





Cyber Resiliency Against Supply Chain Attacks

Ellen Laderman

Overview

- **Goal: Ensure Operational Mission Assurance despite supply chain threats**
 - Mission and supporting cyber resources are able to: anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises caused by supply chain attacks
 - Builds on previously defined supply chain attacks and provides security engineering guidance
 - **FOR** applying Cyber Resiliency Mitigations (techniques) across the entire acquisition life cycle
 - **WITH** emphasis on adversarial threat and mitigating successful attacks on an operational environment

Cyber Resiliency ... Bottom Line

<p>WHY</p>  <p>The bad guys WILL get in</p> <p>Critical missions and operations fail</p>	<p>WHAT</p>  <p>Keep the mission going</p> <p>Resilience of critical cyber resources, mission,</p>	<p>HOW</p>  <p>Transformation of thought</p> <p>Architect</p> <p>Augment traditional approaches</p> <p>Adopt mission-oriented threat-based systems engineering processes</p> <p>Design, build, integrate</p>
<p>WHEN</p>  <p>Apply resiliency throughout system life cycle (requirements, acquisition, training, operation) and across enterprise architecture, policy and operational procedures</p>		<p>Design, build, integrate</p>

Draft NIST Special Publication 800-160
VOLUME 2

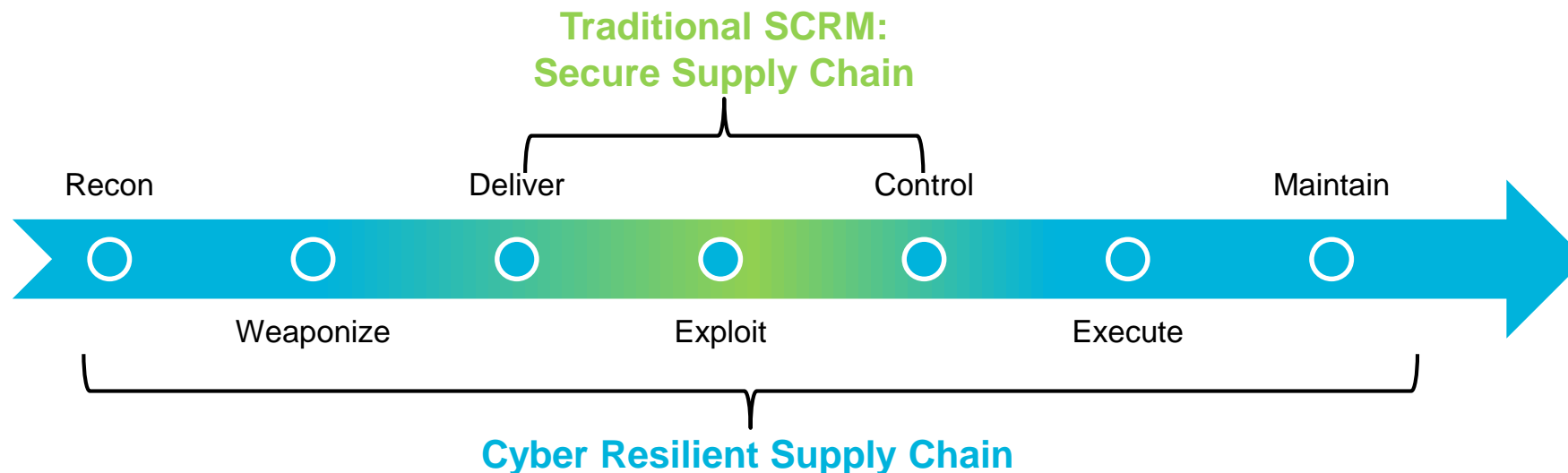
Systems Security Engineering
Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems

RON ROSS
RICHARD GRAUBART
DEBORAH BODEAU
ROSALIE MCQUAID

This document is a supporting publication to the NIST systems security engineering guidance provided in [Special Publication 800-160, Volume 1](#). The content was specifically designed to be used with and to complement the flagship systems security engineering publication to support organizations that require cyber resiliency as a property or characteristic of their systems. The goals, objectives, techniques, implementation approaches...

