Considerations for Improving Cyber Resilience and Security

Dr. Bob Mills
Professor of Electrical Engineering

Maj Logan Mailloux, PhD
Asst Professor of Systems Engineering

Air Force Institute of Technology

June 2017
Perspectives Matter

The AFIT of Today is the Air Force of Tomorrow.

Hackers briefly took down the website of the CIA yesterday...

What people hear: Someone hacked into the computers of the CIA!!

What computer experts hear: Someone tore down a poster hung up by the CIA!!
Cyber “Attacks” on the Rise
Cyber-Physical Systems

The AFIT of Today is the Air Force of Tomorrow.

- Devices that perform physical functions in the real world… but are interconnected
  - Actuators, sensors, motors, control surfaces, pumps, switches, indicators, etc.
  - Critical infrastructure: power grid, water/sewage treatment, air traffic control, HVAC, etc.
  - Planes, trains and automobiles …
  - Operational Technology (OT) vs traditional IT

- Attacks/failures can have physical consequences
The AFIT of Today is the Air Force of Tomorrow.

- Machine-to-machine communications bring new opportunities for automation: Commerce, Smart Home, Telematics, Wearables, Entertainment

http://www.wordstream.com/blog/ws/2015/01/09/the-internet-of-things
IoT Benefits and Risks

The AFIT of Today is the Air Force of Tomorrow.

http://arstechnica.com/

http://www.pubnub.com
How to Break the Internet

On 21 Oct 2016, dyn.com attacked by massive distributed denial of service

- DNS – domain name service – maps domain names to machine readable internet protocol (IP) addresses
- Example: www.google.com → 216.58.216.100
- DDoS worked by sending large volumes of DNS queries for popular websites serviced by dyn.com
- Netflix, Amazon, Twitter, Spotify, Reddit, etc.

Botnets created by compromising unsecured IoT devices

- Mirai malware attacked unsecured IoT devices – IP cameras, home routers… internet-connected embedded systems
- Out of date Linux OS … embedded systems typically do not have good mechanism for updating software and maintaining security!
Embedded Systems

The AFIT of Today is the Air Force of Tomorrow.

• Characteristics:
  • Highly efficient … optimized for specific application or function
  • Often have strict real time operation constraints
  • Interact with external/physical world via sensors & actuators
  • Usually have minimal or no user interface
  • Often not maintained or updated in same way as traditional IT (patching, security updates, bug tracking, etc.)

• Implications for security:
  • Overall system is a collection of components from different manufacturers
  • Status of software in embedded systems may be unknown – may be proprietary and/or not well-maintained and updated
  • Undesirable emergent behaviors

• Bottom line: difficult if not impossible for the system integrator to fully know what is inside the final product
Hacking a Car

The AFIT of Today is the Air Force of Tomorrow.

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

Problem solved....??

Business Standard
Jeep Hack Forces Fiat Chrysler to Recall 1.4 Million Cars.

Nabeel Khan | Japur
July 27, 2015 Last Updated at 13:52 IST
Hacking a Car

The AFIT of Today is the Air Force of Tomorrow.

Vehicle to Vehicle Communication

Engine Control Unit

Transmission Control Unit

Body Controller

Locks/Lights/Etc

Radio

TPMS

Antilock Braking System

OBD-II

Anti-Theft

Telematics

Keyless Entry

HVAC

Internet/PSTN

Bluetooth

Wi-Fi

Checkoway et al., 2010

Does this look familiar???
Threats to Avionics Systems

The AFIT of Today is the Air Force of Tomorrow.

How Iran Hacked Super-Secret CIA Stealth Drone
RT, December 15, 2011

New Hack Could Literally Move a Plane in Flight
VentureBeat, July 28, 2012

How to Hack Into a Boeing 787
Fox News, February 20, 2008

Cyberattack grounds planes in Poland

Chinese Military Suspected in Hacker Attacks on U.S. Satellites
Bloomberg Business Week, October 27, 2011

Hackers Secure F-35 Fighter Plans
ISS Source, January 1, 2013

HackInTheBox, April 10, 2013
What’s the Threat?

