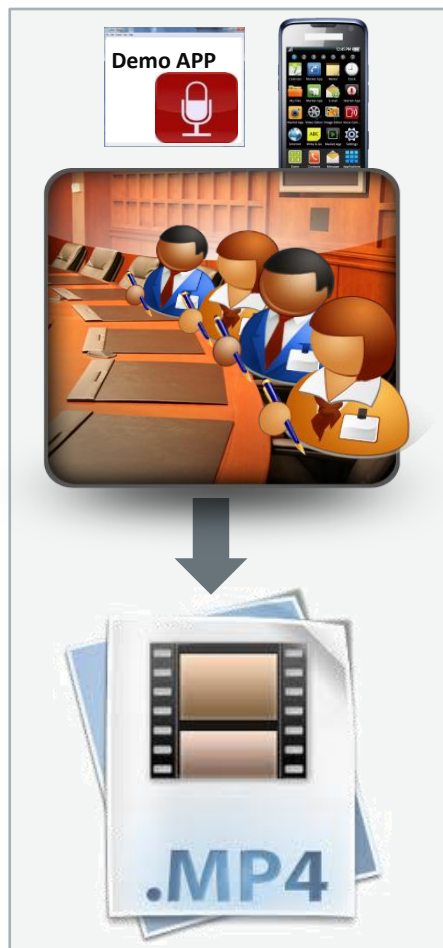
Recording

**Recording File sent to
Attacker's Server**

Anatomy of the Attack



**Recording Device
Activated at Prescribed
Location**



Recording

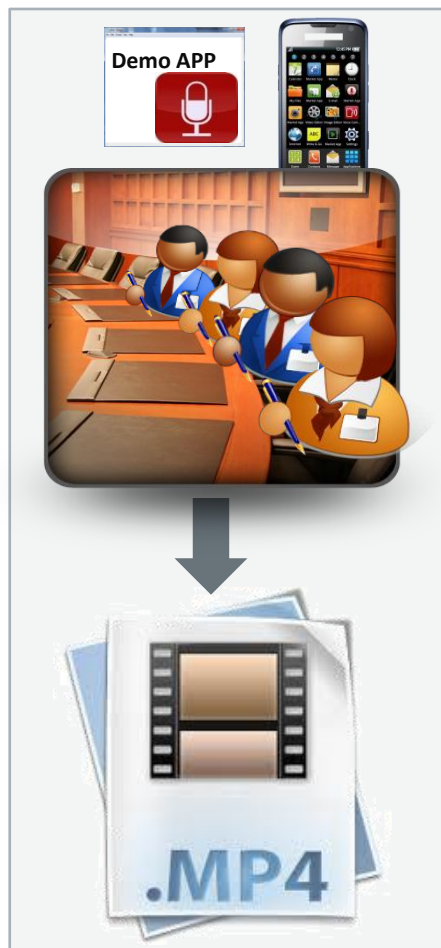


**Recording File sent to
Attacker's Server**

Anatomy of the Attack



**Recording Device
Activated at Prescribed
Location**



Recording

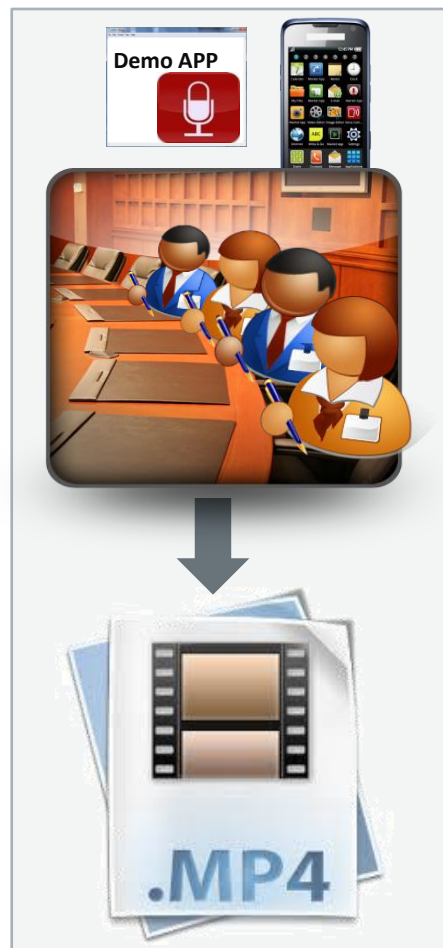


**Recording File sent to
Attacker's Server**

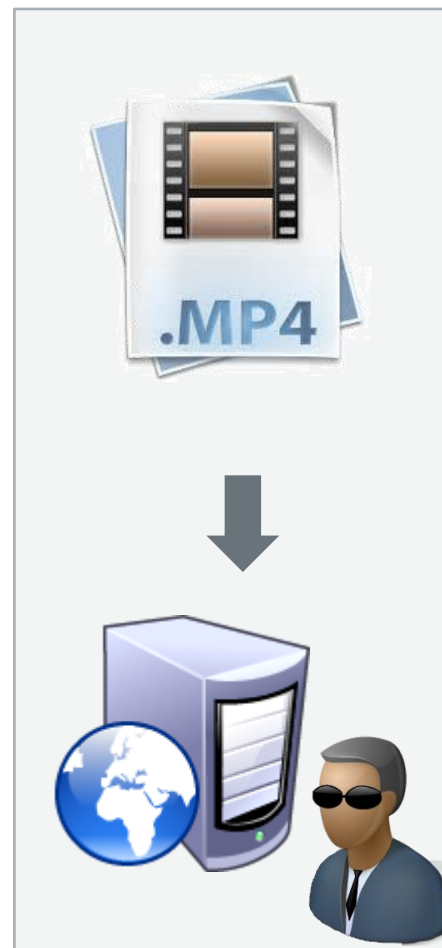
Anatomy of the Attack



**Recording Device
Activated at Prescribed
Location**



Recording



**Recording File sent to
Attacker's Server**



```

Nexus S
aLogcat

V/MW.CONFIG( 1061): Entering downloadAndParseConfig()
V/MW.CONFIG( 1061): Starting HTTP request for: http://
/ [REDACTED] 3.186/commands.txt
V/MW.CONFIG( 1061): HTTP request executed
V/MW.CONFIG( 1061): Command:GPS Length:4
V/MW.CONFIG( 1061): GPS Command:
GPS|-33.868592|151.206379|100
V/MW.CONFIG( 1061): Latitude: -33.868592;-33.868592
V/MW.CONFIG( 1061): Longitude: 151.206379;151.206379
V/MW.CONFIG( 1061): Exiting downloadAndParseConfig()
W/MW.MAIN ( 1061): Position: Lat: -33.8684631 Lon:
151.2063855
W/MW.MAIN ( 1061): Distance: 14.310233
W/MW.MAIN ( 1061): Starting recording...