Focus & Cyber Attack Lifecycle

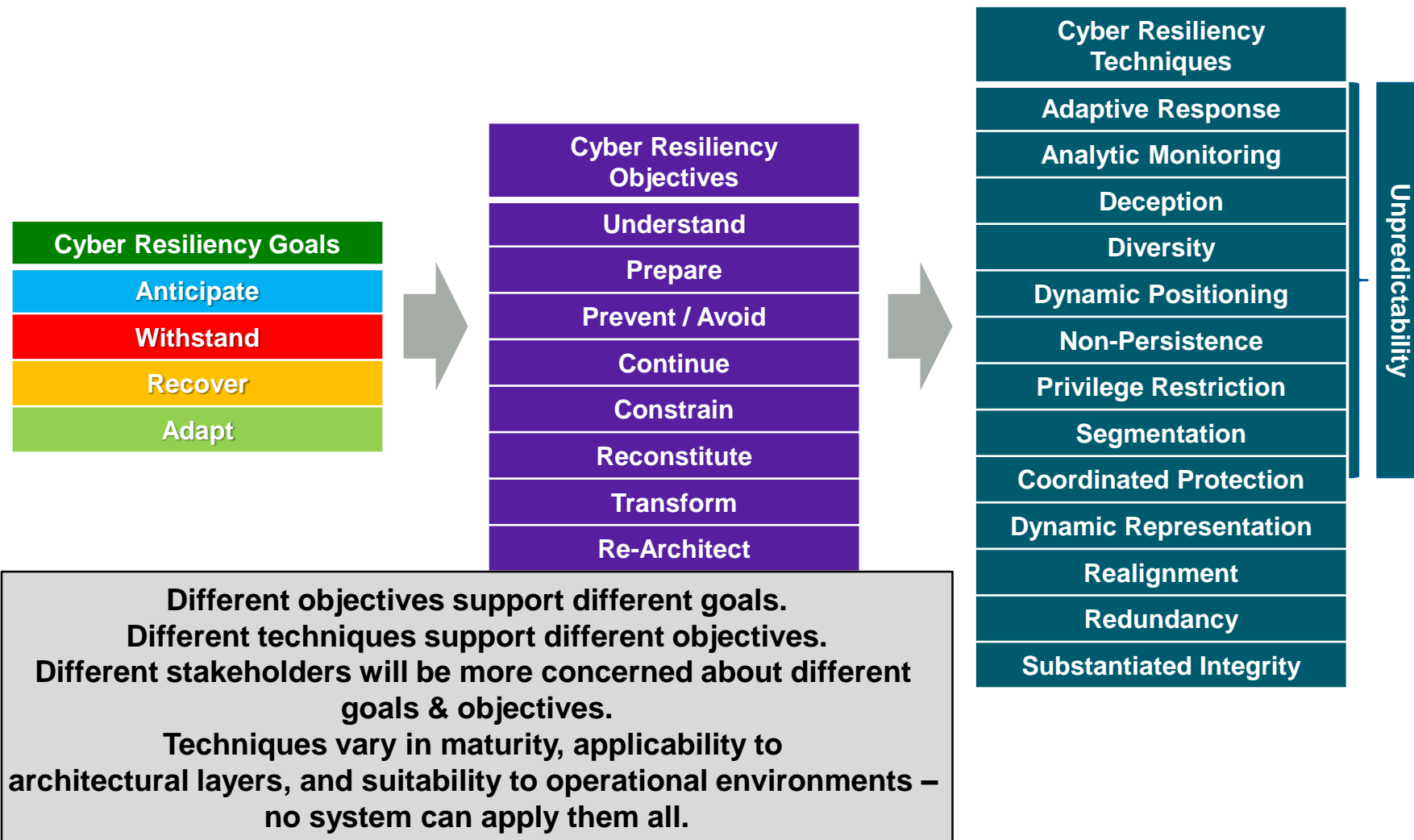
- **Traditional SCRM and acquisition requirements focus on cybersecurity and preventing adversary exploit and delivery**
 - e.g., DoDI 5000.02; NLCC; NIST SP 800-53
- **Our effort complements SCRM by increasing cyber resiliency against the whole cyber attack lifecycle**



