BAE SYSTEMS

Cyber Resilience-in-Depth™ solutions

baesystems.com/cyberresilience

Detection, response, and recovery **where it counts**

Cyber frameworks

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 PCAM 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.

Platform cyber attack model (PCAM)

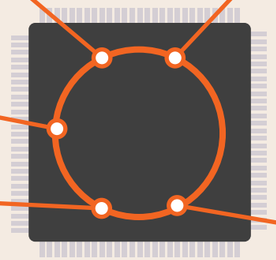
Figure 1

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



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 rmware security functions

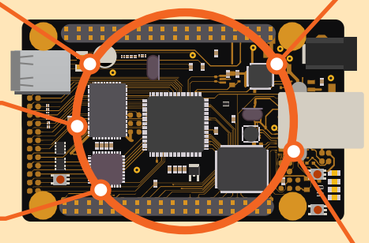
Silicon malware backdoors, kill switches, and trojans (intended and unintended) built into the silicon level of an IC

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



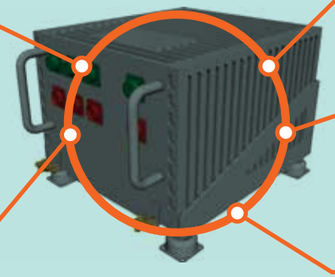
Test-point intrusion use of Universal asynchronous receiver/transmitter (UART), Joint test action group (JTAG) and other test-points to disclose information, reconfigure devices, change execution flow and insert malware

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



Cross-board trust relationships unauthenticated/implicit trust between boards

Unsecured data storage manipulation of local data stores to compromise data confidentiality and integrity

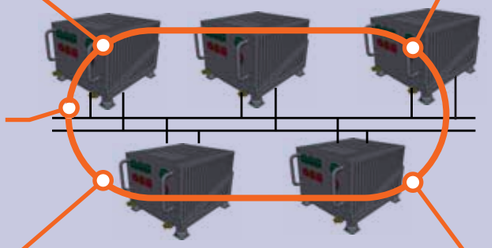
Embedded behavior exploitation of default line replaceable unit (LRU)/electronic control unit (ECU) behaviors (fault response, default configurations)

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



Bus man-on-the-middle (MOTM) rogue devices sit on the bus and sniff, modify, replay, and inject malicious message traffic

Sensor data manipulation tampering with sensor data allows attackers to set LRU/ECU state and response

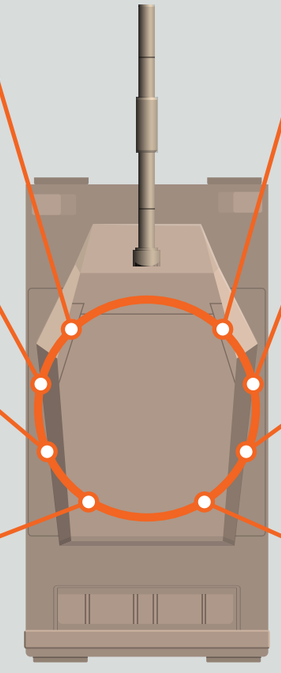
Platform attacks

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 conguration 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)

