Building Threat Models for the Mobile Ecosystem

Joshua M Franklin, NIST / NCCoE

Michael Peck, MITRE

Android Security Symposium
March 8, 2017

Joshua M Franklin

- Security Engineer – National Institute of Standards and Technology
- MS Information Security and Assurance from George Mason University
- Focus on electronic voting, enterprise mobile security, and cellular security in the context of public safety

Michael Peck

- Security Engineer – The MITRE Corporation
- MS Security Informatics from Johns Hopkins University, BS Computer Science from the University of Virginia
- Focus on mobile application security, mobile device security, and network security protocols

VISION

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

STAKEHOLDERS

SPONSORS

Advise, assist, and facilitate the Center's strategic initiatives

- The White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- Maryland State

TEAM

Collaborate with innovators to provide real-world cybersecurity capabilities that address business needs

- NCCoE
- National Cybersecurity FFRDC*
- Tech Firms
- Industry
- Academia
- Government
- Project Specialists
- Project-Specific Collaborators
- National Cybersecurity Excellence Partnership (NCEP) Partners

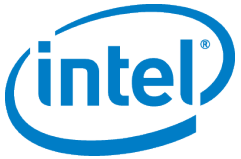
**Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation*

CUSTOMERS

Collaborate with center on project-specific use cases that help our customer's manage their cybersecurity priorities

- Business Sectors
- Individuals
- Academia
- Government
- Cybersecurity IT Community
- Systems Integrators

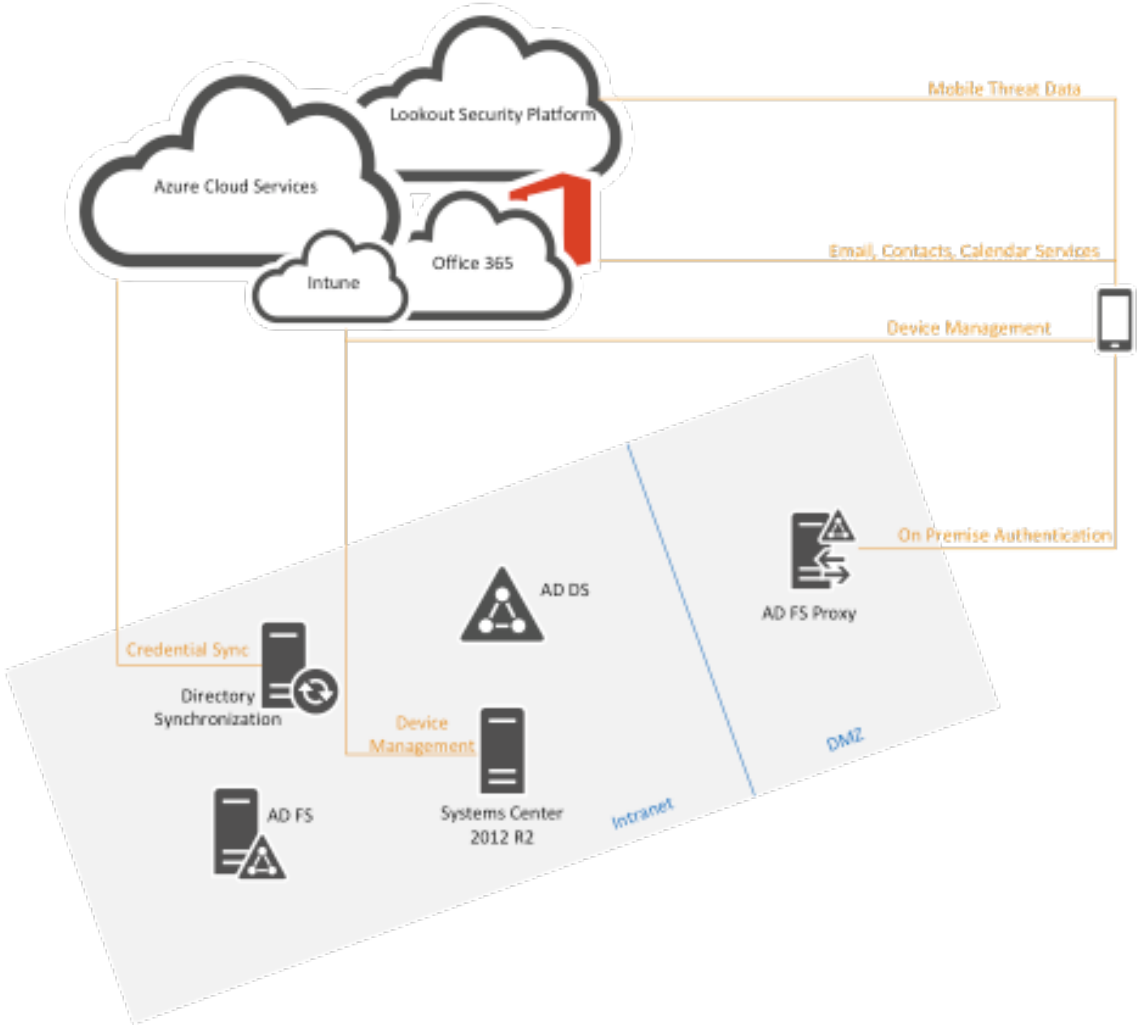
NATIONAL CYBERSECURITY EXCELLENCE PARTNERS



NCCOE MOBILE SECURITY EFFORTS

NIST SP 1800-4

- Broadly applicable across much of a sector, or across sectors
- Addressable through reference designs built in our labs
- Complex enough that our reference designs will need to be based on the combination of multiple commercially available technologies
- Primary goal:
  - Enable email, contacts, and calendar



MOBILE THREAT CATALOGUE

Mobile Threat Catalogue Purpose

- Identify threats to devices, applications, networks, & infrastructure
- Collect countermeasures that IT security engineers can deploy to mitigate threats
- Inform risk assessments
- Build threat models
- Enumerate attack surface for enterprise mobile systems
- Assist in standards mapping activities

Perform a Baseline Review of:

- threat landscape
- mobile security literature
- industry practices
- enterprise protections provided by industry

Information Collected Per Threat

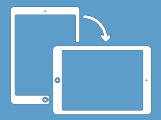
- Identified the following information for each threat:
  - **Threat Category:** The major topic area pertaining to this threat. Topic areas are further divided when necessary.
  - **Threat Origin:** Reference to the source material used to initially identify the threat.
  - **Exploit Example:** A reference to examples of specific instances of this threat.
  - **Common Vulnerability and Exposure (CVE) Reference:** A specific vulnerability located within the National Vulnerability Database (NVD).
  - **Countermeasure:** Security controls or mitigations identified to reduce the impact of a particular threat.
- Links to reference materials (talks, publications, academic papers) included

APPLICATION
Mobile applications

AUTHENTICATION
Something you know, have, or are

CELLULAR
Telecommunications networks

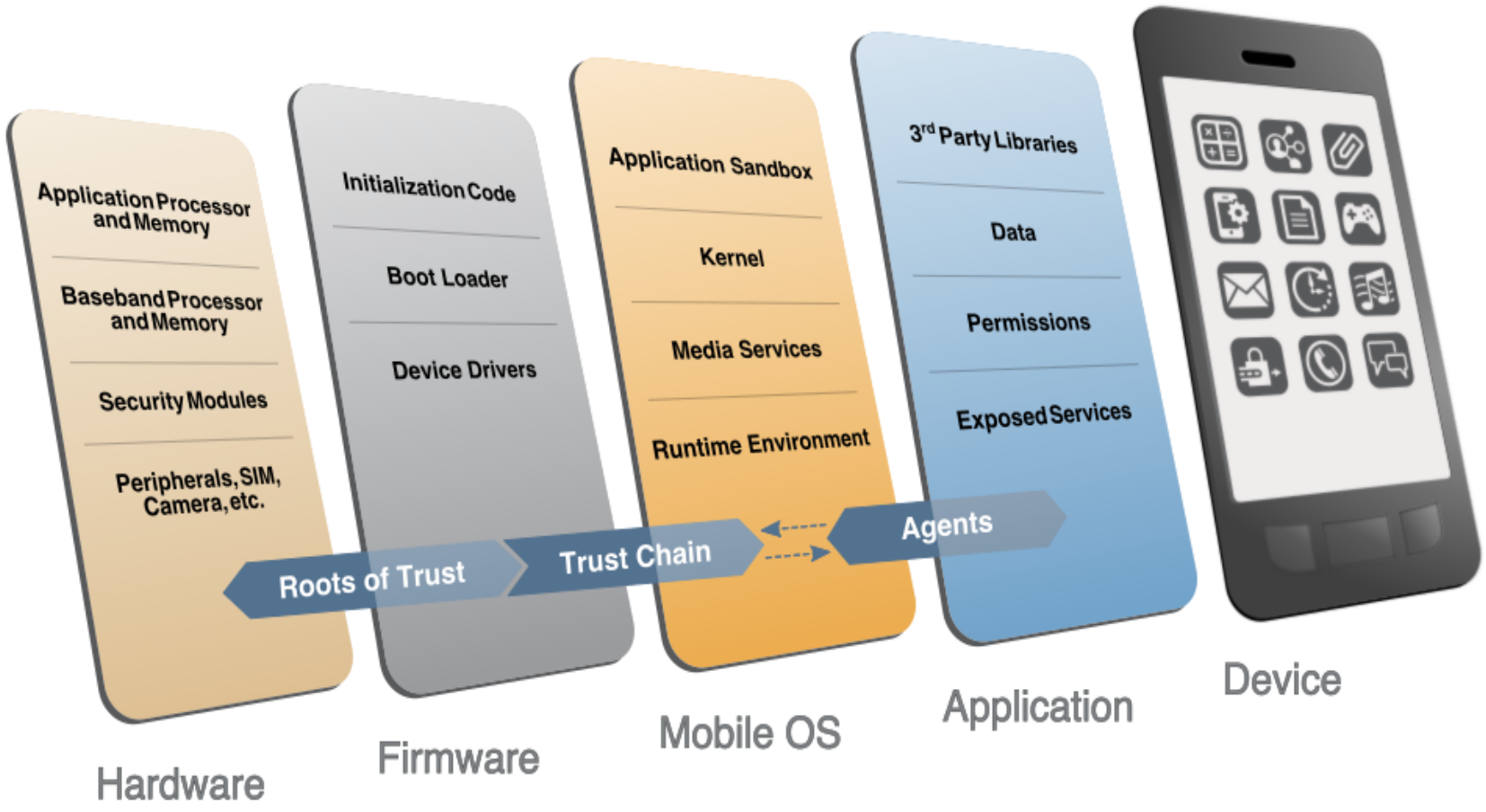
ECOSYSTEM
Vendor infrastructure, application stores