Conventional Cyber Security vs. Cyber Resiliency

	Conventional Cyber Security	Cyber Resiliency
Threat Assumptions with respect to Adversary	<u>Capabilities</u> : Limited <u>Intent</u> : Self aggrandizement, personal benefits <u>Targeting</u> : Targets of opportunity <u>Timeline</u> : Episodic <u>Stealthy</u> : No	<u>Capabilities</u> : Sophisticated, well resourced <u>Intent</u> : Establish & maintain ability to undermine mission <u>Targeting</u> : High value targets, very persistent <u>Timeline</u> : Long term campaigns <u>Stealthy</u> : Very
Adversary Presence	Assumes can be kept out or can quickly be detected and removed	Assumes adversary has established a foothold
Types of Events Focused on	Limited duration intrusions, natural disasters, human errors, insider threats	Ongoing attacks (includes emulating conventional events), long term adversary presence, organization must “fight through” effects of adversary activities
Recovery	Adversary is not present to impede recovery	Recovery must be done despite presence of adversary
Goals	Protect, Detect, React <i>or</i> Identify, Protect, Detect, Respond, Recover	Anticipate, Withstand, Recover, Adapt

Cyber Resiliency Engineering Framework (CREF): A Structured Way to Understand the Domain



The Adversary Can Attack the Entire Acquisition Lifecycle

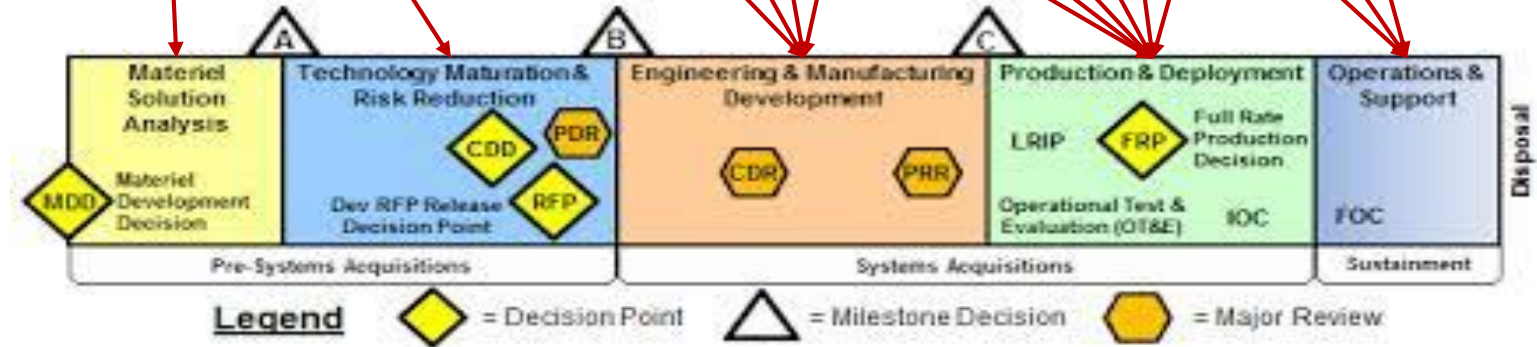
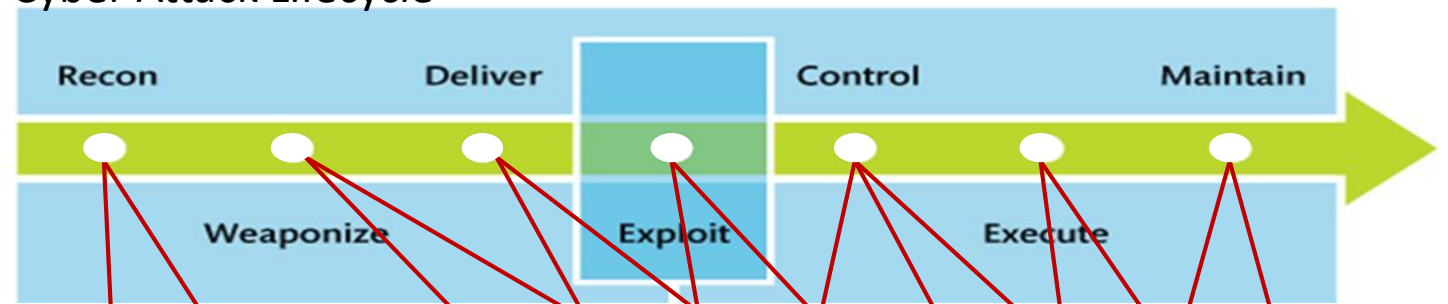
Adversary Goals:

- Acquire information
- Develop tools
- Deliver attack
- Initiate exploit
- Control attack
- Execute main attack
- Maintain presence

Defender Goals (relative to Operations and Support):

- Reduce attacks
- Limit attacks that can't be eliminated
- Gain and share information about attacks