V/MW.RECORDER( 1061): Entering startRecording()
V/MW.RECORDER( 1061): Exiting startRecording()
W/MW.MAIN ( 1061): Stopped recording, file is: /mnt/
sdcard/recordedAudio1336672818219.mp4
V/MW.RECORDER( 1061): Entering stopRecording()
V/MW.RECORDER( 1061): Really stop recording...
V/MW.RECORDER( 1061): Exiting stopRecording()
W/MW.MAIN ( 1061): OK, beginning file upload...
V/MW.UPLOADER( 1061): starting doUpload
E/MW.UPLOADER( 1061): Server Response: HTTP/1.1 200
OK
V/MW.UPLOADER( 1061): doUpload() done!
W/MW.MAIN ( 1061): File upload done.
W/MW.MAIN ( 1061): Position: Lat: -33.8684908 Lon:
151.2063652
W/MW.MAIN ( 1061): Distance: 11.297495
W/MW.MAIN ( 1061): Starting recording...
V/MW.RECORDER( 1061): Entering startRecording()
V/MW.RECORDER( 1061): Exiting startRecording()

ONLINE 480x800 (1.5 Mb) 1130 ms (1.3 Mbits)

```

Elevator



Lobby



Elevator



Lobby



Elevator



Exec Desk



Lobby



Elevator



Exec Desk



Coffee Shop



Lobby



Elevator



Exec Desk



Coffee Shop



A diagram showing a process flow. It starts with a dark grey arrow pointing right, containing the text "No Password". This arrow points into a larger, light grey arrow pointing right, which contains the text "No pin/password controls by default; Not complex by default".

