Cyber Resilience-in-Depth™ solutions

baesystems.com/cyberresilience
Cyber framework.

Platform cyber attack framework

The platform cyber attack framework (PCAF) provides a repository of adversarial attack knowledge used to guide system architects and developers while creating Resilience-in-Depth™ platform solutions. The PCAF repository includes threat intelligence, threat actor specifications, and attack vector models described using model-based engineering techniques. Relevant threats and attacks are extracted from the PCAF to produce specific platform cyber attack models (PCAMs), allowing visualization and understanding of the attack surface. Figure 1 shows an example of a PCAM integrating cyber-attacks across five levels-of-scale for a fictitious military platform. The PCAF promotes the use of “offensive knowledge to solve defensive problems” throughout the product development life cycle.

Platform cyber defense framework

With an understanding of platform cyber-attack, the corresponding platform cyber defense framework (PCDF) identifies related defense and resilience controls leading to a Resilience-in-Depth solution. The PCDF is a repository of cyber defense and cyber resilience techniques linked to relevant attack vectors for military platforms. PCDF allows rapid selection of specific defensive controls for embedded cyber systems and platforms to develop platform cyber defense models (PCDM). Figure 2 shows an example of a PCDM identifying resiliency controls needed to respond to and recover from the cyber-attacks identified in the corresponding PCAM. Together, the PCAM and PCDM models balance knowledge of cyber-attacks and resilience controls needed to develop and deliver Resilience-in-Depth solutions for operational platforms.
Chip-level attacks
IC reverse engineering allows mapping and analysis of integrated circuit (IC) designs; extraction of internal ROM programming; extraction of cryptographic materials
Fault induction rapid writing of memory cells to IP bits in adjacent cells; row-hammer attack
Side-channel analysis timing, power, thermal, and radio frequency emissions allow side-channel attacks on embedded application programming and cryptography; password brute-forcing
Silicon malware backdoors, kill switches, and trojans (intended and unintended) built into the silicon level of an IC

Board-level attacks
PCB reverse engineering allows mapping and analysis of printed circuit boards (PCBs) designs; loss of intellectual property and trade secrets
Embedded OS and applications attacks on the embedded software applications (Linux, RTOS, drivers, embedded software)
Bus intrusion reading/writing bus signals (I2C/SPI, ..) to disclose information, reconfigure devices, change execution flow and insert malware
Hardware implants insertion of malicious circuits to alter/control the host hardware environment

Assembly-level attacks
Backplane intrusion reading/writing backplane signals used for cross-board communication to disclose information, reconfigure devices, change execution flow and insert malware
Malicious/vulnerable boards tampering or compromising less secure boards to access highly secure boards

Firmware/software glitching uses partial clock cycles, power faults, RF fault injection, and laser fault injection to alter execution of embedded programming, allows bypass of firmware security functions

Fault induction rapid writing of memory cells to IP bits in adjacent cells; row-hammer attack
Side-channel analysis timing, power, thermal, and radio frequency emissions allow side-channel attacks on embedded application programming and cryptography; password brute-forcing
Silicon malware backdoors, kill switches, and trojans (intended and unintended) built into the silicon level of an IC

Assembly-level attacks
Backplane intrusion reading/writing backplane signals used for cross-board communication to disclose information, reconfigure devices, change execution flow and insert malware
Malicious/vulnerable boards tampering or compromising less secure boards to access highly secure boards

Bus-level attacks
External message manipulation message data bridged across gateways allow message sniffing, replay and injection
Actuator data manipulation tampering with actuation data allows attackers to set LRU/ECU state and response
Bus man-in-the-middle (MITM) rogue devices split the bus into two physical buses and modifies message traffic infight
Sensor data manipulation tampering with sensor data allows attackers to set LRU/ECU state and response

Platform attacks
Vehicle-to-infrastructure (V2I) network connectivity provides local and remote access to vehicular systems and services
Vehicle-to-vehicle (V2V) compromised vehicles provide a platform for moving laterally in a trust relationship
Radio frequency apertures network connectivity over radio carrier provides remote access to vehicular systems or presentation of false data (e.g., spoofed GPS)
Open data ports allow transport of applications and data to on-board computing systems without checking access permissions or performing data sanitization
Malicious insider changes the configuration of equipment and/or software to compromise the platform
Supply chain poisoning (intentional and unintentional) provides local and remote backdoors through compromised hardware, software and firmware
Open test ports that do not support device authentication provide open access to attackers
Malicious maintenance equipment and test stands provide a pre-authenticated connection to sensitive functions on the platform

NOTE: This is a fictitious vehicle. Any resemblance to a real world military vehicle is unintended and is purely coincidental.
### Platform cyber defense model (PCDM)

**Figure 2**

#### Resilience pillar

<table>
<thead>
<tr>
<th>Prepare</th>
<th>Prevent</th>
<th>Detect</th>
<th>Respond</th>
<th>Recover</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Attack vectors

**Chip-level**

- k-reverse engineering
- decompilation
- Side-channel analysis
- Firmware/software glitching
- Fault Induction

**Board-level**

- PCB reverse engineering
- Embedded OS and applications
- Bus intrusion
- Test-point intrusion
- Hardware implants

**Assembly-level**

- Cross-board trust relationships
- Maliciousovaluable boards
- Unsecured data storage
- Embedded behavior

**Bus-level**

- External message manipulation
- Actuator data manipulation
- Bus man-in-the-middle (MITM)
- Bus man-in-the-middle (Modem)

**Platform-level**

- Vehicle-to-infrastructure (V2I)
- Vehicle-to-vehicle (V2V)
- RF communication network
- Open data ports
- Malicious insider
- Supply chain
- Hardened ports
- Malicious maintenance equipment

---

**Chip-level defensive technologies** provide protection at the IC level of design. These technologies are generally applied inside the supply chain and during the manufacturing process.

**Board-level defensive technologies** provide protection on the PCB by assuring trusted relationships and data flows across the PCB components. These technologies protect against malicious board implants, sensitive data disclosure, and data bus tampering.

**Assembly-level defensive technologies** ensure that board-to-board interaction in the LRU/ECU assembly is trusted and secure. These technologies protect against malicious implants, sensitive data disclosure, and data bus tampering between an assembly’s subsystems.

**Bus-level defensive technologies** protect devices connected to internal platform data buses (e.g., CAN Bus, MIL-STD-1553, FlexRay, Ethernet). These technologies protect against malicious implants and rogue assemblies that may attempt message sniffing, replay, injection and spoofing attacks.

**Platform-level defensive technologies** provide protection for V2I and V2V operations. These technologies protect against on-board attack vectors having physical and electronic access to the platform and generally cross the traditional accreditation boundary.
BAE Systems is a global defense, aerospace and security company with more than 83,000 employees worldwide. The company delivers a full range of products and services for air, land and naval forces, as well as advanced electronics, security, information technology solutions and customer support and services.