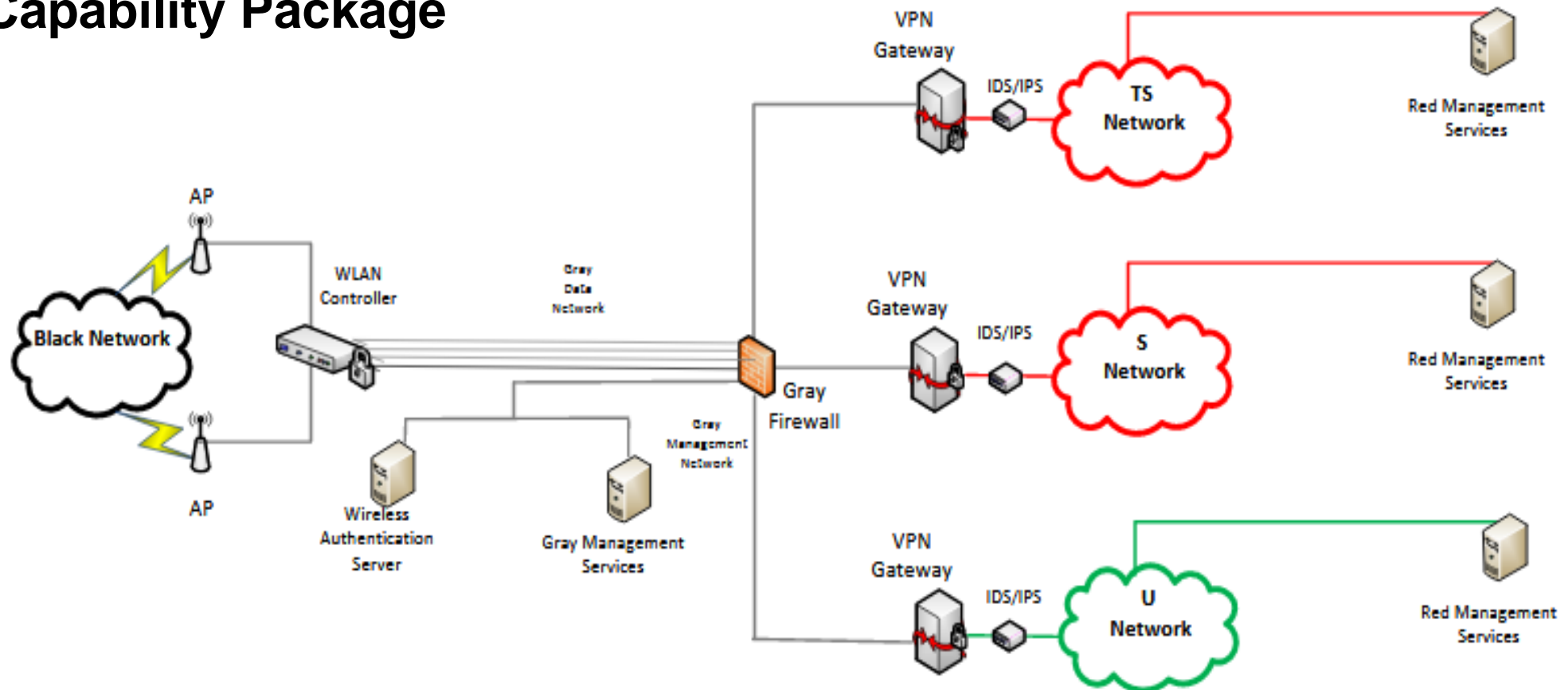
Cyber Attack Lifecycle



Acquisition Lifecycle

Example: Adversary Attack on WLAN Supply Chain

- Architecture based on Campus Wireless Local Area Network (WLAN) CSfC Capability Package



Adversaries have multiple opportunities to attack acquisitions

■ Materiel Solution Analysis and Technology Development

- Modify WLAN ICD/CDD, requirements (e.g., KPPs, KSAs)
- Reconnoiter potential capabilities, risk decisions
- Influence acquisition strategy

■ Engineering & Manufacturing Development

- Modify system, hardware designs
- Implant, modify code
- Modify technical, operational requirements
- Impair validity tests

■ Production and Development

- Implant, modify code
- Introduce counterfeit components

■ Operations & Support

- Implant, modify code
- Modify configurations

Mission Impacts

- Weaker Security
- Reduced Robustness
- Degraded WLAN Service
- Loss of User Confidence
- Increased Data Exfiltration Risk