No Password

**No pin/password controls by default;
Not complex by default**

No Password

**No pin/password controls by default;
Not complex by default**

**Password
Guessing**

**Common password combinations;
Common patterns**

No Password

**No pin/password controls by default;
Not complex by default**

**Password
Guessing**

**Common password combinations;
Common patterns**

**Smudge
Attack**



No Password

**No pin/password controls by default;
Not complex by default**

**Password
Guessing**

**Common password combinations;
Common patterns**

**Smudge
Attack**



**Face
Recognition**

No Password

**No pin/password controls by default;
Not complex by default**

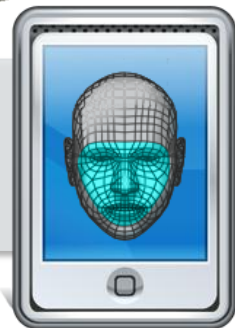
**Password
Guessing**

**Common password combinations;
Common patterns**

**Smudge
Attack**



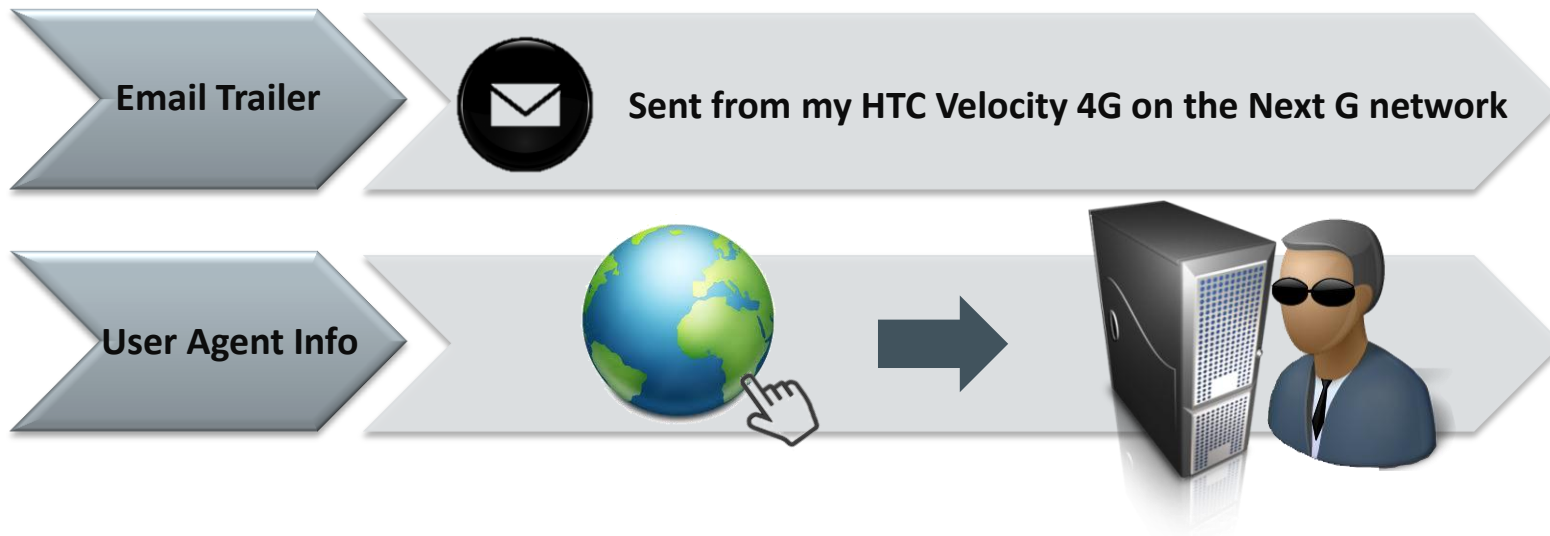
**Face
Recognition**



Email Trailer



Sent from my HTC Velocity 4G on the Next G network



Email Trailer

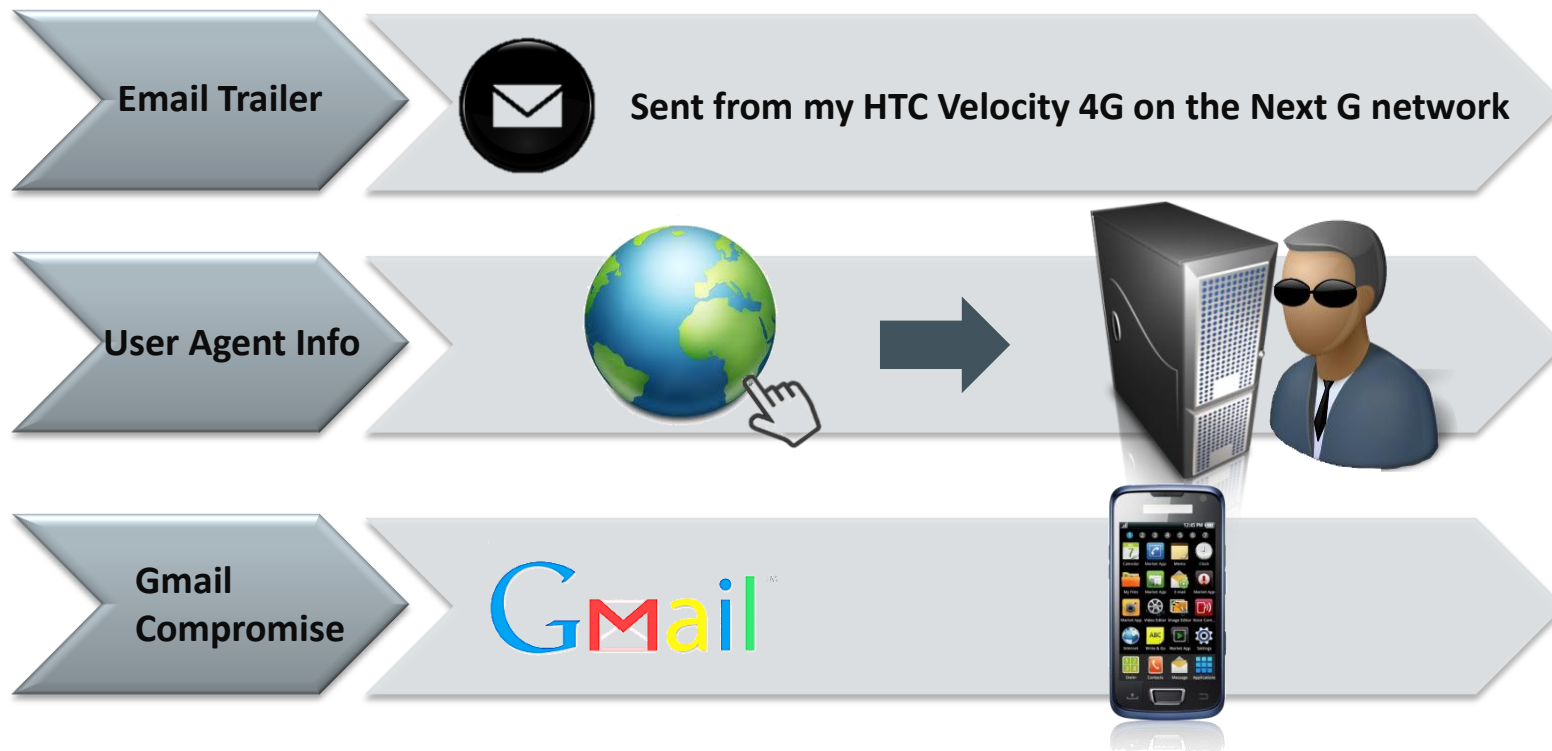


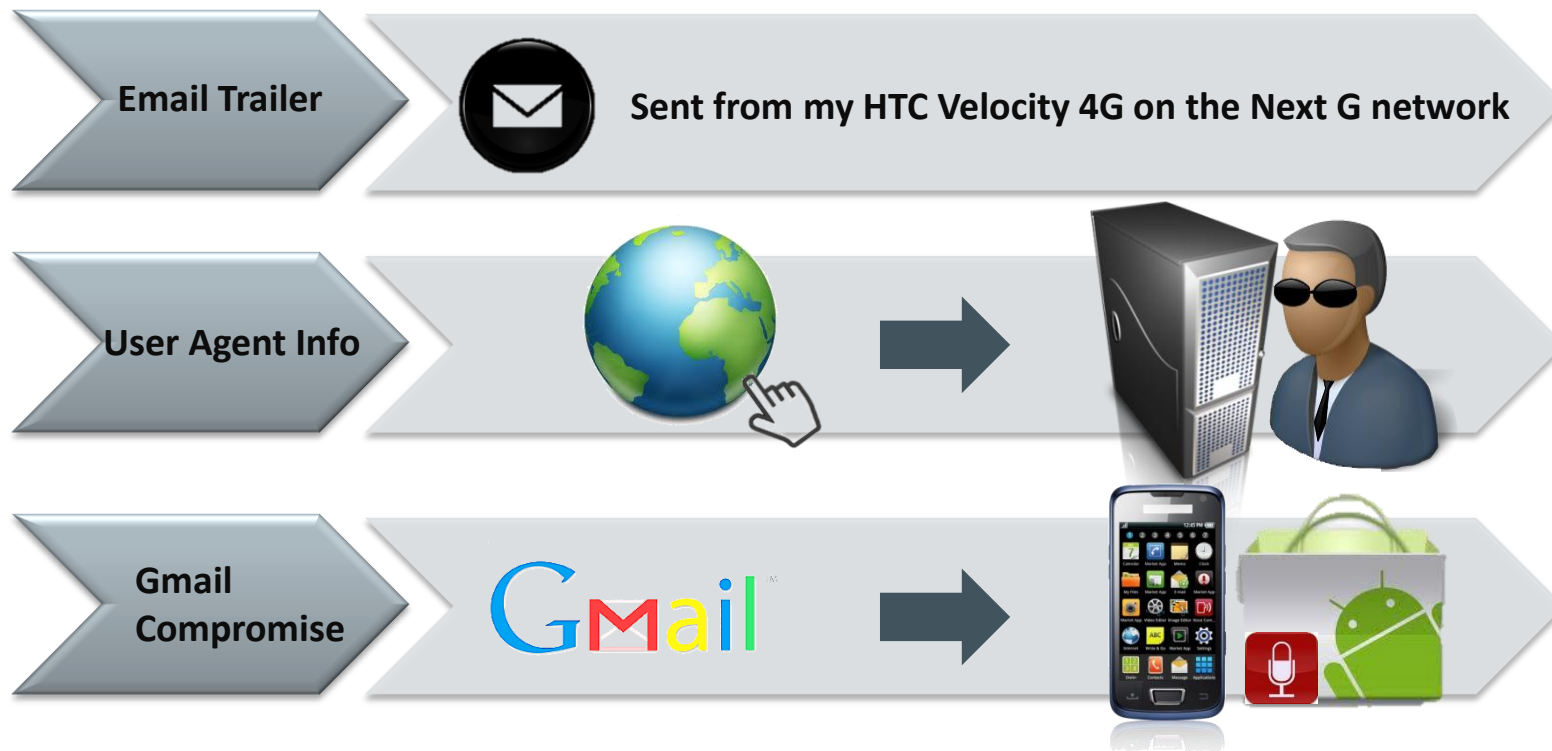
Sent from my HTC Velocity 4G on the Next G network