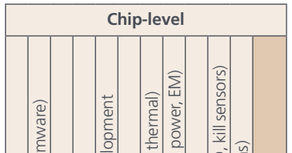
Figure 2

Defensive and resilience controls

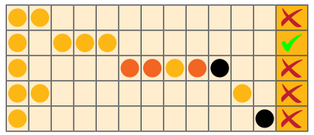
Resilience pillar	Chip-level	Board-level	Assembly-level	Bus-level	Platform-level
	Secure chip engineering	Secure PCB engineering	Host-based intrusion detection system (HIDS)	Intrusion Detection System (IDS)	Platform security center
	Anti-tamper (packaging, hardware, rmware)	PCB Anti-Tamper	Host-based intrusion prevention system (HIPS)	Intrusion Prevention System (IPS)	V2I trusted gateway
	Dynamic logic locking	Secure/trusted rmware (POST, BIOS, bootloader)	Cross-board authentication & authorization	Cross-assembly crypto key management	V2I dynamic trust management
	Silicon malware detection	Secure/trusted OS (Linux, RTOS)	Cross-board secure message transport	Cross-assembly secure key exchange	V2I crypto key management and exchange
	Fault tolerant rmware/software development	Secure/trusted applications (drivers, services, VF)	Cross-board cryptographic key management	Cross-assembly authentication & authorization	V2I encrypted data communication
	Power line filtering/noise generation	Cross-chip authentication & authorization	Cross-board cyrptographic key exchange	Cross-assembly secure message transport	V2I data communications
	Emission control (EM/RF, optical, and thermal)	Cross-chip encrypted data transport	Physical-level configuration change detection	Cross-assembly dynamic trust management	V2V trusted gateway
	Glitch detection and response (clock, power, EM)	Secure key storage	Protocol anomaly detection	Dynamic state snapshots and recovery	V2V dynamic trust management
	Induction tolerant design	Secure, over the board key distribution	Secure data storage technology	**RMF family of controls**	V2V crypto key management and exchange
	Advanced packaging technology (3D, kill sensors)	Data trace protections technologies	Data/configuration tampering detection		V2V encrypted data communication
	Active chip defense (DARPA programs)	PCB test-point hardening	Engineering analysis and design of dynamic behavior		RF Intrusion Prevention System (IPS)
	RMF family of controls	Hardware implant detection/response/recovery	Dynamic embedded response planning		RF data sanitization (integrity, correction, rejection)
		RMF family of controls	**RMF family of controls**		Port security gateway
					Port-level anti-tamper/hardening
					Port-level Intrusion Prevention System (IPS)
					Insider threat modeling, detection, and response
					Supply chain data protection
					Supply chain counterfeit part detection
					Supply chain deep inspection
					Supply chain deep remediation
					RMF family of controls
Prepare	✓ CM SI	✓ CM SI	CM SI	CM SI	SC
Prevent	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ PE	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ MP SC SI	✓ ✓ ✓ ✓ ✓ ✓ ✓ MP SC SI	✓ ✓ ✓ ✓ ✓ AC IA SC	✓ AC MP SC SI
Detect	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ CA SI	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ CA SI	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ AU CA IR SI	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ SC SI	✓ AC AU CA CM SI
Respond	✓ ✓ ✓ ✓ ✓ ✓ IR	✓ ✓ ✓ ✓ ✓ ✓ IR	✓ ✓ ✓ IR	✓ ✓ ✓ IR	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ IR
Recover	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓

Attack vectors

- **Chip-level**
  - IC reverse engineering
  - Silicon malware
  - 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**
  - Backplane intrusion
  - Cross-board trust relationships
  - Malicious/vulnerable boards
  - Unsecured data storage
  - Embedded behavior
- **Bus-level**
  - External message manipulation
  - Actuator data manipulation
  - Bus man-in-the-middle (MITM)
  - Bus man-on-the-middle (MOTM)
  - Sensor data manipulation
- **Platform-level**
  - Vehicle-to-infrastructure (V2I)
  - Vehicle-to-vehicle (V2V)
  - RF communication apertures
  - Open data ports
  - Malicious insider
  - Supply chain
  - Open test ports
  - Malicious maintenance equipment

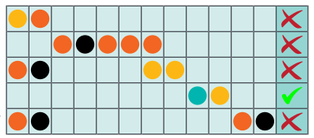


Chip-level defensive technologies provide protection at the IC level of design. These technologies are generally applied inside the supply chain and during the manufacturing process.

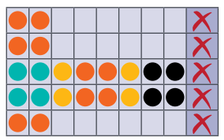


Board-level defensive technologies provide protection on the PCB by assuring trusted relationships and data flows across the PCB components. These technologies protect against malicious board implants, sensitive data disclosure, and data bus tampering.

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.



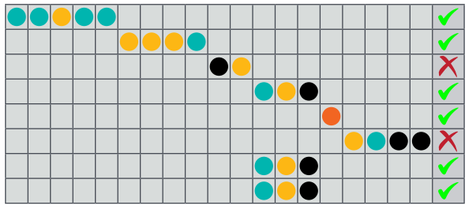
Bus-level defensive technologies protect devices connected to internal platform data buses (e.g., CAN Bus, MIL-STD-1553, FlexRay, Ethernet). These technologies protect against malicious implants and rogue assemblies that may attempt message sniffing, replay, injection and spoofing attacks.



Legend

- Mature technology (TRL 7-9)
- Prototypes emerging (TRL 4-6)
- Science developing (TRL 1-3)
- Future technology / unknown

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.

For more information contact:
BAE Systems
65 Spit Brook Road
Nashua, N.H. 03060
T: 603 885 4321
W: www.baesystems.com
Cleared for open publication on 8/19
Approved for public release; unlimited distribution.
Not export controlled per ES-FL-080219-0172

CS-19-D32