Most Effective Phases to Apply Cyber Resiliency

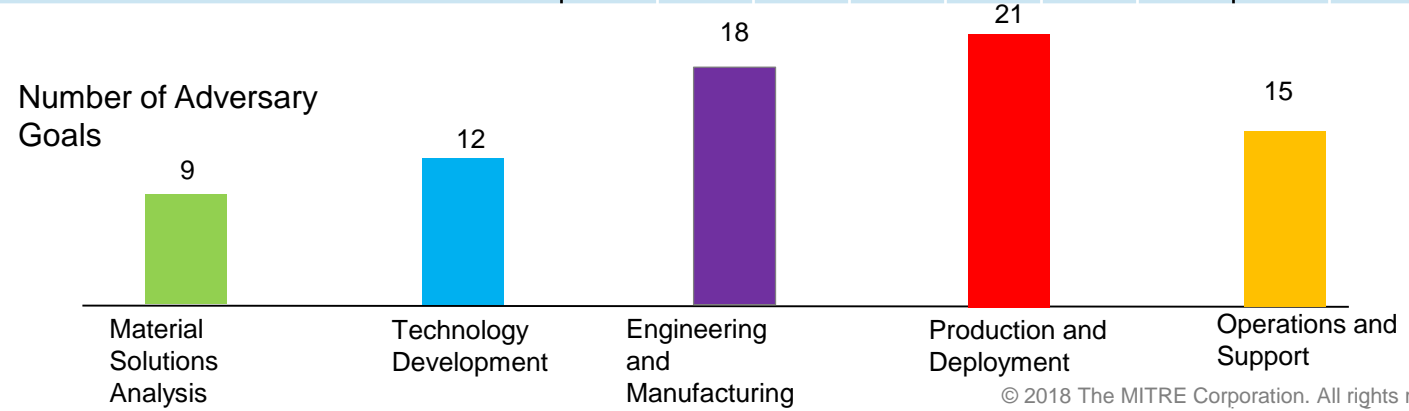
- ***Production & Deployment*** phase is associated with the most adversary Goals
- ***Engineering & Manufacturing Development and Production and Deployment*** phases
 - Product Development and Definition
 - “biggest bang for the buck”
 - Non-operational environments → more flexibility in mitigation deployment
 - Best opportunity for defenders to apply resiliency techniques and approaches
 - Largest impact to adversary goals
 - Best chance to achieve defender goals
- **Supply chain threat mitigations in O&S are a double-edged sword: mitigations enhance operational resilience, but can add additional complexity**

Non Persistence throughout the Acquisition Lifecycle (1 of 2)

Acquisition Lifecycle	Resiliency Mitigation: Non-Persistence	Adversary Goals (per the CAL)						Defender Goals in O&S				
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info	Recover
Materiel Solutions Analysis	Information – Reduce availability of information	x							x	x		
	Services – Reduce the chance of corrupted services in order to gain information	x							x	x		
	Connectivity – reduce the means to get the information	x							x	x		
Technology Development	Information – limit the time the information is available	x							x	x		x
	Services – limit the amount of time the adversary can exploit a service	x							x	x		x
	Connectivity – limit the amount of time paths into the environment are available	x							x	x		x
Engineering and Manufacturing	Information – limit ability to deliver an attack, decrease exploit success rate & reduce the adversary’s ability to control malware	x		x	x	x			x	x		
	Services – limit ability to deliver an attack, decrease exploit success rate & reduce the adversary’s ability to control malware	x		x	x	x			x	x		
	Connectivity – limit ability to deliver an attack, decrease exploit success rate & reduce the adversary’s ability to control malware	x		x	x	x			x	x		

Non Persistence throughout the Acquisition Lifecycle (2 of 2)