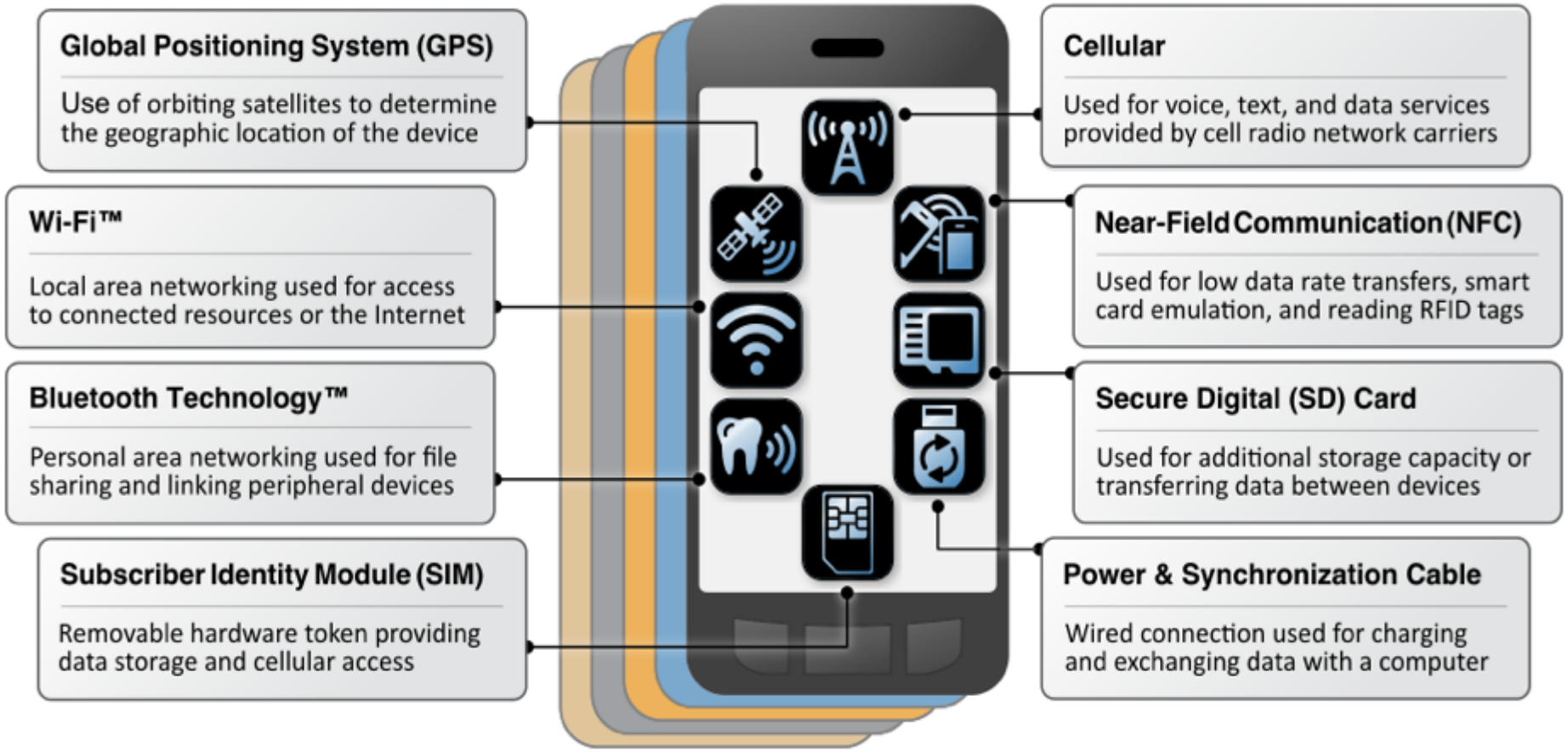
MOBILE DEVICE
Hardware, firmware, OS

NETWORK INTERFACES
Wifi, NFC, bluetooth

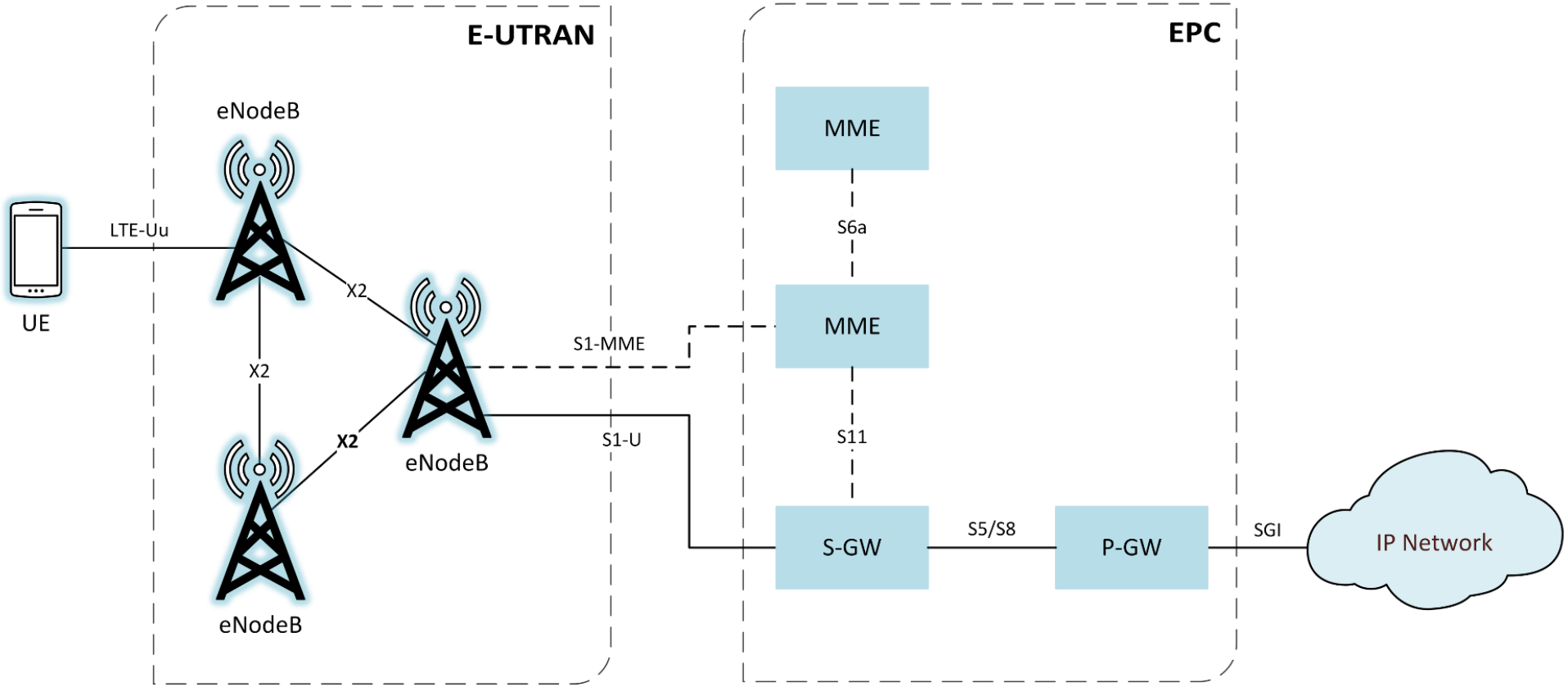
Mobile Device Stack



Network Interfaces



Mobile Network Infrastructure



Air Interface Eavesdropping

Contribute

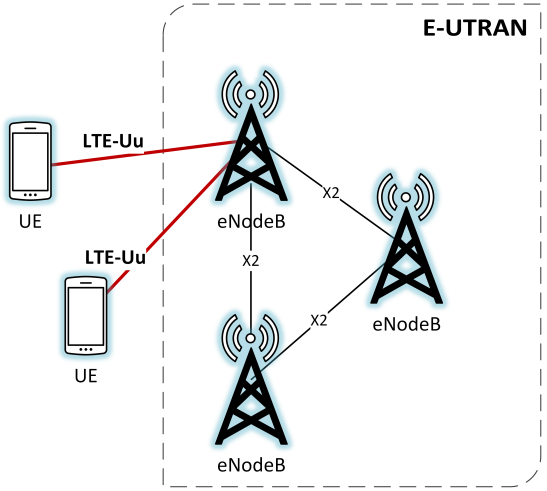
- **Threat Category:** Cellular Air Interface
- **ID:** CEL-0
- **Threat Origin:**
  - 3G Security: Security Threats and Requirements (Release 4) [1]
  - LTE Architecture Overview and Security Analysis (Draft NISTIR 8071) [2]
- **Exploit Examples:**
  - Attacking phone privacy [3]
  - A man-in-the-middle attack on UMTS [4]
- **CVE Examples:**
- **Possible Countermeasures:**
  - **Original Equipment Manufacturer and Mobile OS Developer**: Use of a ciphering indicator in the interface of the mobile device to inform the user as to whether or not user data (e.g. voice calls, SMS/MMS messages, data) are being encrypted.
  - **Mobile Network Operator**: Network level air interface encryption for user-plane traffic.
  - **Mobile Device User and Enterprise**: To prevent an attacker who intercepts traffic on the unencrypted channel between a mobile device and a base station, use a mobile VPN or another third-party over-the-top encryption solution to encrypt data prior to transmission over the air interface.

References

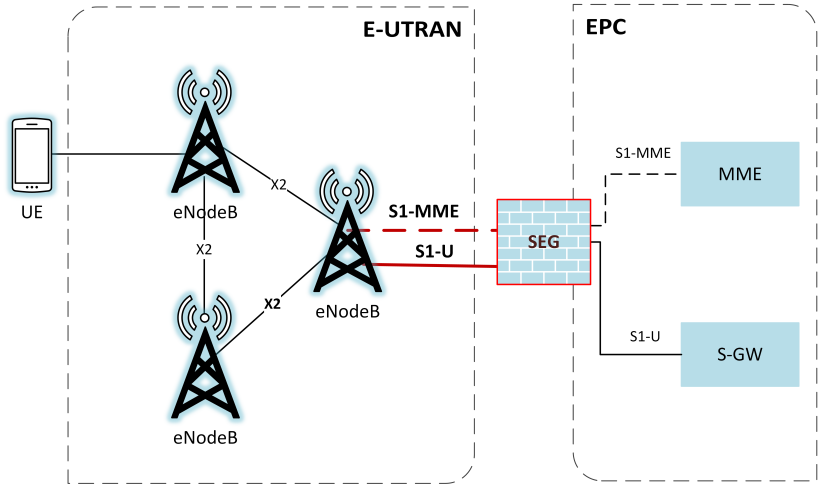
1. 3G Security; Security Threats and Requirements (Release 4), 3GPP TS 21.133 V4.0.0, 3rd Generation Partnership Project, 2003; www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/Old_Vsns/21133-400.pdf [Accessed 8/23/2016] ↩
