U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – GROUND VEHICLE SYSTEMS CENTER

Industry Days - Ground Systems Cyber Engineering

Jeff Jaczkowski

Associate Director

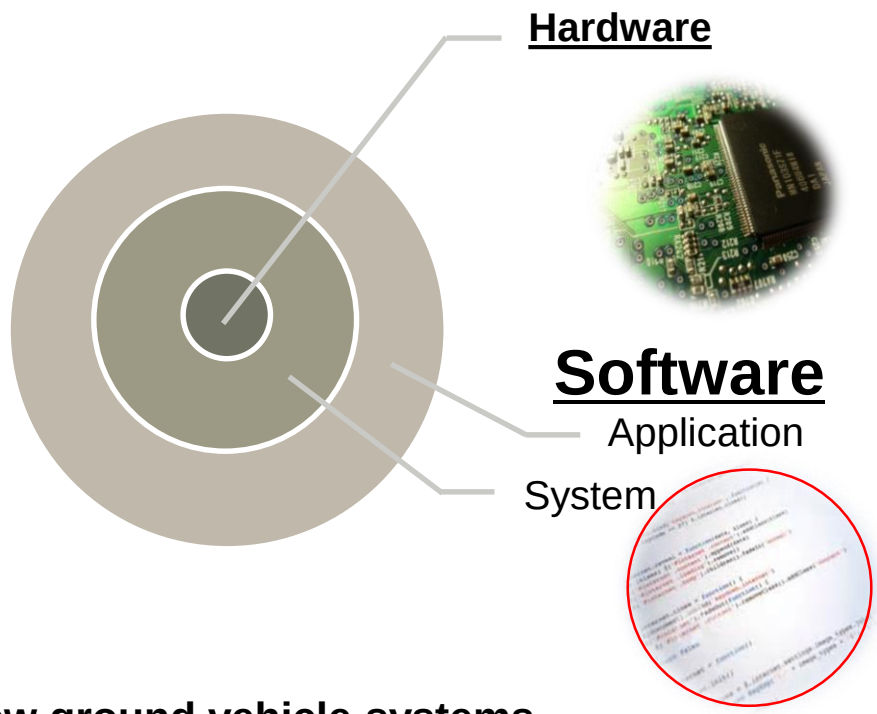
Ground Systems Cyber Engineering

2 April 2019

GROUND SYSTEMS CYBER ENGINEERING

Mission

To identify cyber vulnerabilities and adaptively secure joint service ground vehicles, watercraft and support systems by engineering resilient cyber solutions.



Priorities

#1 Ensure cyber resiliency for new ground vehicle systems

#2 Mitigate "Critical" vulnerabilities in fielded systems

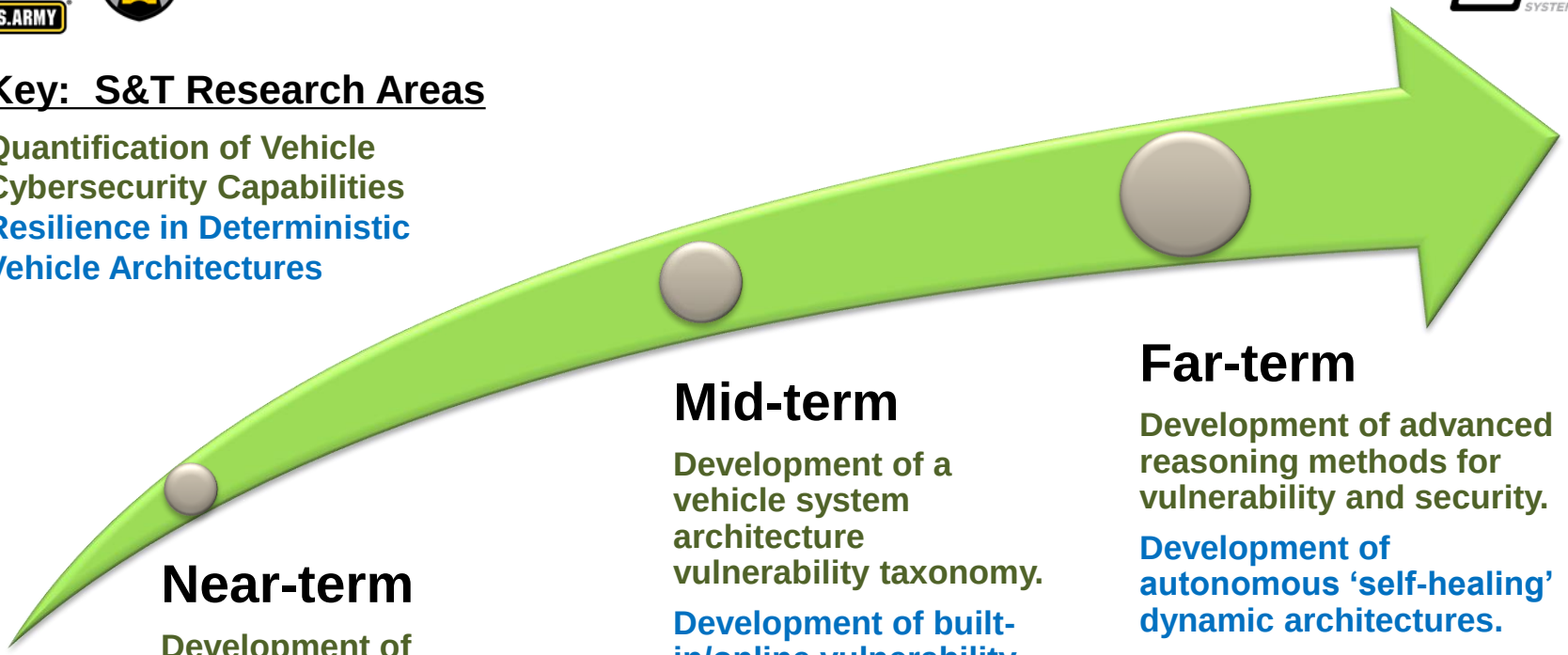
Baking security into the vehicle architecture will significantly reduce the cyber attack surface.