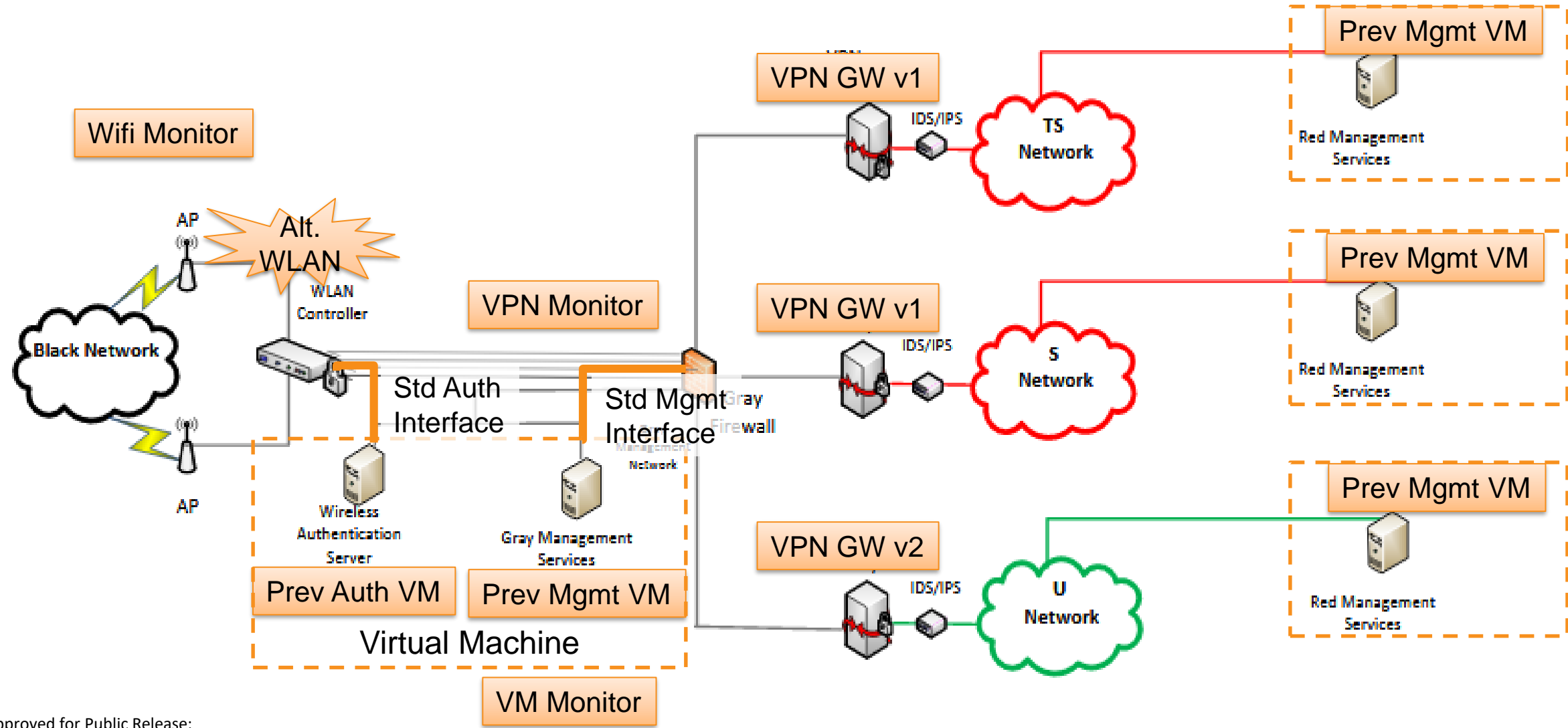
Acquisition Lifecycle	Resiliency Mitigation: Non-Persistence	Adversary Goals (per the CAL)						Defender Goals in O&S			
		Acquire Info	Develop tools	Deliver Attack	Initial Exploit	Controlling attack	Executing Attack	Maintain Presence	Reduce attacks	Limit attack	Gain/Share Info
Production and Deployment	Information – limit the adversary’s presence from delivery through maintenance			X	X	X	X	X	X		
	Services – limit the adversary’s presence from delivery through maintenance			X	X	X	X	X	X		
	Connectivity – limit the adversary’s presence from delivery through maintenance			X	X	X	X	X	X		
Operations and support	Information – limit the adversary’s presence throughout the CAL					X	X	X	X	X	X
	Services – limit the adversary’s presence throughout the CAL					X	X	X	X	X	
	Connectivity – limit the adversary’s presence throughout the CAL					X	X	X	X	X	