2. J. Cichonski, J.M. Franklin, and M. Bartock, LTE Architecture Overview and Security Analysis, Draft NISTIR 8071, National Institute of Standards and Technology, 2016; http://csrc.nist.gov/publications/drafts/nistir-8071/nistir_8071_draft.pdf [Accessed 8/23/2016] ↩
3. K. Nohl, Attacking Phone Privacy, presented at Blackhat, 29 July 2010; https://media.blackhat.com/bh-ad-10/Nohl/BlackHat-AD-2010-Nohl-Attacking-Phone-Privacy-wp.pdf [accessed 8/23/2016] ↩
4. U. Meyer and S. Wetzel, “A Man-in-the-Middle Attack on UMTS”, Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 90-97; http://dx.doi.org/10.1145/1023646.1023662 [accessed 8/23/2016] ↩

Additional Mitigations

- The connection between a phone and the base station is the air interface
- 3 algorithms exist to protect the LTE air interface: Inform risk assessments
  - SNOW 3G = stream cipher designed by Lund University (Sweden)
  - AES = Block cipher standardized by NIST (USA)
  - ZUC = stream cipher designed by the Chinese Academy of Sciences (China)

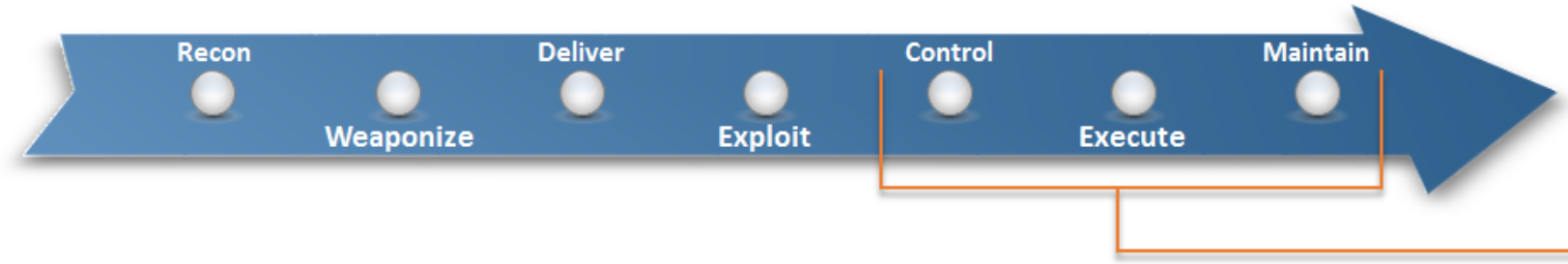



```
▼UE security capability - Replayed UE security capabilities
  Length: 2
  1... .... = EEA0: Supported
  .1.. .... = 128-EEA1: Supported
  ..1. .... = 128-EEA2: Supported
  ...0 .... = 128-EEA3: Not Supported
  .... 0... = EEA4: Not Supported
  .... .0.. = EEA5: Not Supported
  .... ..0. = EEA6: Not Supported
  .... ...0 = EEA7: Not Supported
  1... .... = EIA0: Supported
  .1.. .... = 128-EIA1: Supported
  ..1. .... = 128-EIA2: Supported
  ...0 .... = 128-EIA3: Not Supported
```



THE ATT&CK™ MODEL

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) Model



Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Execution
Collection
Exfiltration
Command and Control

Threat data informed adversary model, focused on right-of-exploit, post-access phases

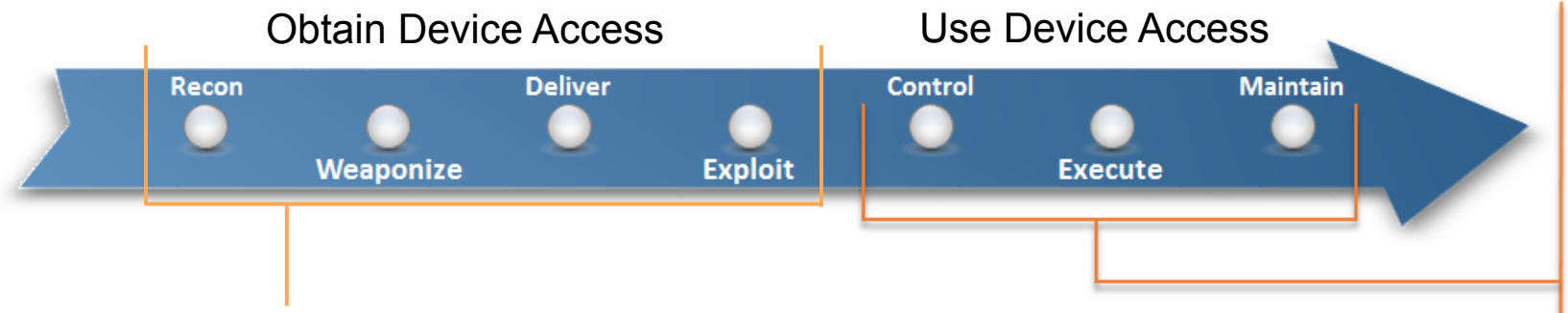
Initially focused on enterprise Windows PC environment

- Tactics derived from Cyber Attack Lifecycle
- Techniques available to adversaries for each tactic
- Possible methods of detection and mitigation
- Documented adversary use of techniques and software

ATT&CK™ Web Site: https://attack.mitre.org/

The ATT&CK™ Mobile Profile

- Tactics and techniques used by adversaries to obtain access to mobile device and to then make use of that access



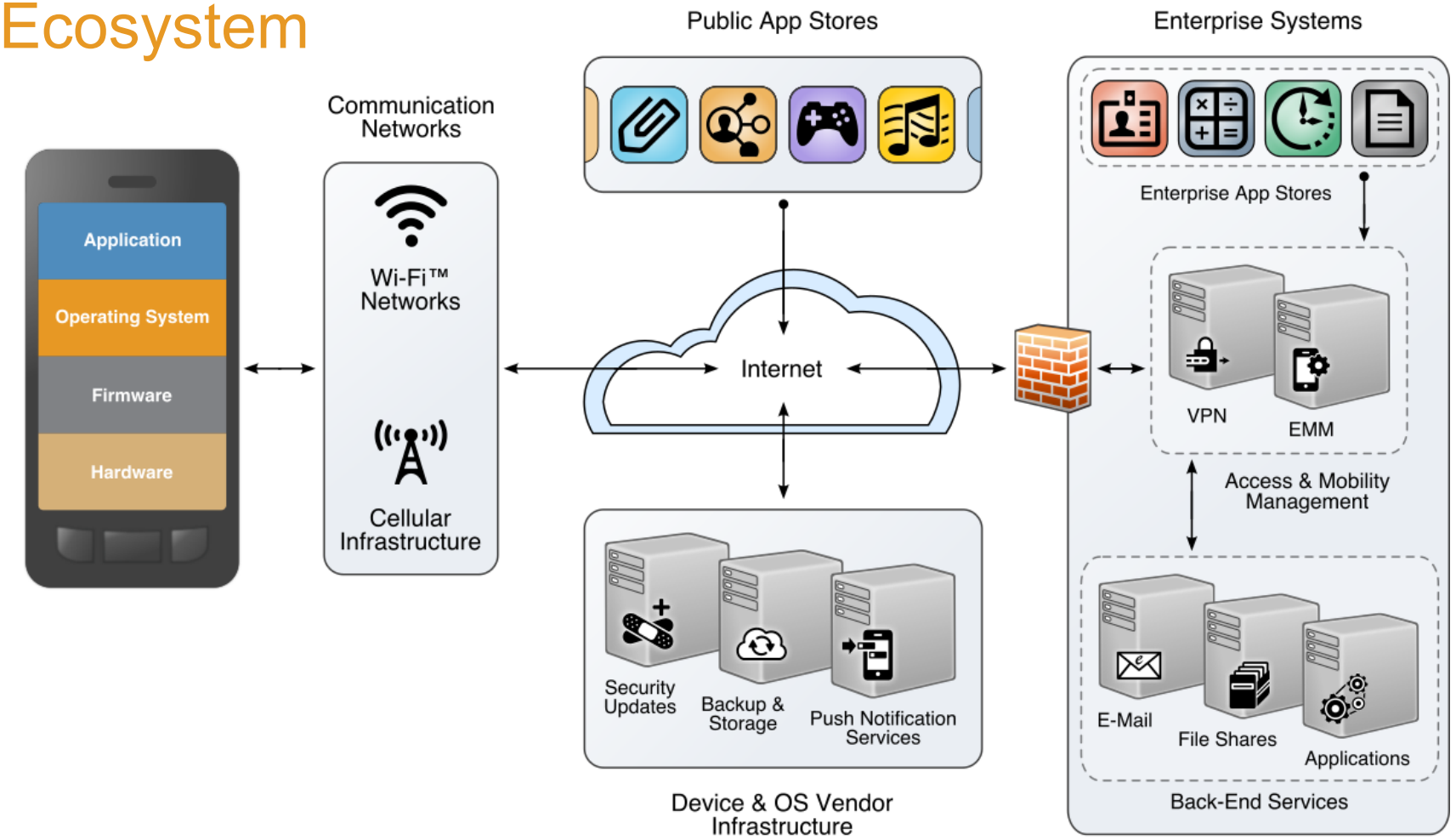
Malicious App Delivered via App Store
Malicious App Delivered via Other Means
Exploit via Cellular Network
Exploit via Internet
Exploit via Physical Access
Supply Chain

Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Effects
Collection
Exfiltration
Command and Control

Use Cases

- **Depict tactics/techniques used by specific adversary campaigns**
- **Perform gap analysis of defenses**
- Determine appropriate enterprise threat mitigation and detection strategies
- Adversarial threat emulation for security testing

Mobile Ecosystem



Mobile devices have security dependencies on the broader mobile ecosystem
The ATT&CK Mobile Profile reflects this by also describing Network-Based Effects

ATT&CK Matrix Example – Pegasus iOS Spyware

Depict Adversary Use of Techniques: **Obtain Device Access**

App Delivery via Authorized App Store	App Delivery via Other Means	Exploit via Cellular Network	Exploit via Internet	Exploit via Physical Access	Supply Chain
Evade Analysis	Abuse iOS Enterprise App Signing Key	Exploit Baseband Vulnerability	Malicious Media Content	PIN/Password Guessing or Brute Force	Malicious Compiler or Other SW Dev Tools
Fake Developer Accounts	App Delivered via Email Attachment	Malicious SMS Message	Malicious Web Content	From Compromised PC or Charging Station	
Remotely Install App				Lockscreen Bypass Attack	Malicious or Exploitable 3rd Party SW Libraries
Stolen Developer Credentials	App Delivered via Web Download			Biometric Spoofing	
Repackaged Application					

Based on Lookout and Citizen Lab analysis

Indicates Techniques Used

ATT&CK Matrix Example – Pegasus iOS Spyware

Depict Adversary Use of Techniques: **Use Device Access**

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Effects	Collection	Exfiltration/Cmd and Ctrl
Abuse Android Device Admin Access to Prevent Removal	Exploit OS Vulnerability	Disguise Root/Jailbreak Indicators	Abuse Accessibility Features	Application Discovery	Attack PC via USB	Encrypt Files for Ransom	Access Contact List, Call Log, or Calendar	Alternate Network Medium/Protocol (e.g. Cellular Data, SMS, NFC, Bluetooth)
	Exploit TEE Vulnerability		Access Credentials in Device Logs	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs	
App Auto-Start at Device Boot		Download New Code at Runtime	Access Credentials in Files	File and Directory Discovery			Access Sensitive Data in Files	
Modify OS Kernel or Boot Partition		Obfuscated or Encrypted Payload	Android Intent or iOS URL Scheme Hijacking	Local Network Configuration Discovery		Lock User Out of Device	Capture Clipboard Data	Commonly Used Port
Modify System Partition			Capture Clipboard Data	Local Network Connection Discovery		Manipulate App Store Rankings or Ratings	Keypress Capture	Standard App Layer Protocol
Modify TEE			Capture SMS Messages	Network Service Scanning			Location Tracking	
Modify Android Cached Executable Code			Exploit TEE Vulnerability	Process Discovery		Premium SMS Fraud	Microphone or Camera Recordings	
			Keypress Capture	System Information Discovery		Wipe Device Data	Network Traffic Redirection	
			Network Traffic Capture					
			User Interface Spoofing					

Based on Lookout and Citizen Lab analysis

Indicates Techniques Used

ATT&CK Matrix: Network-Based Effects

Techniques adversaries may be able to use without access to the mobile device itself

<table>
<tr><th>General Network-Based</th><th>Cellular Network-Based</th><th>Cloud-Based</th></tr>
<tr><td colspan="2">Downgrade to Insecure Protocols</td><td>Obtain Device Cloud Backups</td></tr>
<tr><td colspan="2">Jamming or Denial of Service</td><td rowspan="2">Remotely Track Device Without Authorization</td></tr>
<tr><td colspan="2">Eavesdrop on Insecure Network Communication</td></tr>
<tr><td>Rogue Wi-Fi Access Point</td><td>Rogue Base Station</td><td rowspan="4">Remotely Wipe Device Without Authorization</td></tr>
<tr><td rowspan="3">Manipulate Communication</td><td>Exploit SS7 to Redirect Calls/SMS</td></tr>
<tr><td>Exploit SS7 to Track Location</td></tr>
<tr><td>SIM Card Swap</td></tr>
</table>

Example Technique Entry

Microphone or Camera Recordings

An adversary could use a malicious or exploited application to surreptitiously record activities using the device microphone and/or camera through use of standard operating system APIs.

Contents [hide]

Microphone or Camera Recordings

Technique

ID	T1032
Tactic type	Post-Adversary Device Access
Tactic	Collection
Platform	Android, iOS
MTC ID	APP-19

Examples

- Pegasus has the ability to record audio[1].
- AndroRAT gathers "audio from the microphone."[2]
- As described by Trend Micro[3], RCSAndroid can "[r]ecord using the microphone" and can "[c]apture photos using the front and back cameras".
- Dendroid "can take pictures using the phone's camera, record audio and video"[4].
- SpyNote RAT can activate "the device's microphone" and listen "to live conversations"[5].
- DroidJack RAT performs "call recording" and "video capturing"[6].