GROUND VEHICLE SECURITY & RESILIENCY S&T ROADMAP

Key: S&T Research Areas

Quantification of Vehicle Cybersecurity Capabilities

Resilience in Deterministic Vehicle Architectures



Near-term

Development of measurement, analysis and verification methods for vehicle architectures.

Development of virtualization (M&S) toolsets to design and 'virtually' test potential safeguards and solutions of the vehicle architecture

Mid-term

Development of a vehicle system architecture vulnerability taxonomy.

Development of built-in/online vulnerability identification, adaption and system repair.

Far-term

Development of advanced reasoning methods for vulnerability and security.

Development of autonomous 'self-healing' dynamic architectures.

Baking security into the vehicle architecture will significantly reduce the cyber attack surface.

VEHICLE CYBERSECURITY

“Top Four” Technical Challenges

Technical Challenge 1: Resilience in Deterministic Vehicle Architectures

1. Gap: Lack the ability to defend against unauthorized control or service denial
2. Barrier: Ground systems are highly complex integrated system-of-systems with distributed computer units, wide variances in vehicle iterations, inter-system data communication channels, and vehicle electronic architectures. As such, these platforms are vulnerable to cyber-attack from multiple vectors and multi-faceted approaches.
3. Resolution Timing: 2 - 4 years

Technical Challenge 2: Device Security /Supply Chain Provenance

1. Gap: Lack the ability to harden against reverse engineering, tampering, or unauthorized updates to hardware and software; Lack the ability to mitigate malicious supply chain risk and latent vulnerabilities in microelectronics and embedded software.
2. Barrier: Vehicle system, subsystem and component level supply chain is global and diverse.
3. Resolution Timing: 3 - 5 years

VEHICLE CYBERSECURITY

"Top Four" Technical Challenges

Technical Challenge 3: Embedded cyber-resilient technologies

1. Gap: Lack the ability for real-time threat detection and automated response.
2. Barrier: We don't know what we don't know (exploitable vulnerabilities and evolving adversarial sophistication). Can't test and mitigate every vulnerability.
3. Resolution Timing: 3 - 5 years

Technical Challenge 4: Quantification of Vehicle Cybersecurity Capabilities

1. Gap: Lack a robust evaluation methodology for vehicle cybersecurity that allows for standardized comparison across heterogeneous systems.
2. Barrier: Diversity of cybersecurity ecosystem and wide variety of lenses to assess and/or cybersecurity posture.
3. Resolution Timing: 1 - 2 years

Investment Strategy

Opportunities for Partnership FY20-24

- RFPP and Contract Award FY20 base with options under Detroit Arsenal Automotive OTA
- Funding estimated ~$1.0M-$3M/year
- FY20 Planned $1.45M

GROUND SYSTEMS CYBER ENGINEERING (GSCE)