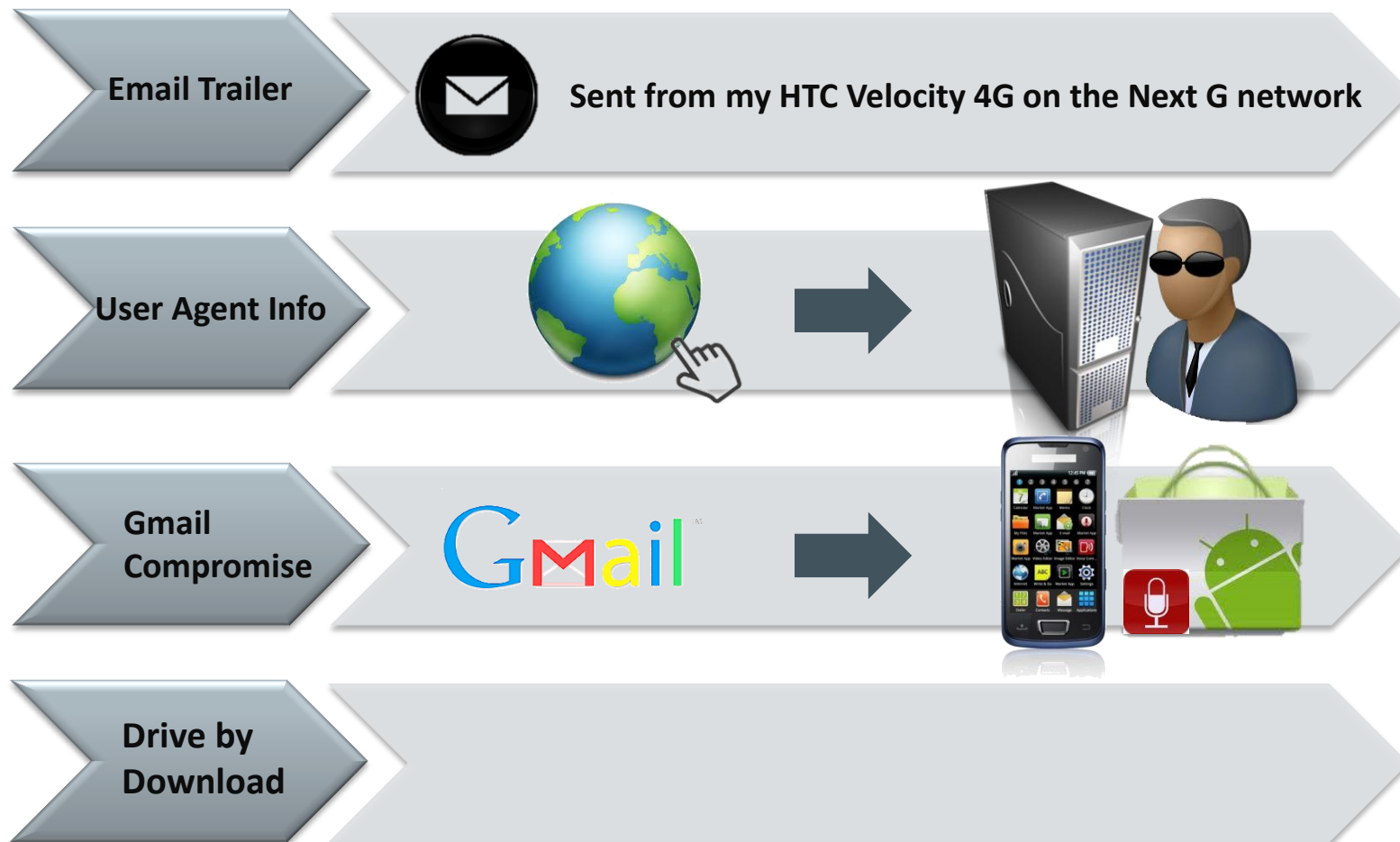
User Agent Info

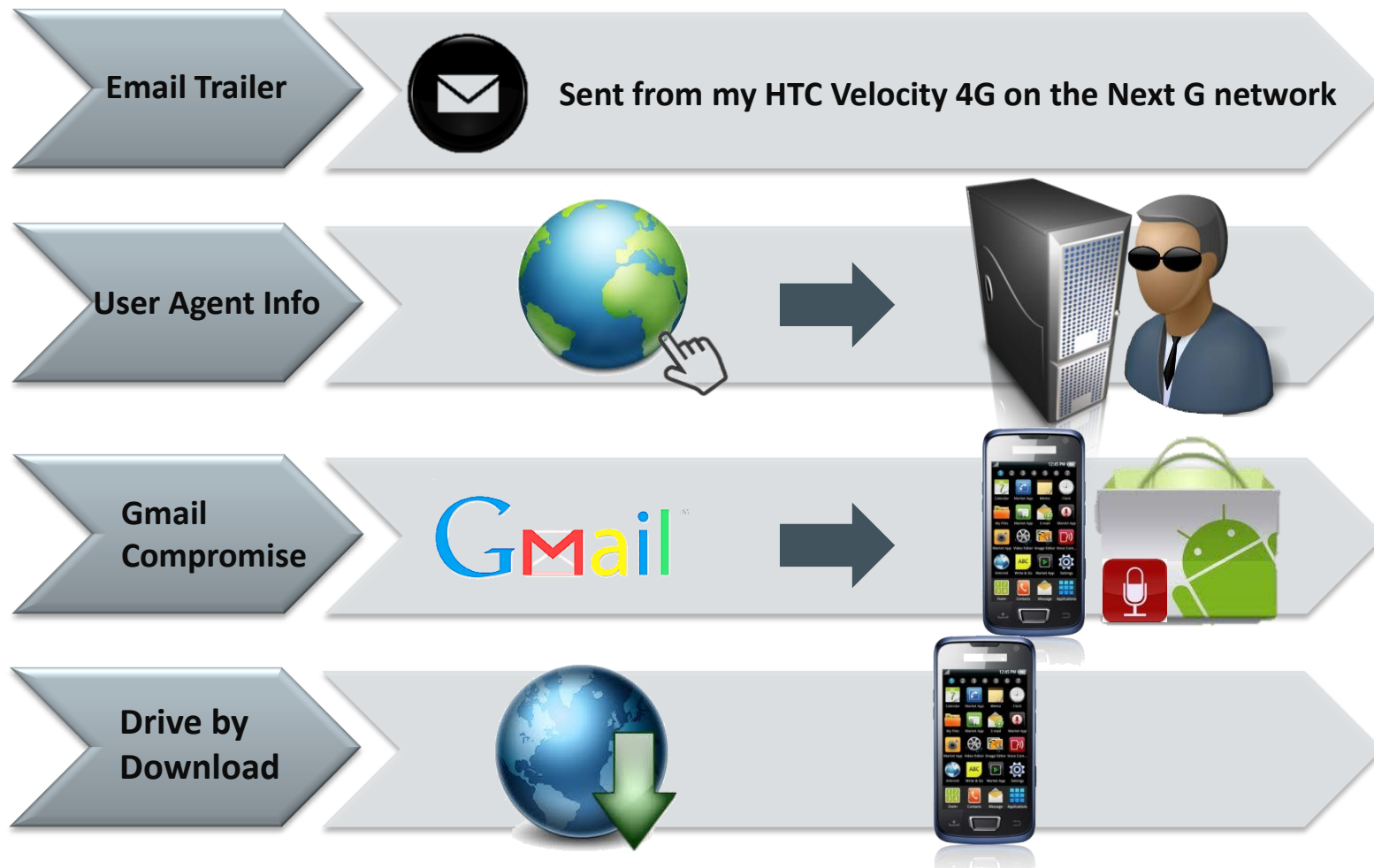


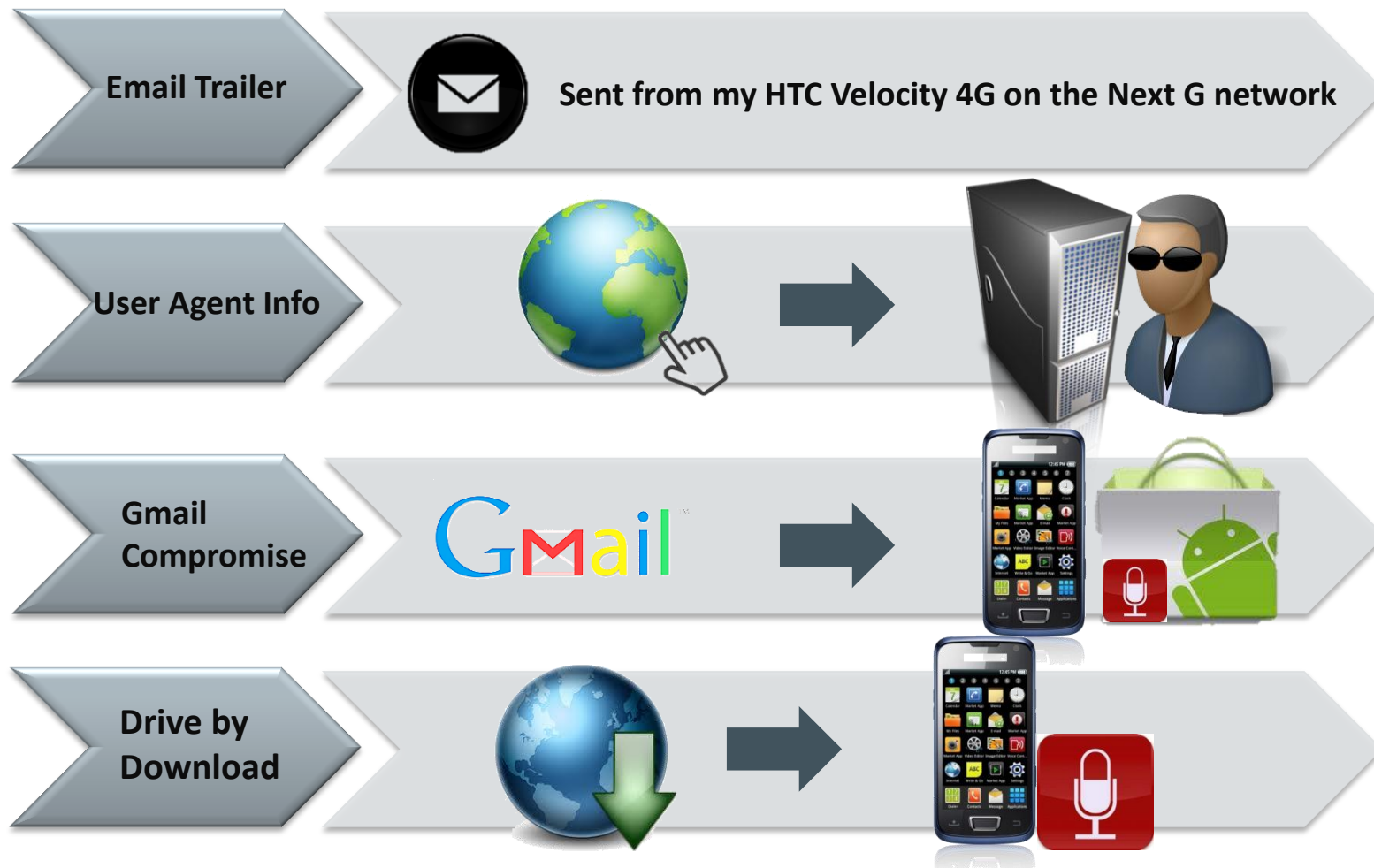
Gmail
Compromise











Email Trailer



Sent from my HTC Velocity 4G on the Next G network

User Agent Info



Gmail Compromise



Drive by Download



Spear Phishing





Access to Personal or Corporate Email



Access to SMS



Access to Images



Access to Network (personal, wireless, corporate, VPN)



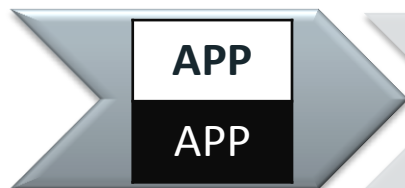
Access to Corporate Apps & Data



Send SMS to Premium Rated Services “Toll Fraud”

Controls and Mitigations

Controls that will assist in addressing this issue



Whitelist specific applications (or blacklist 2nd pref)



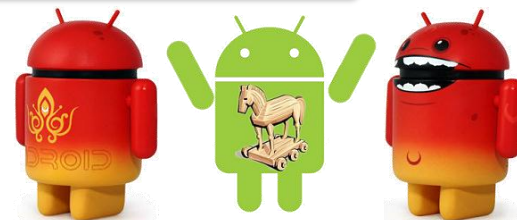
Educate users on best practices regarding mobile devices



Strong alphanumeric passcode; smudge protection



Restrict default apps and resources such as browser, camera, YouTube, and Google Play



Controls and Mitigations

Other MDM controls that should be considered ... but won't all address this issue



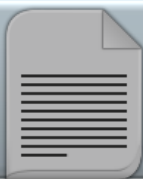
Bring corporate and employee-owned phones under centralised IT management



Connect mobile devices securely to enterprise resources including email, Wi-Fi and VPN



Enforce security policies to protect corporate data



Configure device security such as encryption of data-at-rest and passcodes



Enforce secure bring your own device (BYOD) policies if you allow staff to use their devices inside the network

Controls and Mitigations



Keep highly confidential data off mobile devices



No removable media such as SD cards allowed in corporate mobile devices



Block attachment execution or downloading to the SD card



Detect rooted devices and remote wipe when found



Internal segregation controls on what access mobile devices have inside the network

Controls and Mitigations



Expedite handling of secure lost, stolen or retired smartphones through full and selective wipe



Rogue app protection as well as inventories of installed apps



Ensure anti malware/anti virus is up to date

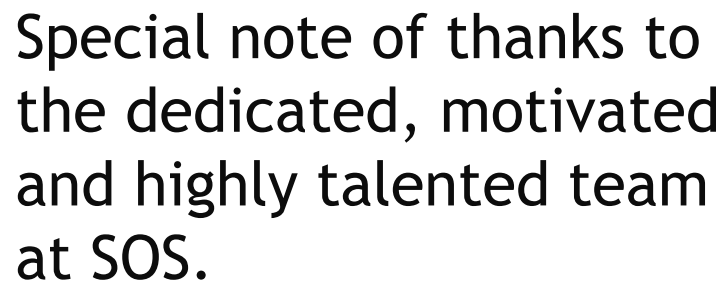


Define and enforce allowed device types, OS, and patch levels

Mobile Device Platforms

These attacks are valid across the other major platforms.





This presentation is the culmination of a research program delivered through effective collaboration, teamwork and perseverance to push the envelope on the cutting edge.



Extreme exposure



Severe implications for privacy of the individual



Severe implications for confidentiality of information for business/government



The fact that every person has/will have a mobile device means that every person is a walking/moving/sitting voice/video recorder that can be exploited



Remote control capability to spy extends the scope and risk



MDM controls are good for general security - but not all will address this issue



Requires user education; however curiosity of users and inclination to trust will result in continued exposure



Thank you

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

Owner of trademark and all copyright is Sense of Security Pty Ltd. Neither text or images can be reproduced without written permission.

This presentation will be published at
<http://www.senseofsecurity.com.au/research/presentations>

Whitepaper will be published at
<http://www.senseofsecurity.com.au/research/it-security-articles>

Attribution – icons from iconfinder.com

Sydney, Melbourne
T: 1300 922 923
info@senseofsecurity.com.au
www.senseofsecurity.com.au