Detection

On both Android (6.0 and up) and iOS, the user can view which applications have permission to use the microphone or the camera through the device settings screen, and the user can choose to revoke the permissions.

Mitigation

- Application Vetting - On Android, applications must request the RECORD_AUDIO permission to access the microphone and the CAMERA permission to access the camera. Extra scrutiny could be given to applications that request these permissions. On iOS, calls to the relevant APIs could be detected during the vetting process.

Example Mitigation Entry

Application Vetting

Enterprises can vet applications for exploitable vulnerabilities or unwanted (privacy-invasive or malicious) behaviors. Enterprises can inspect applications themselves or use a third-party service.

Enterprises may impose policies to only allow pre-approved applications to be installed on their devices or may impose policies to block use of specific applications known to have issues. In Bring Your Own Device (BYOD) environments, enterprises may only be able to impose these policies over an enterprise-managed portion of the device.

Application Vetting	
Mitigation	
ID	M1005

Application Vetting is not a complete mitigation. Techniques such as Detect App Analysis Environment exist that can enable adversaries to bypass vetting.

Techniques Addressed by Mitigation

- Abuse Device Administrator Access to Prevent Removal
- App Auto-Start at Device Boot
- Exploit OS Vulnerability
- Exploit TEE Vulnerability
- Obfuscated or Encrypted Payload
- Download New Code at Runtime
- Access Sensitive Data or Credentials in Files
- Network Traffic Capture or Redirection
- User Interface Spoofing
- Capture SMS Messages
- Access Sensitive Data in Device Logs
- Capture Clipboard Data
- URL Scheme Hijacking
- Android Intent Hijacking
- Malicious Third Party Keyboard App
- Application Discovery
- Device Type Discovery
- Local Network Connections Discovery
- Local Network Configuration Discovery
- Process Discovery
- Insecure Third-Party Libraries
- Microphone or Camera Recordings
- Location Tracking
- Access Contact List
- Access Call Log
- Access Calendar Entries
- Fake Developer Accounts
- Lock User Out of Device
- Wipe Device Data
- Premium SMS Toll Fraud
- Abuse Accessibility Features
- Manipulate Device Communication
- Encrypt Files for Ransom
- Generate Fraudulent Advertising Revenue

Technique/T1036

Example Software Entry

Software: Pegasus

Discovered by Lookout[1] and Citizen Lab[2], Pegasus escalates privileges on iOS devices and uses its privileged access to collect a variety of sensitive information.

Pegasus	
Software	
ID	S0005
Aliases	Pegasus
Type	Malware

Techniques Used

- Local Network Configuration Discovery - **Pegasus** "monitors the current connection state and tracks which types of networks the phone is connected to, potentially in order to determine the bandwidth and ability to send full data across the network"[1].
- Alternate Network Mediums - **Pegasus** uses SMS for command and control[1].
- Microphone or Camera Recordings - **Pegasus** has the ability to record audio[1].
- Modify System Partition - **Pegasus** modifies the system partition to maintain persistence[1].
- Location Tracking - **Pegasus** "constantly updates and sends the location of the phone"[1].
- Exploit OS Vulnerability - **Pegasus** exploits iOS vulnerabilities to escalate privileges[1].
- Capture SMS Messages - **Pegasus** captures "SMS messages the victim sends or receives"[1].
- Access Call Log - **Pegasus** captures call logs[1].
- System Information Discovery - "**Pegasus**...constantly monitors the phone for status and disables any other access to the phone by previous/other jailbreaking software."[1]
- Access Contact List - **Pegasus** "gathers contacts from the system, dumping the victim's entire address book."[1]
- Access Sensitive Data or Credentials in Files - **Pegasus** accesses sensitive data in files, for example it "saves any calls that Skype has previously recorded by reading them out of the Skype database files."[1]
- Malicious SMS Message - **Pegasus** was delivered via an SMS message containing a link to a web site with malicious code[2].
- Malicious Web Content - **Pegasus** was distributed through a web site and exploits vulnerabilities in the Safari web browser on iOS devices[1].

References

1. a b c d e f g h i j k l m ↑ Lookout. (2016). Technical Analysis of Pegasus Spyware. Retrieved December 12, 2016.

2. a b ↑ Bill Marczak and John Scott-Railton. (2016, August 24). The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. Retrieved December 12, 2016.

Using ATT&CK for Defensive Gap Analysis

Obtaining Device Access

<table>
<tr><th>App Delivery via Authorized App Store</th><th>App Delivery via Other Means</th><th>Exploit via Cellular Network</th><th>Exploit via Internet</th><th>Exploit via Physical Access</th><th>Supply Chain</th></tr>
<tr><td>Evade Analysis</td><td>Abuse iOS Enterprise App Signing Key</td><td>Exploit Baseband Vulnerability</td><td>Malicious Media Content</td><td>PIN/Password Guessing or Brute Force</td><td rowspan="2">Malicious Software Development Tools</td></tr>
<tr><td>Fake Developer Accounts</td><td rowspan="2">Email Attachment</td><td>Malicious SMS Message</td><td>Malicious Web Content</td><td>From Compromised PC or Charging Station</td></tr>
<tr><td>Remotely Install App</td><td colspan="2" rowspan="2">Notional analysis</td><td>Lockscreen Bypass</td><td rowspan="2">Malicious or Exploitable 3rd Party SW Libraries</td></tr>
<tr><td>Stolen Developer Credentials</td><td>Web Download</td><td>Biometric Spoofing</td></tr>
<tr><td colspan="2">Repackaged Application</td></tr>
</table>

Full Ability to Mitigate or Detect
Partial Ability to Mitigate or Detect
No/Minimal Ability to Mitigate or Detect

Using ATT&CK for Defensive Gap Analysis

Use Device Access

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Effects	Collection	Exfiltration/Cmd and Ctrl
Abuse Android Device Admin Access to Prevent Removal	Exploit OS Vulnerability	Disguise Root/Jailbreak Indicators	Access Credentials in Device Logs	Application Discovery	Attack PC via USB	Encrypt Files for Ransom	Abuse Accessibility Features	Alternate Network Medium/Protocol (e.g. Cellular Data, SMS, NFC, Bluetooth)
			Access Credentials in Files	Device Type Discovery	Exploit Enterprise Resources	Generate Fraudulent Advertising Revenue	Access Contact List, Call Log, or Calendar	
App Auto-Start at Device Boot	Exploit TEE Vulnerability	Download New Code at Runtime	Android Intent or iOS URL Scheme Hijacking	File and Directory Discovery			Access Sensitive Data in Device Logs	
Modify OS Kernel or Boot Partition		Obfuscated or Encrypted Payload	Capture Clipboard Data	Local Network Configuration Discovery		Lock User Out of Device	Access Sensitive Data in Files	Commonly Used Port
Modify System Partition			Capture SMS Messages	Local Network Connection Discovery		Manipulate App Store Rankings or Ratings	Capture Clipboard Data	Standard App Layer Protocol
Modify TEE			Exploit TEE Vulnerability	Network Service Scanning			Keypress Capture	
Modify Android Cached Executable Code			Keypress Capture	Process Discovery		Premium SMS Fraud	Location Tracking	
			Network Traffic Capture	System Information Discovery		Wipe Device Data	Microphone or Camera Recordings	
			User Interface Spoofing				Network Traffic Redirection	

Full Ability to Mitigate or Detect

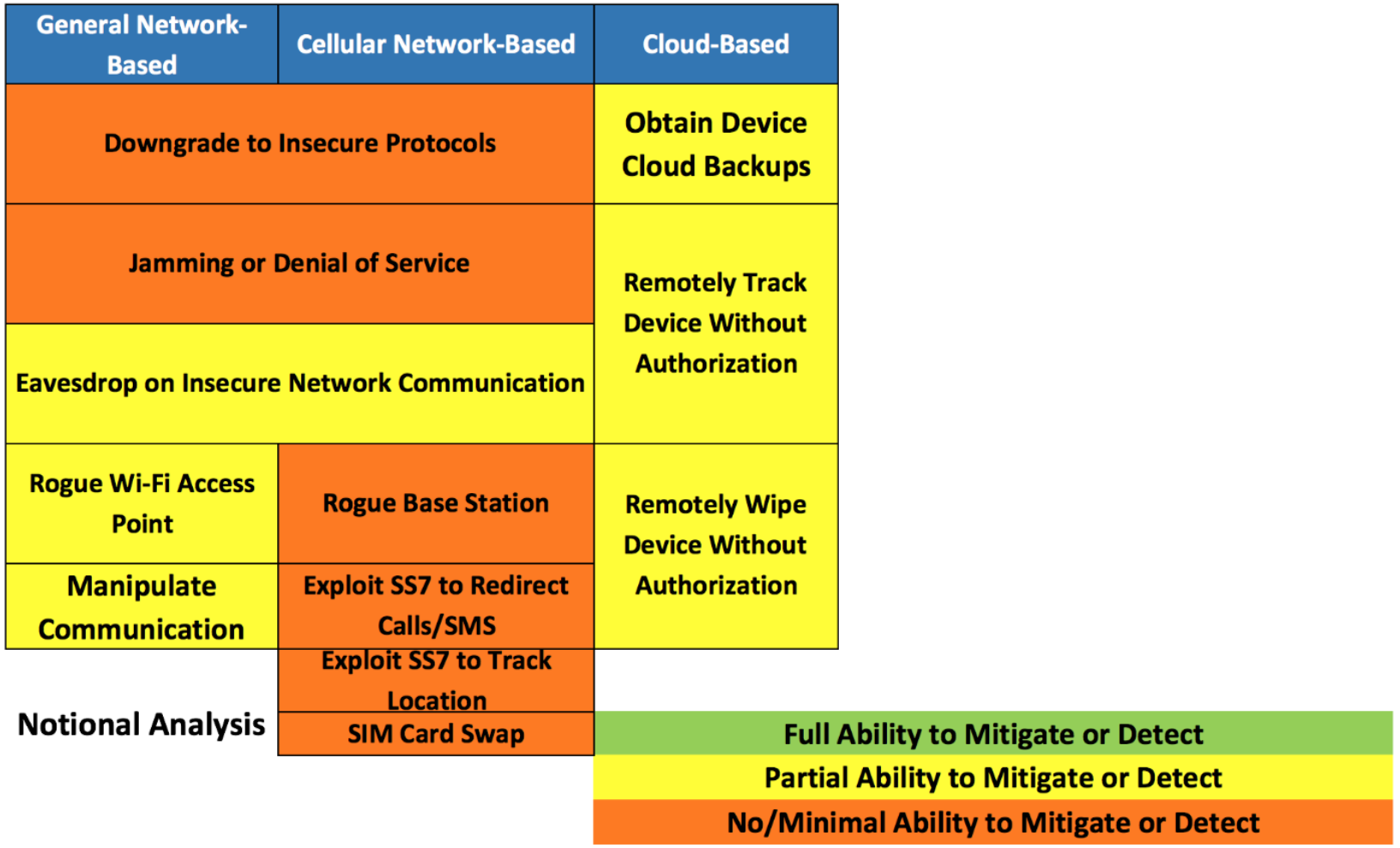
Partial Ability to Mitigate or Detect

No/Minimal Ability to Mitigate or Detect

Notional analysis

Using ATT&CK for Defensive Gap Analysis

Network-Based Effects



Bringing It All Together

- NIST / NCCoE is using ATT&CK and the MTC to perform risk assessments
  - And create NIST Cybersecurity Framework Profiles

Next Steps

- Update the MTC and ATT&CK
- Soliciting Participation from this community
  - NCCoE Mobile Device Security Project
  - Mobile Threat Catalogue
  - ATT&CK Model