Achieving Defendable Architectures via Threat-Driven Methodologies

Michael Muckin  
LM Fellow, Cyber Architect  
Lockheed Martin

Scott Fitch  
LM Fellow, Cyber Architect  
Lockheed Martin
The system shall encrypt data at rest.

Why?
The Threat Driven Approach

System Threat Analysis + Threat Intelligence
Threat Intelligence

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Actions on Objectives

Synthesis
Analysis
Synthesis
Analysis
Synthesis
Analysis
Synthesis
Analysis
Synthesis
Analysis
System Threat Analysis Methodology

There are no IDDIL (idle) Threats; they ATC (attack)

- Identify the Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors

Discovery Phase

Analysis and Assessment

Triage

Controls

Implementation Phase
System Threat Analysis Methodology

Mission Needs

- Critical Assets
- Knowledge of Industry
- Mission Impacts

System Threat Analysis

- Identify the Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors
- Analysis and Assessment
- Triage
- Controls

Threat Intelligence

- Targeted Assets
- Tactics, Techniques, & Procedures
- Campaigns, Motivation, Skill
- Inputs on likelihood
- Control Effectiveness

Mission Needs:
- Critical Assets
- Knowledge of Industry
- Mission Impacts
Threat Methodology Integration

Threat Modeling & Analysis

IDDIL

ATC

Concept → Reqs → Design → Build → Test/QA → Deploy → Ops

Testing Aligned to Threat Model

Threat Actors, TTPs, Existing Controls

Infrastructure & Service Enhancements

Current TTPs and Targeting Intel

Threat Intelligence
Threat Methodology Practices

- Threat Models
- Attack Trees
- Threat Profiles
- Cyber Kill Chain®
- Controls Effectiveness Matrix
Case Study

Assets:
- Smart Card
- OS and Applet
- ID codes
- Keys
- I&AM Systems
- Workstations
- Facilities

Threat Actors/Attack Vectors:
1. Man-in-Manufacturer (a)
2. Man-in-Manufacturer (b)
3. Interception of Master Key
4. Compromise of I&AM System
5. Malicious Insider
6. Compromise Critical Role
7. Compromise middleware
8. Physical attacks
Determining Focus Threats

System Threats
- Physical Attacks
- Malicious Code on Card
- Compromised Middleware
- Lateral Movement
- Disclosure of Keys
- Critical Role Exploited
- Malicious Insider

Focus Threats
- Threat Intelligence
- Adversary Objectives
- TTPs

Mission and Business Needs
# Addressing Threats

<table>
<thead>
<tr>
<th>Asset/ Objective</th>
<th>Threat Types</th>
<th>Resultant Condition(s)</th>
<th>Attack Surface/ Vector</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmartCard OS</td>
<td>• Tampering</td>
<td>Dependent upon # of cards and level of access of user</td>
<td>• Card</td>
<td>• Code Audits</td>
</tr>
<tr>
<td></td>
<td>• Disclosure</td>
<td></td>
<td>• Card OS code</td>
<td>• Contract language</td>
</tr>
<tr>
<td></td>
<td>• Elevation of Privilege</td>
<td></td>
<td>• APDU manipulation</td>
<td>• Privileged account restrictions</td>
</tr>
<tr>
<td></td>
<td>• Lateral Movement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Role</td>
<td>• Spoofing</td>
<td>Unauthorized, privileged and potentially untraceable activity to critical infrastructure</td>
<td>• I&amp;AM Systems</td>
<td>• Admin gateways</td>
</tr>
<tr>
<td></td>
<td>• Repudiation</td>
<td></td>
<td>• Specific interfaces</td>
<td>• Multi-factor AuthN</td>
</tr>
<tr>
<td></td>
<td>• Elevation of Privilege</td>
<td></td>
<td>• Specific services</td>
<td>• Local accounts wherever possible</td>
</tr>
<tr>
<td></td>
<td>• Lateral Movement</td>
<td></td>
<td>• Targeted user and service accounts</td>
<td>• Privileged account password controls</td>
</tr>
<tr>
<td>Workstation</td>
<td>• Disclosure</td>
<td>Exfil data and/or credentials; Use machine as foothold for further actions</td>
<td>• SmartCard</td>
<td>• System patching</td>
</tr>
<tr>
<td></td>
<td>• Elevation of Privilege</td>
<td></td>
<td>• Middleware</td>
<td>• HIPS</td>
</tr>
<tr>
<td></td>
<td>• Lateral Movement</td>
<td></td>
<td>• Memory</td>
<td>• Memory protections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Penetration testing / assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Configuration controls</td>
</tr>
</tbody>
</table>
Defend the System as a Whole

- **Visibility** into current and historical system activity
- **Manageability** of system configuration, updates, and control settings
- **Survivability** to deliver services through attack, detection, and recovery
Designing for Defense

Visibility
- Server logging
- Workstation logging
- Network monitoring
- Cardstock inventory
- Insider detection
Designing for Defense

Visibility

- Rules based on new threat intel
- Control points for tactical mitigations
- System patching
- Controlled admin access

Manageability

- Rules based on new threat intel
- Control points for tactical mitigations
- System patching
- Controlled admin access
Designing for Defense

Visibility
Manageability
Survivability

- System segmentation
- Strong admin authentication
- Separate card use from issuance
- Assured system recovery
System Threat Analysis + Threat Intelligence

Use IDDIL/ATC to select *protection* and appropriate compensating controls
Design the system to be *defended* through *visibility*, *manageability*, and *survivability*
Building Defendable Architectures and Applying Threat-Driven Methodologies

Start identifying your organization’s critical systems and assets

For the next system you build, modify, operate, or assess

Use IDDIL/ATC to select protection and appropriate compensating controls
Design the system to be defended through visibility, manageability, and survivability

As your cyber defense capabilities mature

Integrate threat intelligence into design, development, and operations
http://lockheedmartin.com/cyber