The AFIT of Today is the Air Force of Tomorrow.

2013 DSB Report on Resilient Military Systems and the Advanced Cyber Threat

- **Layers**
  - Tiers V-VI: $Bs
  - Tiers III-IV: $Ms
  - Tiers I-II: $10s

- **Threat Levels**
  - Nuisance
  - Discovers unknown vulnerabilities
  - Creates vulnerabilities using full spectrum
  - Exploits pre-existing known vulnerabilities
  - Existential

---

**Iranian hackers compromised airlines, airports, critical infrastructure firms**

---

**Chinese PLA Soldiers “Mastermind Cyber-Espionage Cold War”**

The Register, February 19, 2013

---

**NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history”**

---

**Russia hacks into Ukraine power grids a sign of things to come for U.S.?**

---

**China’s Military Behind Hacking Attacks in U.S.**


---

An Iranian cyberattack dubbed Operation Cleaver compromised more than 50 organizations worldwide, researchers said.
Cybersecurity

Biggest source of DOD’s cyber threats: inept co-workers

By Kevin McCaney | Mar 28, 2014

Defense Department IT professionals are nearly as concerned about internal threats as they are external hacking of their networks — and most concerned about careless or poorly trained insiders as a source of threats, according to a recent survey by SolarWinds, an IT management software provider.

Careless / untrained users

Malicious insiders
We’re Doing it to Ourselves

The AFIT of Today is the Air Force of Tomorrow.

Is Ted really inept…

Or is he just a victim of a poorly designed system?
Anything that depends on software is hackable

Let’s assume that all our systems will be compromised

Some tech improvements coming along…but no silver bullets

Need to work towards a mission assurance mindset
The AFIT of Today is the Air Force of Tomorrow.

Issues

- Wicked problems
- S/W dependence & system complexity
- Security as a non-functional requirement
- Expensive to fix
- How to validate and measure security and resilience?
- Emergent behaviors & unintended consequences

Acquisition process
The AFIT of Today is the Air Force of Tomorrow.

Different Perspectives

Operations *of* Cyberspace
(Construct)

- *Construct* the Domain
- Build, maintain, support
- Operate and maintain networks
- Allocate bandwidth
- Passive defenses and security
- Information Assurance

Operations *through* Cyberspace
(Use)

- Logistics / TPFDD
- RPA/RPVs
- Influence Ops
- ATO processing
- Air Battle Mgmt
- ISR
- etc...

Operations *in* Cyberspace
(Control)

- Create effects
- Attack, Defend, Exploit
- Hold adversary capabilities at risk
- Protect our own ability to operate
Different Perspectives

The AFIT of Today is the Air Force of Tomorrow.

Engineers, system developers, system SMEs

1. System Susceptibility
   - Vulnerabilities

2. Threat Accessibility
   - Logical and Physical Reachability
   - Tools
   - Techniques

3. Threat Capability
   - Resources

Value to Attacker

Successful Attack

Cyber operators: monitor, attack, defend, protect

Intelligence: adversary capabilities and intent, I&W, R&D
Different Perspectives

The AFIT of Today is the Air Force of Tomorrow.

- Traditional IT communities focus on defense in depth, **compliance and security**
- Acquisition communities focus on how to build adaptable and **resilient systems**
- Operational communities focus on **detection, response and maneuver**

Who’s making the risk decisions at each level? Are they the best ones?
Different Kinds of “Defense”

The AFIT of Today is the Air Force of Tomorrow.

- How do I find and defeat a sophisticated maneuvering adversary?
- How do I make it difficult for an enemy to stay?
- How do I make it difficult for an enemy to achieve objectives?
- How do I get my mission done while under attack?
- How do I make it difficult for the enemy to get access?
- How do I make it hard to successfully attack my systems?
The Systems Security Problem

For the last ~20 years, we have been embedding IT or “Cyber” into nearly all core business processes, mission systems, and weapon systems

- **Increases** operational efficiency and decision quality
- **Decreases** confidence that systems will function as intended

The Systems Security Problem

• For the last ~20 years, we have been embedding IT or “Cyber” into nearly all core business processes, mission systems, and weapon systems
  • **Increases** operational efficiency and decision quality
  • **Decreases** confidence that systems will function as intended

What is the Actual “Requirement” for Security?

Confidentiality: is the info/data safe from prying eyes?
If not, what could be done with the info?

Integrity: is the info/data safe unauthorized manipulation?
How do we know? Can we trust it?

Availability: is the system/info available for use, even though it might have been compromised?

Tradational IT systems generally focus on confidentiality & integrity.
Cyber physical systems traditionally focus more on availability and safety.
Embedded systems often overlook security entirely.

Bottom line issue – how do we write “security” as an acquisition requirement that a contractor can build towards?
Security & Resiliency Metrics

• We want our weapon systems to be “more resilient”

• What does that mean, exactly?
• How do we measure resiliency?
• Are we doing better now than we were 5-10 years ago?
• Will what we’re doing now make it better in 5-10 years?
• How do we know?
• How much will it cost?
• What do we have to give up in functionality?
Inconsistent Terminology

Words mean things, but we often talk past each other

- Functionality … reliability … resilience … robustness … survivable … safety … security … hardened … sustainability … fault tolerance … assurance … ?

- What do these terms all mean, and how do they relate?

- Note that people are still arguing about what exactly “cyber” means!
Examples

Safety: reduce/avoid inherent dangers in the environment

Security: information and critical system functions are protected against unauthorized access/use (external focus)

Hardening: vulnerability surface is reduced via technical and policy control mechanisms

Stability: system maintains its integrity when subjected to a disturbance (think control systems theory)

Reliability: minimize chance of random failures (e.g., MTBF)

Survivability: degrades gracefully and does not fail catastrophically

Resilience: system is able to recover and get better over time
Why Does it Matter?

The AFIT of Today is the Air Force of Tomorrow.

- Concepts are related, but are not equivalent – different levels of assurance
- Hardened systems are harder to break in the first place… but this doesn’t imply resilience
- Unsecured systems may be driven into an unstable state, which may then result in a safety issue
- Survivable systems will keep operating, but they won’t necessarily get better with time
- Concepts may be related – e.g., an unreliable system may result in unsafe situations
- Resilience only has meaning in the context of what the system is supposed to do
Software Dependence

The AFIT of Today is the Air Force of Tomorrow.

S/W: 0% (of $50K)

95% of $104M

a computer that

thinks it’s a fighter

5% (of $2.4M)
Software Complexity

- Programmers make ~ 10-50 errors per 1000 lines of code
- Careful ones can cut down to 0.5 per 1000, but that’s still a lot of bugs
- All that’s needed is for the system to execute a few commands that we don’t want
Testing and Validation

• We typically test to functionality requirements
  • Relatively easy to do, but we typically only spot check certain things

• Testing for reliability
  • Requires more effort … must stress the system and ensure it still continues to operate
  • Focuses on specific conditions and stated behavior … test the things we care most about (often safety)
  • Ignores “other” functions that may be security issues (e.g., back doors)

• Testing for security & resilience
  • We don’t build provably secure systems
  • Red teaming and penetration testing only catch certain aspects of the overall search space
  • Absence of a problem doesn’t prove there isn’t a problem
The AFIT of Today is the Air Force of Tomorrow.

- “We need to *bake-in* rather than *bolt-on*” … but how???

- Focus on mission assurance … what has to work on “the worst day of the Air Force?”

- System design is too late – need to start with operational concept

- Also need to think outside the system/subsystem boundary

![Table](image_url)

<table>
<thead>
<tr>
<th></th>
<th>Traditional IT</th>
<th>Operational Technology</th>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission-Level</td>
<td>1</td>
<td>4</td>
<td>7</td>
</tr>
<tr>
<td>System-level</td>
<td>2</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>Component-level</td>
<td>3</td>
<td>6</td>
<td>9</td>
</tr>
</tbody>
</table>
Mission Assurance Example

1. Target Acquired
2. Information Communications Technology transmits data
3. Commander at distant center observes
4. Mission Commander Loses surveillance and aborts
5. SOF team aborts mission
6. Attempt to determine cause

Based on Vautrinot, 2012 (Strategic Studies Quarterly), and W.E. Young (MIT, USAF)
Need to Address Security & Assurance Early in Concept Phase

The AFIT of Today is the Air Force of Tomorrow.

We need to focus more here

Where we tend to focus a lot of effort

Problem Analysis & Concept Development

Secure System Development

Bolt-on Security Hardening

Solution Development & Implementation

Mission Failure Attack Response

Cost to Fix vs. Effectiveness of Fix:
- Low Cost to Fix: Secure System Development
- High Cost to Fix: Bolt-on Security Hardening

We need to focus more here.
Designing for Mission Assurance

The AFIT of Today is the Air Force of Tomorrow.

- Capabilities for operators to be aware of different and changing adversarial strategies as well as environmental and system conditions
- Options & alternatives to accomplish mission under different circumstances
- Tools to assess advantages and risks of available response options and alternatives
- Ability to transition to a selected option while simultaneously continuing the mission

- Systems engineering for MA extends across entire traditional acquisition life cycle
System Resiliency Framework

The AFIT of Today is the Air Force of Tomorrow.

Systems Security Engineering — A Foundation for System Resiliency
The application of basic security design principles and concepts within life cycle-based systems engineering processes can achieve adequate security and resiliency—both emergent properties of a system that contribute to its trustworthiness.

GOALS
- ANTICIPATE
- WITHSTAND
- RECOVER
- EVOLVE

OBJECTIVES
- UNDERSTAND
- PREPARE
- PREVENT/AVOID
- CONTINUE
- CONSTRAIN
- RECONSTITUTE
- TRANSFORM
- RE-ARCHITECT

TECHNIQUES
- ADAPTIVE RESPONSE
- ANALYTIC MONITORING
- DECEPTION
- DIVERSITY
- DYNAMIC POSITIONING
- NON-PERSISTENCE
- PRIVILEGE RESTRICTION
- SEGMENTATION/ISOLATION
- COORDINATED DEFENSE
- DYNAMIC REPRESENTATION
- REALIGNMENT
- REDUNDANCY
- SUBSTANTIATED INTEGRITY
- UNPREDICTABILITY
Some Really Hard Questions

The AFIT of Today is the Air Force of Tomorrow.

• How do we get past the cliché saying *baked in vs bolted on*?
  • How do we write better system specs to address security concerns?
  • How to incentivize developers to emphasize security?
  • Addressing security during system design is too late… need to address it during initial concept phase

• *Balancing (?)* operational capability and security / mission assurance requirements
  • Know/understand all mission parameters – how will system be used?
  • Ensure functionality justifies added security risks
  • How do we measure security, resilience and mission assurance considerations?

• How do we ensure that T&E processes accurately capture what is important to mission assurance?
  • Ensure negative testing is part of the T&E process… is that enough?
We Can Solve This
(We Have to Solve This)

The AFIT of Today is the Air Force of Tomorrow.

• Just because it’s cyber doesn’t mean it’s a completely new challenge
  • Attack problem with systems engineering and all aspects of DOTMLPF-P

• Cyberspace is a constructed domain … it will only do what we allow when we build and connect things
There I was, stuck in a Chinese firewall, when suddenly our router lit up like the Fourth of July... Bots to the left of me, Trojans to the right... We lost some good servers that day.

Future War Stories