Architecture, Flows, and Capabilities for .govCAR Spin 5 (Mobile)
Aug 2018
govCAR Methodology
Spin 5 Architecture View

SPIN 1 = Einstein, TIC, related network services
SPIN 2 = Exemplar Agency Endpoint environment
SPIN 3 = Cloud (IaaS and SaaS) basic structures
SPIN 4 = Exemplar Agency Data Center
SPIN 5 = Mobile
Architecture and Flows Relationship

Architecture

Architectural Layers

Mobile Device

Mobile <-> Internet Protected

Mobile <-> Internet Unprotected

Close Access

Mobile <-> Agency

Internet

NEST

TICAP/MTIPS

Agency Boundary

Agency Mobile Services

Gateway and Security Stack

Enterprise Core Services

*Mobile Device includes Unmanaged and Agency Managed Devices
Agency Mobile Device to Internet (Protected) Capabilities

**NCPS/EINSTEIN:**
- E1 Collector & Analytics
- E2 Flow, IDS, PCAP, SIEM
- E3A IPS (SMTP & DNS)
- E3A DGA Analytic
- E3A EXE-MANA

**TICAP/MTIPS:**
- FW
- Passive Sensor
- WCF
- Ib/Ob SMTP Proxy
- Recursive DNS Proxy
- Auth DNS Proxy

**Agency Boundary:**
- NGFW
- Passive Sensor
- WCF
- Ib/Ob SMTP Proxy
- Recursive DNS Proxy
- Auth DNS Proxy

**Agency Mobile Services:**
- MDM
- MAM
- VPN
- MIM
- DLP

**Agency Mobile Device:**
- Container
- App Wrapping

---

**Current:**

**Planned:**

**NCPS/EINSTEIN:**
- E1 Collector & Analytics
- E2 Flow, IDS, PCAP, SIEM
- E3A IPS (SMTP & DNS)
- E3A EXE-MANA Enh Analytic

**TICAP/MTIPS:**
- FW Enh
- Passive Sensor
- WCF Enh
- Ib/Ob SMTP Proxy Enh
- Recursive DNS Proxy
- Auth DNS Proxy Enh

**Agency Boundary:**
- NGFW
- Passive Sensor
- WCF Enh
- Ib/Ob SMTP Proxy Enh
- Recursive DNS Proxy
- Auth DNS Proxy Enh

**Agency Mobile Services:**
- MDM
- MAM Enh
- MTD
- VPN
- MAV
- MIM
- DLP

**Agency Mobile Device:**
- Container
- App Wrapping
- TPM
Agency Mobile Device to Internet (UnProtected) Capabilities
Agency Mobile Device to Agency Capabilities

Current

- TICAP/MTIPS: FW Passive Sensor
- Agency Boundary: NGFW Passive Sensor
- Agency Mobile Services: MDM, MAM, VPN, MIM, DLP
- Agency Mobile Device: Container, App Wrapping

Planned

- TICAP/MTIPS: FW Enh Passive Sensor
- Agency Boundary: NGFW Passive Sensor
- Agency Mobile Services: MDM, MAM Enh, MTD, MAV, VPN, MIM, DLP
- Agency Mobile Device: Container, App Wrapping, TPM
# External Mobile Device to Agency Capabilities

<table>
<thead>
<tr>
<th>Current</th>
<th>Planned</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TICAP/MTIPS:</strong>&lt;br&gt;FW Passive Sensor</td>
<td><strong>TICAP/MTIPS:</strong>&lt;br&gt;FW Enh Passive Sensor</td>
</tr>
<tr>
<td><strong>Agency Boundary:</strong>&lt;br&gt;NGFW Passive Sensor</td>
<td><strong>Agency Boundary:</strong>&lt;br&gt;NGFWW Passive Sensor</td>
</tr>
<tr>
<td><strong>Agency Mobile Services:</strong>&lt;br&gt;MDM&lt;br&gt;MAM&lt;br&gt;MIM DLP</td>
<td><strong>Agency Mobile Services:</strong>&lt;br&gt;MDM&lt;br&gt;MAM Enh&lt;br&gt;MAV&lt;br&gt;MIM DLP&lt;br&gt;IDS</td>
</tr>
<tr>
<td><strong>Agency Mobile Device:</strong>&lt;br&gt;Container App Wrapping</td>
<td><strong>Agency Mobile Device:</strong>&lt;br&gt;Container App Wrapping</td>
</tr>
</tbody>
</table>
Cyber Threat Framework

STAGES
The progression of cyber threats over time to achieve objectives

OBJECTIVES
The purpose of conducting an action or a series of actions

ACTIONS
Actions and associated resources used by a threat actor to satisfy an objective

Set of Threat Actions requiring counteraction by Protect / Detect / Respond
Mapping ATT&CK Mobile to NSA 2.0 Structure

PRE-EVENT
- Intent/Resource Development
- Reconnaissance/Staging
- Weaponization

GET IN
- Delivery
- Initial Compromise/Exploitation
- Installation

STAY IN
- Persistence
- Privilege escalation
- Defense Evasion
- Credential Access
- Host Enumeration/Internal Recon
- Lateral Movement
- Execution
- Command & Control

ACT
- Monitor/Exfiltration
- Alter/Deceive

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

Use Device Access
- Persistence
- Privilege Escalation
- Defense Evasion
- credential Access
- Discovery
- Lateral Movement
- Effects
- Collection
- Exfiltration
- Command and Control

Network Based Effects
- General Network Based
- Cellular Network Based
- Cloud Based
## ATT&CK Mobile in *CAR Structure*

|----------------------------|--------------------------|--------------|----------|---------------------------------|--------------|------------|---------------------|----------------|------------------|----------------------------------------|----------------|-----------|-----------------------|-----------|--------------------------|------------------|

### 100+ Threat Actions

**Initial Sources:**

* MITRE’s Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)