Guidance for Applying Cyber Resiliency

- **Identify effective mitigations by “thinking backwards”**
 - Start with the “as-is” or “to-be” mission system
 - Working in reverse through the Acquisitions Lifecycle phases
 - For each phase, answer the following questions
- **Q1 What are the likely impacts of a successful supply chain attack to the identified critical assets?**
- **Q2 How can you tell if the supply chain is attacked or compromised?**
 - Authenticity, verification testing
 - Baseline and trend monitoring can identify counterfeit and potential compromise
- **Q3 How will you recover from the attack or compromise?**
 - The earlier in the acquisition the attack took place, the harder it is to recover
 - Agile, segmented design and virtualization allows for quick replacement
 - Supporting technology standards allows for easier product replacement

Mitigating WLAN CP Supply Chain Threats



Applying Resilience Against Supply Chain Threats

Resilient Acquisitions

- Use access-controlled “gold master” images for designs, documents, and software
- Limit the connectivity to, duration of, and information stored on user’s machines
- Design around industry standards
- Design and build in ways for verification testing
- Compartmentalize acquisitions insight and knowledge
- Substantiate provenance with each transfer of stewardship

Resilient Operations

- Validation & verification testing of updates and new components
- Enable efficient rollback to previous versions: swappable WLAN Controllers, Versioned VMs
- Maintain list of alternate supply chain products and providers: WLAN Controller, VPN Gateways
- Monitor behavior: wireless RF, VPN, VM
- Segment management and data channels to minimize visibility
- Consider alternative ways to prevent/detect instead of patching vulnerabilities (e.g., CDS, IDS)

Findings

- **During operations, Cyber Attacks and Supply Chain attacks are not easily differentiated. However:**
 - For Supply Chain attacks pre-exploit actions (weaponize and deliver) happen in early acquisition phases
 - This early established presence is difficult to detect at perimeter
- **Resiliency mitigations can be applied for all assets across all acquisition phases**
- **Best when “built in” early in acquisition**
- **Best Phases are Engineering and Manufacturing Development and Production and Deployment**
 - More Flexibility
 - Less Complexity
 - As compared to O&S
 - Provenance and integrity validation can be designed in
 - Most mitigations in these phases also mitigate supply chain threats during O&S

Cyber Resiliency Resources

- **NIST SP 800-160 Volume 2, Initial Public Draft – Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems.**

<https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf>

- ***Supply Chain Attacks and Resiliency Mitigations***

<https://www.mitre.org/publications/technical-papers/supply-chain-attacks-and-resiliency-mitigations>

Questions ?

Cyber Resiliency Resources

Get a sense of the area

- **Cyber Resiliency FAQ (2017)**
https://www.mitre.org/sites/default/files/PR_17-1434.pdf
- **Cyber Resiliency Resource List (2016)**
<http://www2.mitre.org/public/sr/Cyber-Resiliency-Resources-16-1467.pdf>
- **Industry Perspectives (2015)**
<http://www2.mitre.org/public/industry-perspective/>

Situate in terms of cyber preparedness

- **Short summary (2017)**
<https://www.mitre.org/sites/default/files/publications/15-0797-cyber-prep-2-motivating-organizational-cyber-strategies.pdf>
- **Extended version (2017)**
<https://www.mitre.org/sites/default/files/publications/16-0939-motivating-organizational-cyber-strategies.pdf>

Cyber Resiliency Resources

Start with the most recent resources

- **Cyber Resiliency Design Principles (2017)**
<https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MT-R17001.pdf>
- **Structured Cyber Resiliency Analysis Methodology (2016)**
<https://www.mitre.org/sites/default/files/publications/pr-16-0777-structured-cyber-resiliency-analysis-methodology-overview.pdf>
- **Cyber Resiliency Engineering Aid (2015)**
<http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf>

Augment with resources which answer specific questions

- **Cyber Resiliency Metrics: Key Observations (2016)**
<https://www.mitre.org/sites/default/files/publications/pr-16-0779-cyber-resiliency-metrics-key-observations.pdf>
- **The Risk Management Framework and Cyber Resiliency (2016)**
<https://www.mitre.org/sites/default/files/publications/pr-16-0776-cyber-resiliency-and-the-risk-management-framework.pdf>
- **Cyber Resiliency Controls in NIST SP 800-53R4 (2016, in 2nd Public Draft of NIST SP 800-160)**
http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf
- **Resiliency Mitigations in Virtualized and Cloud Environments (2016)**
<https://www.mitre.org/sites/default/files/publications/pr-16-3043-virtual-machine-attacks-and-cyber-resiliency.pdf>
- **A Measurable Definition of Resiliency Using “Mission Risk” as a Metric (2014)**
<https://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf>