CSRA
CYBER SECURITY
RESEARCH ALLIANCE

Designed-In Cyber Security for Cyber-Physical Systems

Workshop Report by the Cyber Security Research Alliance

4-5 April 2013 in Gaithersburg, Maryland

Co-sponsored with the National Institute of Standards and Technology

Workshop Report Abstract

Cyber-physical systems (CPS) are a diverse group of systems used to physically manipulate critical infrastructure such as power and water, industrial systems, transportation systems, medical devices, security systems, building automation, emergency management, and many other systems vital to our well-being. When CPS malfunction or fail, the operation of corresponding systems in the real world can impair physical safety or trigger loss of life, cause enormous economic damage, and thwart the vital missions of businesses, cities, states and the nation. On 4-5 April 2013, The Cyber Security Research Alliance conducted a workshop with the National Institute of Standards and Technology (NIST) to explore emerging research needs for cyber security in cyber-physical systems with the diverse cyber-physical community at large. This Report presents findings of workshop participants from the six topic-specific sessions, including a roadmap for research on ways to improve security of CPS.

Contents

1.0 Overview and Summary of Recommendations

1.1 Purpose of the Workshop

Cyber-physical systems (CPS) are a diverse group of systems used to physically manipulate critical infrastructure such as power and water, industrial systems, transportation systems, medical devices, security systems, building automation, emergency management, and many other systems vital to our well-being. When CPS malfunction or fail, the operation of corresponding systems in the real world can impair physical safety or trigger loss of life, cause enormous economic damage, and thwart the vital missions of businesses, cities, states and nations.

On 4-5 April 2013, The Cyber Security Research Alliance conducted a workshop with the National Institute of Standards and Technology (NIST) to explore emerging research needs for cyber security in cyber-physical systems with the diverse cyber-physical community at large. The sponsoring organizations held discussions on the following topics:

- Supply Chain: Its Impact on Securing CPS
- Approaches to Assurance and Assurance Composition for CPS
- Getting Reliable Information on Vulnerabilities and Threats
- Working with What We Have: Securing the Base
- Buying the Black Box: Security in Acquisition and Implementation
- Enabling Trustworthy Operation Readiness

1.2 Results from the Workshop

The workshop brought together engineering and IT experts who have dealt with security issues related to CPS. It provided an environment for interactive discussions among the attendees including industry representatives, academics, and government representatives. The workshop encouraged attendee participation through break-out discussions with limited presentations to frame the topics to be explored, allowing attendees to share experiences integrating security into existing organizations, i.e., lessons learned and examples. The first day of the workshop explored four of the above topics, while the second day of the workshop explored the last two. The discussions for the workshop provided input and material for leaders who then wrote white papers on the

related research needs, both short- and long-term, of the listed topics. All of those white papers are included in this report. This Overview section also includes a Summary of Recommendations for Research to improve the security of CPS, followed by a Summary of Recommendations by Topic.

1.3 Challenges in Architecting and Protecting CPS

Most CPS were designed for core functionality, not security. Cyber security concerns are a relatively recent issue that most CPS manufacturers did not factor into their original product development requirements.

CPS are susceptible to cyber security breaches for a variety of reasons. Some of them are listed below.

- Sometimes, vulnerabilities in firmware and software are incorporated into the system by rapid adoption of commercial off-the-shelf (COTS) technology and protocols. Long lifespans of CPS combined with changes in security mechanisms during their lifetime are a contributing factor.
- CPS are exposed to exploits due to systematic connectivity via the Internet, or via private communications systems connected to the Internet. Remote access for support and operations from anywhere in the world is expected functionality, providing additional vectors for attackers.
- Efforts to integrate CPS across facilities, companies and around the world also lead to increased attack surface.
- Many CPS use inherently insecure protocols such as MODBUS increasing the risks of connected operations.
- Even critical infrastructure providers[1] often use legacy CPS with industrial control systems that may not have enough memory or processing power to integrate security protocols and frequently rely on poor authentication practices.
- Lack of personnel training in security continues to be an issue.
- CPS may originate from vendors or suppliers that no longer exist. Heavy use of legacy components with little or no support is yet another source of vulnerabilities in CPS.
- Effects of change management could be a contributing factor.
- Finally, requirements for continuous operations that prevent changes or upgrades.

CPS comprise a variety of components, ranging from COTS commodity platforms to application specific devices that handle physical processes (e.g., Programmable Logic Controllers). This diversity and specific architectural requirements where high assurance components must be architecturally isolated (but need to share information with low assurance components) lead to many challenges in CPS design. Some research questions could be asked with regard to optimal CPS architectures:

[1] For a summary of critical infrastructure sectors by the U.S. Department of Homeland Security, see http://www.dhs.gov/critical-infrastructure-sectors.

- Which, and how many, architectural components can be controlled by an adversary without compromising system security?
- If we cannot build reliable systems with *all* compromised components, what access structures can be defined to allow the system to operate with integrity even after it has become compromised?
- Can a system's architecture enable continuity of operation even when an *adversary has penetrated the system*?
- Which data and components one can continue to trust?
- Does the architecture enable the definition of a *trust anchor* that maintains its integrity in the presence of an adversary?
- Can physical control structures (e.g., sensors) help in defining and protecting trust anchors?
- Can we establish a provable *Root of Trust* in CPS?
- Can we define architectures that support safety and fault tolerance without compromising security?

Although the workshop did not intend to address all the challenges presented above, it has formulated broad cross-cutting recommendations that can help address the most pressing issues in cyber-physical systems.

1.4 Summary of Recommendations by Topic

This section presents workshop recommendations by topic.

1.4.1 Supply Chain

	Recommendation	Details
	Short- and Mid-Term	
A	Create timeline of legislative and regulatory drivers that Impact CPS.	

B	Development of supplier reliability and monitoring methodologies.	Supplier reliability and monitoring methodologies will help acquirers to validate that suppliers are doing what they were asked to do.
		• Research and develop / adapt technical testing tools, including tools that:
		  ○ Attest to basic logic in different layers.
		  ○ Identify vulnerabilities in the stack (e.g., OSI model) and how can they be fixed.
		• Review existing and emerging practices

		and tools and adapt them to acquirer-supplier collaboration and information sharing, including obfuscation and non-attribution to protect the source.
Long-Term		
A	Build security into CPS to accommodate the special needs and environments.	• To maintain an appropriate security posture throughout their lives, which are often much longer than the lives of IT systems, and build cyber physical systems so that they can be modified in the future. • Build open interfaces to ensure interoperability in the present and in the future. • Build in technology refresh consistent with the evolving cyber threats.
B	Use data analytics to predict the future of securing CPS.	• Use data analytics to predict the future by applying emerging data analytics techniques to analyze the vast amounts of data that can be gathered from various cyber physical systems. Develop a methodology and tools that can analyze potential failures and counterfeits through pattern recognition and other techniques.

1.4.2 Assurance

	Recommendation	Details
A	Software designs for CPS and CPS properties.	Attempt to leverage physical system properties; i.e., discover methods to leverage physical properties for security assurance. Develop methodologies to increase assurance using physical properties.
B	Domain-specific taxonomy of risk and mitigation.	Research the domain-specific taxonomy of risk, and risk mitigation via assurance. Scientific determination of risk is imperative. • Need to define methodology for risk assessment. • Need to find specific security software design methodologies to provide tangible

		CPS assurances. • Need to find principles / best practices / taxonomy of measureable cyber security. Also, need to determine whether these different principles and practices depend on the infrastructure or types of control systems.
C	End-to-end determination of security assurance.	
D	Architectures for assurance in CPS.	Research architectures for assurance, notions of attack tolerance, hardened nodes, self-monitoring of CPS systems. Research must address these factors in legacy systems.
E	Composition of CPS components and assurance properties.	Research how the composition of CPS components leads to composition of CPS assurance properties.
F	Properties of CPS architecture.	Find properties of the overall CPS architecture – not only properties of individual components, but properties of the component composition. This will help derive end-to-end system assurances.
G	Specify combinations of CPS components and properties.	Specify precisely how the individual components are combined and how well the assurance properties of the overall system are understood and specified.
H	Economic incentives for CPS manufacturers.	Research the economic incentives for designing, deploying, and maintaining CPS systems from the perspective of CPS manufacturers.
I	Economic incentives for CPS owners and operators.	Research incentives to secure CPS from an owner / operator's business perspective: Where is the incentive to move down pathway towards secure CPS?

1.4.3 Threat Information

	Recommendation	Details
A	Develop configuration standards for CPS.	Develop configuration standards for control systems and cyber-physical systems in

		general. More guidance is needed on how to correctly deploy and configure individual components of CPS in specific environments and on standardization of these activities.
B	Detection and mitigation of vulnerabilities in CPS.	Research the detection and mitigation of vulnerabilities in CPS. We must employ a combination of various techniques, including artificial intelligence and machine learning (just to name a few) in order to detect security issues in cyber-physical systems. • Standard taxonomies and modeling/formalization of physical world systems would greatly help. • We must recognize the difference between current models we are well familiar with (e.g., cyber security of networks and operating systems) and cyber-physical systems.
C	Develop CPS taxonomy.	Develop a CPS taxonomy that focuses on the major cyber threats, vulnerabilities, consequences and mitigation measure linkages.
D	Develop cyber-physical models to quantify the impacts of potential cyber attacks upon essential equipment.	
E	Develop good reference implementations for these systems.	
F	Provide guidance on best practices for cyber security.	
G	Consolidate CPS standards.	Consolidate CPS standards to help people comprehend the overwhelming and overlapping amount of material available today.
H	Incentivize compliance by CPS owners and operators.	Incentivize owners and operators of CPS to voluntarily comply with industry best practices and standards.

1.4.4 Securing the Base

	Recommendation	Details

A	Develop a CPS taxonomy.	Develop a CPS taxonomy that focuses on the major cyber threats, vulnerabilities and consequences and mitigation measure linkages.
B	Develop cyber-physical models.	Develop cyber-physical models to quantify the impacts of potential cyber attacks upon essential CPS equipment.
C	Develop good reference implementations for CPS.	
D	Provide guidance on Best Practices for Cyber Security.	
E	Consolidate CPS standards.	Consolidate CPS standards to help people comprehend the overwhelming and overlapping amount of material available today.
F	Incentivize compliance by CPS owners and operators.	Incentivize owners and operators of CPS to voluntarily comply with industry best practices and standards.
G	Incentivize testing and certification by CPS manufacturers.	Incentivize manufacturers of CPS products and systems to have their products independently tested and certified for cyber security.
H	U.S. federal agencies should lead by example.	U.S. federal agencies should lead by example by purchasing cyber security tested and certified products and software to secure their own CPS.
I	Offer CPS cyber security education.	Offer CPS cyber security education at the high school, trade school and university level.

1.4.5 Black Box

	Recommendation	Details
A	Evaluate procurement and deployment practices to engage the CPS supply chain in security.	Evaluate practices to engage the supply chain function to understand the role of security in the acquisition and implementation practices. Within the supply chain function there needs to the development of reusable security requirements and the inclusion of specific and evaluated security procurement language.

B	Clarify the CPS threat landscape.	Develop and define a uniform threat landscape for CPS that can be used to quantify "secure." Is security the same as resiliency? How much resiliency is enough to say that CPS is secure?
C	Evaluate risks of the CPS security ecosystem.	Using the definition of security and understanding of resiliency, evaluate the risks of ensuring a trustworthy and composable CPS security ecosystem.
D	Define practices to ensure whole-system trust of CPS.	Evaluate what practices can be used by vendors when they are presenting a system-of-systems, and what practices can be used by acquirers to ensure that the whole system can be trusted as a single architecture. • What factors of reliability, performance, survivability, and assurance are necessary to ensure trustworthiness?
E	Integrate conformance assessment as a core component of the CPS procurement lifecycle.	Develop a consistent definition of security and resiliency, specific procurement language, and an understanding of what makes for a trustworthy composable architecture. A long-term research opportunity is to integrate conformance assessment as a core component of the procurement lifecycle. The practices need to protect the intellectual property of the vendor, but still provide sufficient demonstrable evidence to the acquirer that the vendor's solution is secure. • Is the conformance assessment process something that is initiated by the acquirer? • Is conformance assessment something provided by the vendor during the requirements analysis? • What level of detail is provided to the acquirer?

1.4.6 Trustworthy Operations

	Recommendation	Details
A	Develop security vulnerability and threat taxonomy for CPS.	
B	Define security metrics for CPS, including lifecycle metrics.	
C	Develop new approaches to CPS certification and verification.	
D	Establish a research field focusing on run time trust evidence.	
E	Define viable trust languages to improve design of secure components and protocols.	
F	Work on finding commonalities for establishing cross-domain security in CPS and beyond.	
G	Start work on economics of security for CPS.	
H	Expand research on usability and use cases for CPS.	

1.5 Common Research Ideas

The workshop discussions and reports revealed many common themes. A summary view of these themes is presented below.

1.5.1 Understand the Field of CPS by Creating Taxonomy.

Most of the reports suggested starting CPS-related cyber security research at the foundation, by assessing currently available mechanisms and directions and defining the field of research. Understand the diverse field of CPS, its commonalities, and connections, and its relationship to evolving threats and available mitigations could be started by developing a taxonomy or ontology that can serve as a foundation and starting point of research.

1.5.2 Develop a Notion of Valid and Optimal CPS Architectures.

This can be done by engaging in research that draws from achievement in specific CPS contexts (e.g., aeronautical applications) and adjacent fields to develop building blocks of optimal CSP architectures.

1.5.3 Develop More Resilient and Responsive CPS.

CPS with greater assurance need to be developed. We can use achievements in adjacent fields and general pioneering ideas to develop innovation in CPS, such run time integrity checking, a new generation of secure protocols and trust languages to assess the state of CPS communicating with each other and beyond. This area can also include the ability to change trust posture over the lifespan as threats change, and the ability to heal CPS when attacked.

1.5.4 Establish Approaches to Security and Trust Composition in CPS for Coherent In-Domain and Cross-Domain Operations.

With greater connectivity and integration in all CPS areas, we need to develop methodologies and approaches for end-to-end trust and assurance in CPS that assess security of CPS at design and operation stages

1.5.6 Establish New Approaches to Security Assessment and Certification.

Using approaches to certification and verification in adjacent fields, we need to create techniques that work for CPS.

1.5.5 Establish Metrics and Assessment Models for CPS.

Based on theoretically established baselines and data analysis, we need to establish metrics and assessment models for CPS. The approach to metrics will use analytics and available data combined with newly formulated theoretical knowledge to provide insights into the functionality of current and future CPS.

1.5.7 Establish New Methodologies to Study CPS Supply Chain and Provisioning.

We need to define new methodologies to study supply chain and provisioning in CPS based on unique characteristics of these systems. CPS have unique features that require a fresh view of supply chain and provisioning activities for these systems; research in this area is needed.

1.5.8 Collect and Streamline Best Practices in CPS.

Research in CPS could draw extensively from best practices that are already established in different CPS contexts, to inform practical short term research. It will help R&D to makes these best practices available to researchers in a format that is easy to use and understand.

1.5.9 Define Standards for Greater Uniformity of Security Functions and Better Interoperability in CPS.

Some of the best practices and available mechanisms for CPS security could benefit more consistent and general standardization. Standardization will streamline approaches and increase adoption of more secure design and operations.

1.5.10 Define Economic and Business Incentives for Secure CPS.

There are no economic studies focusing on CPS or economic models based on specific features of CPS and the contexts of their use. Research in this area will be beneficial for devising a new generation of the technologies and for adoption of more secure CPS.

1.5.11 Establish Cyber Security Curricula for Studying CPS to Ensure Supply of Skills and Expertise.

There is a dearth of security specialists understanding security and CPS. We need to define useful curricula to ensure there are skills and expertise to develop and maintain more secure CPS in the future.

2.0 Supply Chain: It's Impact on Securing Cyber-Physical Systems

Presenters: Nadya Bartol, UTC; and Jon Boyens, NIST

4-5 April 2013 in Gaithersburg, Maryland

Abstract

Information and Communication Technology (ICT) products are assembled, built and transported by multiple vendors around the world – and not always with the knowledge of the acquirer. Abundant opportunities exist for malicious actors to tamper with and sabotage products, which can compromise system integrity, reliability and safety. Organizations acquiring hardware, software and services are not able to fully understand and appropriately manage the security risks associated with the use of these products and services. The challenges range from insufficient acquirer practices to lack of visibility into, and understanding of the supply chain. The same challenges apply to ICT that is used in cyber-physical systems (CPS). The workshop addressed four primary objectives: (1) validate supply chain as an issue for CPS; (2) get up to speed on the current body of knowledge about the supply chain; (3) identify CPS-specific aspects of the problem; and (4) identify future research topics.

2.1 Discussion of Issues

Facilitators presented numerous efforts to develop ICT supply chain risk management practices by U.S. government and industry, including several international standards efforts. Facilitators noted that many of these efforts and the resulting practices are rooted in the common source originating within the Department of Defense (DoD). Within the DoD context, the practices were developed to encompass IT-intensive systems, rather than information systems. The latter includes cyber-physical systems, such as weapons systems or industrial control systems. Figure 1 shows the timeline of numerous existing and emerging practice development and availability.

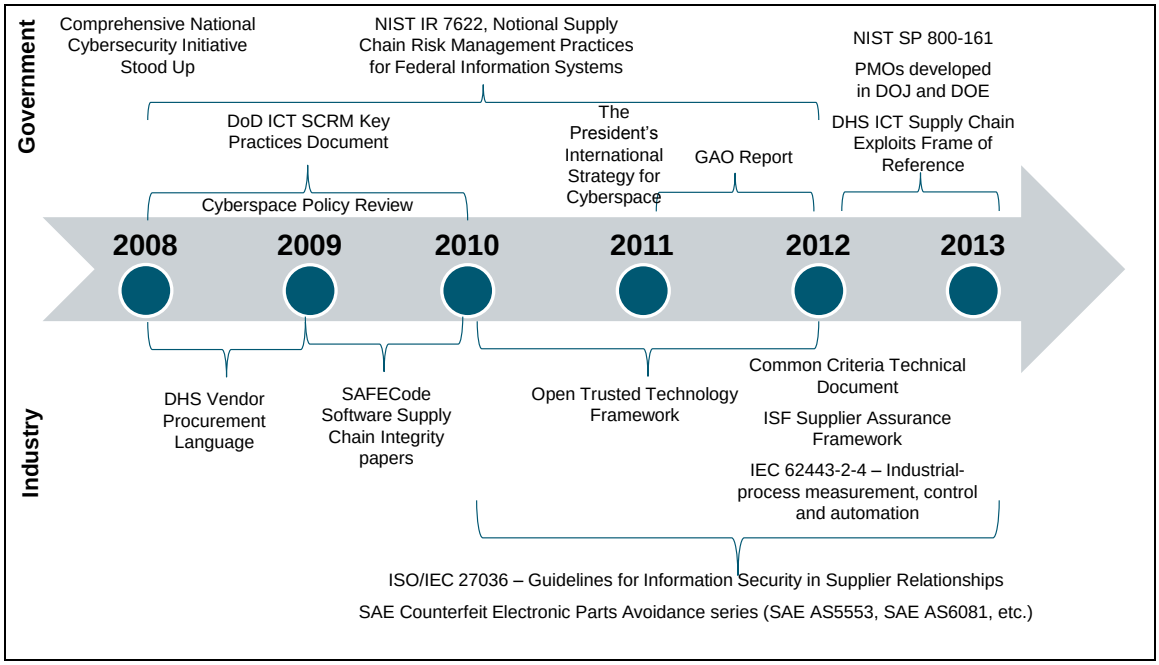

Figure 1. Existing and Emerging ICT SCRM Practices

Facilitators guided discussion at the workshop on the following key questions:

- How is supply chain for cyber-physical different from cyber-cyber?
- What are the best ways to facilitate real-time collaboration among suppliers and acquirers – establishing long-term productive supplier relationships?
- How to produce cross-organizational integration? Examples include quality, acquisition, cyber security, supply chain and logistics.

2.2 Key Findings

Workshop participants expressed a broad variety of views on whether supply chain concerns for CPS differ from those concerns for the information technology systems, from passionate "yes" to passionate "no." Participants did agree that the context and the objectives for CPS differ from industry to industry and, in many cases, differ from those of IT systems, including:

- Many CPS are built to last much longer.
- Organizations using CPS operate with different business models.
- Many CPS technologies have different supply chains than IT systems.
- Objectives of CPS are to provide reliability and availability to support the mission rather than confidentiality, integrity and availability to support cyber security.

Overall, the challenges can be summarized by quoting one of the participants for the aerospace industry who stated: "We are building tomorrow's legacy system today."

While consensus was not achieved, the workshop participants agreed that it is appropriate to use practices developed in other contexts and apply them to the ICT supply chain risk management concerns for CPS, including:

- Existing ICT supply chain practices.
- Safety and other 'ilities."
- Telecom industry.
- Airline industry – air-worthiness for broader cyber-physical.

The participants also agreed that to implement ICT supply chain risk management, the organizations have to implement good basic security practices first as pre-requisites. Participants articulated the challenges for CPS that are quite similar, if not the same for the IT systems. These include the need for the business case in managing ICT supply chain risk management concerns, constraints related to business liability in the acquirer-supplier relationships, and the need to establish the language for conducting a dialog between acquirers and suppliers.

2.3 Research Opportunities

As a result of the themes discussed in the workshop, participants identified the following short term, mid-term and long-term research opportunities:

2.3.1 Short-Term Research

2.3.1.1 Determine a timeline of legislative and regulatory drivers that impact cyber physical systems. The timeline would help individuals trying to improve cyber security of CPS demonstrate the related need and compliance drivers. Ultimately, this will help create motivators to build business cases for change.

2.3.1.2 Develop supplier reliability and monitoring methodologies to help acquirers validate that suppliers are doing what they were asked to do. For example, development could repurpose and adapt existing open source assessment / measurement tools to assess / measure supplier-based reliability.

2.3.1.3 Research and develop/adapt technical testing tools, including tools that

- Attest to basic logic in different layers.
- Identify vulnerabilities in the stack (e.g., OSI model) and how can they be fixed.

2.3.1.4 Review existing and emerging practices and tools, and adapt them to acquirer-supplier collaboration and information sharing – including obfuscation and non-attribution to protect the source in cyber-physical space.

2.3.2 Mid- and Long-Term Research

2.3.2.1 Build security into cyber physical systems in a way that would accommodate the special needs and environments of those systems:

a. To ensure that CPS can maintain an appropriate security posture throughout their lives, which are often much longer than the lives of IT systems, and build CPS so that they can be modified in the future.
b. Build open interfaces to ensure interoperability in the present and in the future.
c. Build in technology refresh that is consistent with the evolving cyber threats and requirements.

2.3.2.2 Predict the future by applying emerging data analytics techniques to analyze the vast amounts of data that can be gathered from various CPS. Develop a methodology and tools that can analyze potential failures and counterfeits through pattern recognition and other techniques.

3.0 Approaches to Assurance and Assurance Composition for CPS

Presenters: Hal Aldridge, Sypris Electronics; Virgil Gligor, Carnegie Mellon University (Moderator); and Michael Peters, Lockheed Martin Corporation

5 April 2013 in Gaithersburg, Maryland

Abstract

This session addressed security assurance and assurance composition in Cyber-Physical Systems (CPS) in the presence of a well-defined adversary threat. Workshop participants focused on the (1) definition of assurance, (2) assurance types and properties, (3) architectures for assurance, and (4) assurance composition in CPS. Discussion also addressed the adversary definition and distinguished it from that of system vulnerability. Finally, participants urged the need for economic incentives to produce end-to-end system assurances. A few topics were proposed for the NIST research agenda and a set of seven research priorities were outlined in the Plenary Session.

3.1 Generic Definition of Assurance in Security

In security, the notion of assurance is typically defined by the evidence that a system has a set of *desired properties that hold in the presence of an adversary*. This definition implies that *no other properties may hold*. In short, we say that a security-assured system has a set of desired properties – and nothing else. For CPS, this definition suggests that the focus addresses (1) the types of properties are required in a system, (2) the definition of the adversary, and (3) the nature of "nothing else," namely on the absence of unintended functions, which may (not) be found in the system design and implementation. Participants agreed that "perfect assurance" may be obtained only if one has a fully specified system, where specifications range from design to implementation and from tools to operational processes and procedures. Rather than address perfect assurance, participants concluded a more appropriate objective would be defining assurance metrics, which capture the degree of *operational CPS resilience* in the face of an adversary.

3.2 Assurance Types and Properties for CPS

Given the above definition of security assurance, the immediate question is: what types of properties are we seeking for CPS? Also, how are these properties different from the

more mundane assurances defined for ordinary cyber-security such as the Common Criteria.

Participants noted two areas in which some of the security goals of CPS are different from those of ordinary computer systems and networks of the past thirty years. The first refers to the changed relative importance of security goals in CPS. Availability and integrity are the most important properties of a CPS and the importance of confidentiality is relevant only as a supporting goal for the previous two. Availability is generally understood to be the ability to maintain continuity of operations during attacks (e.g., DoS and DDoS) that target the CPS infrastructure. System integrity is generally understood to mean the condition under which a system operated within its prescribed parameters and limits. Confidentiality is the condition under which unauthorized disclosure of protected information cannot take place.

The second area in which CPS differ from ordinary computing systems and networks is that at least some of their availability and integrity parameters and limits are defined by physical processes. The *properties of these physical processes* are provided by other engineering and science disciplines, and are well understood. Hence these properties can be leveraged to define required assurances.

Two areas of similarity between CPS assurances and ordinary computing platforms and networks were also noted. After all, a large number of CPS components comprise commodity (e.g., COTS) computing platforms and networks and their assurance – or lack thereof – directly affects the CPS operation.

The first area of similarity is that assurances may be design / implementation assurances or operational assurances. Design / implementation assurances refer to the definition of system components whose properties can be verified via standard methods and tools; e.g., formal specification and verification, and testing. Operational assurances refer to the set of procedures and processes that are executed to maintain certain properties as the system runs; e.g., trusted facility management, network monitoring and detection of intrusions, and safe operator interaction with the “outside world.” Here the outside world consists of networks to which the CPS may be externally connected, such as private business networks and the public Internet. Such connectivity may in fact breach designed-in “air gaps” that are supposed to physically isolate a secure network. However, lack of outside world connectivity does not guarantee the integrity of air gaps. These can be breached by social engineering, which is the largest single vector of malware propagation today.

The second area of CPS-assurance similarity with ordinary systems and networks is that of *heterogeneity of assurances*. That is different system and network components function at different levels of assurance; e.g., typically COTS components have low assurance, whereas application-specific CPS components can have higher assurance. Undocumented components have – by definition – the lowest assurance, since they have no definable properties that can be verified either at design and implementation time or during system operation. In contrast, complete assurances require complete system

specifications; e.g., design, implementation and operation specifications, and specifications of system generation, configuration and initialization. Several workshop participants noted the pervasiveness of unspecified / undocumented system features and pointed out the severity of this problem, particularly in certain government systems.

A question was raised as to whether the adoption of assurance properties found in avionics in a more general CPS setting would be appropriate. Although undoubtedly useful for some isolated CPS components, avionics assurances are unlikely to apply directly to all components of CPS due to the higher level of heterogeneity of CPS properties, and differences in the adversary (threat) models adopted.

3.3 Architectures for Assurance

Given that CPS comprise a variety of components, ranging from COTS commodity platforms to application specific devices that handle physical processes (e.g., Programmable Logic Controllers), there is a question of how to partition the system into separate components and apportion assurance properties to these components. Furthermore, specific system architecture is also driven by the heterogeneity of assurances; i.e., high assurance components must be architecturally isolated from the low assurance components so that their operation is unaffected by failures and/or penetration of the low assurance components by a (defined) adversary. Finally, the architecture must enable high assurance components to send data and commands to low assurance components, but high assurance components must not receive data and commands from low assurance components unless and until the validity of those data and commands is established.

The participants noted a variety of other questions related to the design of architecture for assured systems. For example:

- Which, and how many, architectural components can be controlled by an adversary without compromising system security?
- If we cannot build reliable systems with *all* compromised components, what access structures can we define such that some components can be fully compromised by an adversary and yet allow the system to operate with availability and integrity?
- Can a system's architecture enable continuity of operation even when *adversary has penetrated the system*? Does one know or can one find which data and components one can continue to trust? Does the architecture enable the definition of a *trust anchor* that maintains its integrity in the presence of an adversary? Can physical control structures (e.g., sensors) help in defining trust anchors? Can we establish a provable *Root of Trust*?

Participants also observed that since assurances for secure operation differ from those for safe / reliable / fault-tolerant operation, architectures for secure system operation are likely to differ from those for safety, reliability, and fault tolerance. In particular, they noted that:

- Safety/reliability/fault-tolerance differ from security in several areas since deliberate compromise may not necessarily cause a detectable safety violation/failure.
    - Safety revolves around repeatable points where an operational problem arises.
    - Safety is inherent to the design of the system.
    - Safety is statistically provable and repeatable.
    - Safety does not exist if cyber security incidents arise.
- Fail-safe operation can be circumvented by an adversary (e.g., by malware).
    - The goal of safety architecture is to be resistant to failure.
    - Security has different causes for failures; i.e., penetrations, intrusions.
    - In security, failure isolation by safety mechanisms is insufficient; instead remediation becomes necessary; e.g., if a CPS is manipulated from afar, and valves open and close arbitrarily causing an adverse event, mitigation/ remediation action – not just isolation -- is required.

3.4 Composition of Assurances in CPS

Several participants emphasized the challenge of composing different CPS components and protocols to provide end-to-end assurances within a system. In particular, they noted that the security properties of communication protocols would have to be composed with those of operator consoles, application servers, and controllers of physical systems, and that those protocols are typically insecure. In CPS, communication protocols are designed by industry / trade associations and foundations with limited regard and expertise for security properties. For example, the Modbus protocol provides no security against unauthorized commands or interception of data; and similarly, DNP3 was not designed to counter the attacks of an adversary who wishes to disrupt or disable CPS.

Another area of assurance composition is that of physical systems properties and underlying computing system and network properties. Several participants remarked that physical system invariants could potentially be leveraged to monitor and possibly verify the operation of computer and network components in the face of external adversary attacks. However, once malware penetrates a system, it could simulate correct responses to verification commands sent by an operator while at the same time compromising the operation of the CPS.

3.5 Adversary Definition

The discussion addressed the questions of how to define the adversary threat (i.e., threat modeling) and how to use the adversary threat in defining access structures that are able to counter the threat. It was observed that objective measures of threat and corresponding security metrics differ from metrics for system vulnerabilities. In particular, an adversary attack is characterized by an adversary goal and capabilities necessary to reach that goal against a specific system. The adversary capabilities may enable exploitation of specific

system vulnerabilities to reach the attack goal. An adversary may have to reach an intermediate goal to acquire a specific capability for a larger attack goal, and this gives rise to the notion of attack trees.

Merely neutralizing a known attack / exploit enabled by a vulnerability may not eliminate all other exploits / attacks that might be enabled by that vulnerability. On the other hand, a system vulnerability may be left unexploited by an adversary attack, at least for a while, given that other more effective exploits might leverage other vulnerabilities to reach an adversary goal. In short, assurance metrics must capture the notion of the "weakest link" in a system and the highest payoffs for an adversary attack.

Participants discussed the following topics of adversary definition. Several research topics were outlined based on these discussions.

- A system design must assume the presence of malware presence (and other vulnerabilities) in the system. There is a need to assume that certain components of a system can be compromised.
- Adversary goals and capabilities (threat) against a CPS may be different than those of an ordinary computer system and network.
- Operational detection of an adversary's presence in a system is necessary. There is a need to develop intelligence tools that enable detection of adversary within a system. Current CPS infrastructure in the US is not even doing basic detection and blocking of malware. Systems are often left unpatched for a long time.
- The effect of an adversary attack on a system must be determined by a critical analysis of the system components; e.g., one must determine the number of components controlled by adversary. Is each system component equally valuable with respect to overall system security? What is level of access needed to compromise a system? What is the maximum level of and type of access structure needed to operate a system securely in the presence of an adversary?

3.6 Research Opportunities

During the plenary session, seven research areas were proposed for collaboration with the U.S. government (and in particular, NIST):

3.6.1 Software Designs for CPS and CPS properties.

This research should attempt to leverage physical system properties; i.e., discover methods to leverage physical properties for security assurance. Develop methodologies to increase assurance using physical properties.

3.6.2 Domain-Specific Taxonomy of Risk.

This research is for domain-specific taxonomy of risk, and risk mitigation via assurance. Scientific determination of risk is imperative, including:

- Need to define methodology for risk assessment.

- Need to find specific security software design methodologies to provide tangible CPS assurances.
- Need to find principles / best practices / taxonomy of measureable cyber security. Also, need to determine whether these different principles and practices depend on the infrastructure or types of control systems.

3.6.3 End-to-End Determination of Security Assurance.

Workshop participants proposed research on architectures for assurance, notions of attack tolerance, hardened nodes and self-monitoring of CPS systems. The research must address these factors in legacy systems. It also should examine the how the composition of CPS components leads to composition of CPS assurance properties, including:

- Find properties of the overall CPS architecture – not only properties of individual components, but properties of the component composition. This will help derive end-to-end system assurances.
- Specify precisely how the individual components are combined and how well the assurance properties of the overall system are understood and specified?

3.6.4 Economic Incentives for CPS Manufacturers and Operators.

This research should suggest economic incentives for designing, deploying, and maintaining CPS systems; e.g., economic incentives for equipment manufacturers and operators.

- Provide incentive to secure CPS from a business perspective: where is the motivation to move down pathway towards secure CPS?
    - Regulatory.
    - DOD / Intelligence / Appropriations.
    - Use regulatory power to mitigate some of the risk.
- Find methods to better communicate the business case for assurance in CPS based on cost-benefit analyses to enterprise management.

3.6.5 Methods and Tools to Analyze Security of Existing / Legacy CPS.

This research should take an opportunistic approach, since time is of the essence; i.e., improve assurances for existing system COTS components in incremental steps rather than wait until the perfect solutions appear.

- Types of system patching; e.g., online vs. offline; frequency, extent of remediation.
- Analysis of security properties of legacy systems.
- Tools / methods to analyze security of existing / legacy systems.
- Tools needed to recognize an attack has occurred (not necessarily try and stop it).
    - Light weight network monitoring tools; extremely affordable.
    - Tool scalability is important; e.g., whitelisting of uncompromised operational components is useful but does not scale well.
    - Tools must enable operators to feel like they are in control as much as possible, and must not produce false positives.

3.6.6 Convert Specifications Into Security Assurances.

This research should explore how to convert design specifications of CPS and operational specifications into actual security assurances.

3.6.7 CPS Situational Awareness.

This research should start with detection of current state properties and develop tools for the prediction of future system states; e.g., anticipate the onset of adversary attacks.

4.0 Getting Reliable Information on Vulnerabilities and Threats

Presenters: Edward Bonver, Symantec Corporation; David Dagon, Damballa;
and Lisa Kaiser, Department of Homeland Security

4 April 2013 in Gaithersburg, Maryland

Abstract

The workshop participants strongly expressed the need for methodologies which uniquely apply to risk assessment of cyber-physical systems (CPS). Unlike computer and network systems, CPS are complex “systems of systems” where vulnerability in a sub-component can have unknown, distributed impacts – even the disruption of devices controlled by CPS that can result in catastrophic failure of critical infrastructure and services. If such methodologies assessing risks in CPS exist, participants were not well aware of them, and expressed the need to develop them. Presenters guided participants through background on the challenges of securing CPS. Consideration was given to the use of information about vulnerabilities and threats from the end-user perspective, and how this information is distributed by vendors. Participants also suggested several paths for research to help improve the ability to secure CPS.

4.1 Background on Security of CPS

In order to understand security of cyber-physical systems (CPS) we first need to define what a CPS is – and how different such a system is from other familiar systems. Despite the existence of formal definitions of cyber-physical systems by NIST and other organizations, most of the workshop participants were unaware of these or were not well versed in this baseline.

4.1.1 Security is Straightforward for Known Systems

To set the stage for discussion, presenters noted examples of models and systems that are well understood:

- We understand what a personal computer system is. Such a system consists of well-understood hardware and software components. For example, hardware consists of a CPU, hard-disk, random access memory, etc., while software consists of firmware, operating system and applications on top of the operating system.
- We also understand the networking paradigms. For example, there is a client-server architecture, where a server may be providing certain services to the clients over some network connections.

Our knowledge of such systems provides a better grasp about vulnerabilities and threats in environments that employ such systems. For example, if there is a buffer overflow vulnerability in a component of a personal computer system described above, we can analyze it and conclude the impact, severity, exploitability, etc. within this (arguably relatively simple) model. In our client-server example above, if there is a denial of service threat on the server component, we understand the consequences and can perform risk management activities based on that sure knowledge.

4.1.2 “Systems-of-Systems” Visibility is Limited for CPS Security

The security situation is quite different for CPS. These “systems of systems” are usually much more complex and extend well beyond just direct intelligence on any particular vulnerability or threat. Within a CPS, a buffer overflow in a component might have drastically different consequences (e.g., it might affect other components; hence it can affect security of the entire system), and ultimately, the consequences can be of physical nature. If we learn of this vulnerability from the vendor / manufacturer of the component, we might still not be in a position to understand how this vulnerability influences security of the entire system. In other words, we need to understand threats as they apply to complete integrated systems instead of within individual components. Given the complexities of distributed complex systems like CPS, how do we truly determine the true impacts of vulnerabilities? And how can we manage risk in the CPS world where the systems cross multiple domains, some of which might be outside of our control (e.g., owned by customers who are outside the direct chain of command)?

Context is extremely important in the CPS world where threats exist because of the integration of multiple components within multiple systems. Immediately after several components are integrated into their unique operating environment, new hard-to-identify vulnerabilities and threats arise that might not have been previously observed. As a further complication, a breach of CPS security may trigger physical events depending on the characteristics of the system and devices under its control. Threats may manifest themselves uniquely in one way or another within physical systems and within cyber

systems; once you combine the two types of systems together, the same vulnerabilities may carry different impacts, and threats may manifest themselves completely differently. For this reason it is crucial for the stakeholders to understand physical cyber interaction of their systems. Currently we lack such understanding.

Ultimately, assuming sufficient information from the underlying component vendors, it is the end consumer of the system who is better fit to understand the impact of any given vulnerability in any given component of the system as it is deployed within the end consumer's environment. However, obtaining such information with relevant and sufficient detail is rarely possible. Frequently an end consumer or a vendor who is part of the supply chain does not have a good grasp on the system inventory, nor is there a list of all components and their vendors. Without this inventory, they may not be in a good position to properly judge impacts of vulnerabilities or even realize that the CPS is at risk.

4.1.3 Illustrating the Challenge of CPS Security: Patch Management

There are many standard processes for ensuring the security of an IT system. To illustrate the challenge of performing just one of these for a CPS, consider requirements for software or firmware patch management. How do you go about performing patch management in CPS? Many physical devices either completely lack upgrade / patching capabilities, or are very hard to patch. For example, in order to patch, a technician might need to physically operate a device in the field via a direct wired connection. Doing this may require taking the device / system off-line to apply a patch. This, in turn, means that planning for a patching event might need to happen well in advance. Taking a CPS offline is often not economical and can result in putting the system into a vulnerable state (unpatched) for a long period of time – sometimes months, years or permanently. Also, owners of the CPS justifiably have fears based on past experience of complications with patching. In those cases, a system might not have operated properly after application of a patch, might have malfunctioned, or remained vulnerable to additional threats as a result of the applied patch.

Workshop participants strongly expressed the need for methodologies that uniquely apply to risk assessment of CPS. If such methodologies exist, participants were not familiar with them. And where the required methodologies do not exist, participants said these should be developed for securing CPS.

4.2 Customer View: Getting Reliable Information from Vendors

One of the challenges identified in the workshop was obtaining information on vulnerabilities from vendors in sufficient depth so that engineers and architects could understand the impact within their own systems. There needs to be more context about what impact a vulnerability would have in a CPS.

4.2.1 Illustrating the Importance of Good Vendor-Provided Vulnerability Data

Recalling the previous example of a buffer overflow, when a vendor releases information that there is a buffer overflow in one if its components, engineers or architects who work

on CPS where that component is used need to understand impact of this specific vulnerability within their system. (As noted, impact varies based on the environment where the vulnerable component is deployed). Stakeholders need to understand how adversaries might target specific vulnerabilities in the systems deployed within specific cyber-physical environments. Unfortunately, workshop participants overwhelmingly said the way vendors currently release vulnerability information does not include required details. Consider that organizations like the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) release alerts for vulnerabilities related to cyber security of CPS do get vulnerability notifications from vendors going as deep/technical as operating system driver level. Providers of this information, however, do not know details about the architecture of the different topologies of various affected entities. Hence, they cannot understand and report the true impact of the related vulnerabilities. According to workshop participants, information reported by such organizations is perceived to be overwhelming to end users.

The research community has expressed interest in getting access to as much raw data as possible in order to study the threat landscape of CPS. However, access to such data is rarely available because vendors, governments and other organizations are often reluctant to share information about vulnerabilities. A good information sharing method is absent.

4.2.2 High-Level Summaries of Vulnerability Data

Workshop participants expressed the need for high-level (executive) reports from the vendors. Such reports should be aimed at people who are decision makers, but are not very technical. Also, such reports should propose viable solutions in order to for these individuals to be able to make decisions on how to address and mitigate the reported vulnerabilities and threats.

4.2.3 Timing the Release of Vulnerability Data

Another issue is timing the release of vulnerability information. Real-time flow of information is extremely important and is currently perceived as inadequate, according to workshop participants. For this reason, quarterly reports produced by U.S. government do not seem to do the job, as the information they contain quickly becomes stale. For example, based on this report, an organization might determine that its system is vulnerable to an attack. At that point it could mean that adversaries were exploiting the vulnerability in the system for the past three months, and the organization did not have an opportunity to act upon it because they didn’t know about it until the report came out.

We note that to be effective, machine learning and artificial intelligence techniques rely on fresh data. This is true for those techniques that operate in real-time (e.g., anomaly-based intrusion detection systems that use artificial intelligence algorithms), as well as for those that perform calculations outside of the deployed environment (e.g., machine learning techniques, used to calculate rule sets that will be applied to the deployed system at a later time). If vendors don’t release vulnerability information quickly enough, such

techniques that do not have access to the freshest data may lose their effectiveness as well as efficacy. Losing effectiveness and efficacy of security technologies (e.g., intrusion detection, firewalls, antivirus, or any other automated threat response technologies) is a major concern when it comes to protection of CPS.

4.2.4 Impact of Language on Vulnerability Data

Major focus on the English language in current vulnerability databases, such as Common Vulnerability Enumeration (CVE) system was also expressed by the workshop audience as a concern. Many system administrators, engineers and architects around the world might not possess sufficient knowledge of English in order to understand information reported in such databases. Hence, they may not understand the impact, perform the necessary threat analysis and proceed to appropriately protect their affected systems – despite that an English-only report could contain correct and sufficient information for threat remediation and mitigation.

4.3 Vendor View: Communicating Information on Vulnerabilities and Threats

Vendors always face the following dilemma when releasing information about vulnerabilities in their components to the public. On the upside, such information could be helpful to customers / consumers of the component. As noted, the information is useful to help users protect themselves by patching, modifying the environment, tweaking firewall and intrusion detection rules, disabling the component altogether, and performing other security processes. However, on the downside, such information can also get into the wrong hands. Malicious actors could employ this information in order to create new attacks / exploits. Their actions would put customers / consumers at risk of additional threats related to the vulnerability without corresponding corrective action. In recent years many vendors have followed better practices of releasing vulnerability information about their products/components. But there are still vendors that would prefer to either not release information or not provide sufficient technical detail about their vulnerabilities.

4.3.1 “Need-to-Know” Provision of Security Data

Part of the dilemma for vendors is how to disseminate such information to the parties that need to know about it without having that information fall into the wrong hands. Also, communicating information to a privileged “white list” of parties raises a number of questions: How can a vendor have such a white list? What would qualify an entity in order to be listed? How do the downstream parties obtaining that information ensure its safety? For example, do they store that data securely within their own infrastructure? Do they disclose it to any of their own customers? What other security controls do they have in order to control this information within their own environments?

Many vendors find themselves in the middle of the supply chain for CPS, where they need to understand impacts of vulnerabilities of third-party components used in the system. Vendors may need to communicate this information up the chain in addition to sharing

information on vulnerabilities discovered in the components they have created and control. In other words, information flow could be improved in the complex CPS vendor / supply chain / customer relationship. There is a need for standards related to this information flow so that everyone in the listed relationship understands their own roles and responsibilities, knows where to obtain information relevant to threats on their system, who to pass the information to, and how to make appropriate decisions in order to quickly act upon it.

4.3.2 Disclosure of Vulnerability Data to the Media

Several workshop participants said a major source of information related to real vulnerabilities is from the media / press and other public resources such as security bloggers. Frequently security researchers do not follow responsible disclosure guidelines. They go directly to the press with new vulnerability information instead of first approaching the vendor. In other words, zero-day information (when a vendor has not had an opportunity to find out about the vulnerability and to release a patch or other mitigating information related to the vulnerability) becomes public knowledge, and adversaries may use it to their advantage. Unfortunately, this behavior cannot be easily controlled. Vendors would like to have an international information sharing network in place that is actionable and applicable.

4.4 Research Opportunities

As a result of the themes discussed in the workshop, participants identified the following research opportunities:

4.4.1 Configuration Standards for CPS

An important area for research is developing configuration standards for control systems and CPS in general. Workshop participants noted the lack of standards for security of CPS. More guidance is needed on how to correctly deploy and configure individual components of a CPS in specific environments, as behavior of any single component may vary based on the environment where it is deployed.

4.4.2 Detection and Mitigation of Vulnerabilities

Detection and mitigation of vulnerabilities in CPS is currently an underdeveloped field. We cannot rely on rule-based (a.k.a. signature-based) techniques for detection. We must employ a combination of various techniques, such as artificial intelligence and machine learning in order to detect security issues in CPS. This is where having standard taxonomies and modeling / formalization of physical-world systems would greatly help us. For example, we would like to use machine learning to understand what state of a system causes it to be vulnerable. We must recognize the difference between current familiar models (e.g., cyber security of networks and operating systems) and CPS. Surveying industrial control systems could provide insight toward that end.

4.4.3 Managing Risk of Threats and Vulnerabilities

New research will help provide guidance for managing risk of threats and vulnerabilities in CPS. Risk management is well understood for non-CPS, but there is a significant lack of understanding how multiple complex CPS work together. We must learn how threats in one part of the system could affect other components and the system as a whole. Assistance is needed with ranking and understanding how vulnerabilities and threats impact a system in a specific environment. We need to be able to extend current reporting systems / mechanisms to make this task easier.

4.4.4 Visualization Tools for Modeling Risks

We propose research to establish visualization components that support various models of CPS. It is hard to visualize and understand diverse complex systems that consist of a large number of interconnected components – especially which components influence other components, and how to properly conduct threat analysis and risk assessment for the system as a whole. Visualization tools could provide a way to get a better understanding of the system and its interactions. Visualization tools can also assist with analysis by representing vulnerabilities and threats in specific environments, as severity of vulnerabilities and threats greatly depends on exploit opportunities specific environments. Also, such tools could assist with understanding how threats can propagate across different domains by factoring relevant deployed environments.

4.4.5 Best Practices for Sharing Vulnerability Data

Participants also recommend research on best practices for sharing data about CPS security. Organizations are generally reluctant to release information on vulnerabilities in their products. Part of it is lack of trust that the release information can be contained and will not get into the wrong hands.

5.0 Working with What We Have: Securing the Base

Presenters: John Cusimano, exida Consulting; and
Glenn Feidelholtz, Department of Homeland Security

4 April 2013 in Gaithersburg, Maryland

Abstract

Given the complexity of most cyber-physical systems (CPS) and the safety concerns, CPS do not lend themselves to the rapid upgrade cycles of traditional IT systems. However, the threat environment changes as rapidly for CPS as for traditional IT systems. This workshop focused on identifying current tools, practices and techniques for securing current systems, their limitations and gaps.

5.1 Definition of Cyber-Physical Systems

CPS use computer networks to integrate sensors, processors and actuators to form a system that is able to sense, interact and perform real-time control of objects in the physical world. For example, CPS have the ability to stop or start devices (e.g. motors, pumps, lighting, engines), open or close items (e.g. doors, valves, gates) and move objects (e.g. conveyors, rudders, switches). Because of their ability to interact with the physical world they have the potential to cause physical harm to objects, living organisms and the environment. In many cases, these systems perform vital or mission critical functions that if disrupted can lead to large scale interruption of basic services such as energy production, power generation and distribution, transportation, etc.

Examples of CPS in critical infrastructure include:

- Industrial control systems (ICS)
- Building automation systems
- Transportation systems (avionics, rail, automotive, etc.)
- Locks / dams
- Medical Devices
- Electronic security / access control systems
- Emergency management systems

5.2 Industrial Control Systems

Industrial control systems operate the critical infrastructures throughout the United States. They typically have a network architecture comprised of sensors, controllers, actuators, routers, modems and switches. The current and more state-of-the-art systems may have additional defense layers such as an intrusion detection system / intrusion protection system, demilitarized zone and other tools to prevent, detect and mitigate in response to cyber exploits and malicious intrusion attempts.

Currently, the concept of ICS security for CPS is rapidly changing. The idea that air-gapped systems exist is quickly fading away. Integration of wireless and remote technologies, processes and capabilities are enabling cost reduction and increased operational efficiencies. However, with these emerging technologies come increased cyber security risk and vulnerability.

An adversary that successfully attacks an ICS may have the capability to affect the integrity and availability of the operational data of the plant resulting in malfunction or shut down the systems. Depending upon the sector and scope / scale of the cyber attack upon the physical equipment, there may be loss of life and significant consequences.

5.3 Challenges in Securing CPS

1. CPS are more vulnerable to cyber security breaches today than they were in the past for several reasons.
2. The first reason is the rapid adoption of commercial off-the-shelf technology and protocols.
3. The second reason is the ability to integrate CPS across facilities, across companies and even around the world.
4. The third reason is that remote access for support and operations from anywhere in the world is now expected functionality.
5. Information on how to use CPS systems is readily available these days to anyone with an Internet connection. Chat rooms, blogs, and various websites are available to provide even the novice with a great deal of information on the actual use of CPS; even information like default passwords for most products are available online.
6. Another challenge is that most CPS were designed for functionality, not security. Cyber security concerns are a relatively recent concern that most CPS manufacturers didn't factor into their product development requirements until recently. For example, most CPS use inherently insecure protocols such as MODBUS.
    - Industrial manufacturers often have a goal of enhancing economic efficiencies in their plants. With this, there is a focus of using mobile devices and wireless technology to achieve this end. Although remote

access may improve the productivity of workers and improve efficiencies of collecting and analyzing data, the critical infrastructure sectors may be susceptible to a host of vulnerabilities due to external connectivity.

- Other challenges identified in the workshop include:

7. Threats are more sophisticated and attackers have better tools that are readily available over the Internet.
8. Legacy Products.
    - Lifecycle of lots of products is designed in terms of decades with long-term update cycles.
    - Vendor may have gone out of business or merged with another company; or the vendor's suppliers may be out of business, no longer produce required components, or may have merged with another company.
9. Change management restrictions (ex. FDA valid).
10. Trust authentication.
11. Continuous operations.
12. Lack of training.
13. Patch / anti-virus update cycles.

5.4 Existing Guidelines and Resources

In recent years, many organizations have collaborated to develop standards on cyber security for control systems. Today there are several major cyber security standards in place that are being used in several industries. The following are brief summaries of some of the most prominent standards.

5.4.1 NIST Special Publication 800-82.

The "Guide to Industrial Control Systems (ICS) Security," was published in June 2011, by the National Institute of Science and Technology (NIST) as Special Publication 800-82. This standard provides comprehensive control system security guidance. While this standard / guideline was specifically prepared for use by U.S. federal agencies, it may be used by nongovernmental organizations on a voluntary basis.

5.4.2 ISA 99 / IEC 62443.

In 2002 the International Society of Automation (ISA) began writing a series of standards entitled ISA 99, which address the subject of cyber security for industrial automation and control systems. The standards describe the basic concepts and models related to cyber security, as well as the elements contained in a cyber security management system for use in the industrial automation and control systems environment. They also provide guidance on how to meet the requirements described for each element.

One technical report and three standards have been released so far with the most recent being ANSI/ISA-99.02.01:2009 entitled, "Security for Industrial Automation and Control

Systems: Establishing an Industrial Automation and Control Systems Security Program." This useful document is focused on control system security practices for owners and operators of industrial automation systems.

TC 65 WG 10 of the International Electrotechnical Commission (IEC) has joined with ISA 99 and will publish IEC versions of the standards under IEC 62443. There are currently two documents published in the series. One is IEC 62443-2-4, which is the IEC equivalent of ANSI/ISA-99.02.01:2009.

Over the next few years, these standards are expected to become the core standards for industrial control security worldwide.

5.4.3 NERC CIP.

The North American Electric Reliability Corporation (NERC) is responsible for writing and monitoring compliance with numerous standards devoted to protecting the reliability of the North American bulk power system (i.e. "the grid"). The Critical Infrastructure Protection (CIP) series of NERC standards primarily address security measures with the majority of documents focused on protection of "Critical Cyber Assets."

The NERC standards are mandated by law in the United States by the Federal Energy Reliability Center (FERC). In Canada, each province has the responsibility to review and adopt or create a provincial version of the standard. For example, in Alberta the Alberta Electric System Operator (AESO) is mandated to carry out the compliance monitoring function for the Alberta Reliability Standards. AESO has been working to adopt the (NERC) reliability standards as the Alberta Reliability Standards. Many reliability standards have already been adopted in the province of Alberta while others are in various stages of undergoing rigorous review by the AESO.

The NERC CIP standards have been evolving rapidly based on feedback from operators, findings from audits and to address remaining FERC Order 706 directives. Version 1 was approved by the NERC Board of Trustees in 2006, Version 2 in early 2009, Version 3 in late 2009 and Version 4 in early 2011. Version 5 is currently under development. While most stakeholders agree the updates provide necessary clarification, the rapid changes are making it difficult for regional efforts, such as AESO's, to keep pace.

5.5 Key Findings and Discussion from the Workshop

The responsibility for protecting CPS from cyber security breaches is shared between the owners and operators of these systems and the companies that manufacture them. Governments, standards bodies, industry organizations and private consultants are able to provide assistance.

5.5.1 Asset Owners.

There are seven basic steps that the owners and operators of CPS can follow to secure their systems:

- Understand / assess risks.
- Define cyber security policies, standards and procedures.
- Train personnel in OPSEC and grow a security culture.
- Segment networks (Defense in Depth).
- Control physical, logical and remote access to systems.
- Harden systems.
- Monitor systems for intrusions and maintain security controls, have incident response plans and methodology, and contingency plans.

5.5.2 Vendors and Suppliers.

There are well established strategies and techniques that automation suppliers can employ to discover and mitigate security vulnerabilities and improve the inherent security of their products. Learning and adopting these strategies will allow suppliers to better serve their customers and stay ahead of security researchers who aim to expose their flaws.

Software Security Assurance (SSA) is the process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability or misuse of the data and resources that it uses, controls, and protects. SSA is best achieved by integrating security into the software development life cycle (SDLC).

Vendors and suppliers are encouraged to adopt a lifecycle approach to ensuring that security is built into their products and systems.

Other tactics that vendors and suppliers can adopt include:

- Cyber security fuzz and abuse case testing.
- Cyber security certification (e.g. ISASecure™, Achilles™, Common Criteria).
- Documenting application guidance and configuration identification.
- Secure the supply chain.
- Vulnerability management.
- Adopt / support standards.

5.6 Research Opportunities

The workshop participants identified several study areas for the U.S. government, and particularly NIST, related to improving the understanding and security of CPS.

5.6.1 CPS Taxonomy.

Develop a CPS taxonomy, which focuses on the major cyber threats, vulnerabilities, and consequences and mitigation measure linkages.

5.6.2 Cyber-Physical Models.

Develop cyber-physical models to quantify the impacts of potential cyber attacks upon essential equipment.

5.6.3 Reference Implementations.

Develop good reference implementations for CPS.

5.6.4 Best Practices.

Provide guidance on best practices for cyber security of CPS.

5.6.5 Consolidate Standards.

Consolidate standards to help CPS owner / operators and manufacturers to comprehend the overwhelming and overlapping amount of material available today.

5.6.6 Provide Incentives to Owners / Operators.

Incentivize owners and operators of CPS to voluntarily comply with industry best practices and standards.

5.6.7 Provide Incentives to Manufacturers.

Incentivize manufacturers of CPS products and systems to have their products independently tested and certified for cyber security.

5.6.8 Government Should Lead by Example.

Government agencies should lead by example by purchasing cyber security tested and certified products and software to secure their own systems.

5.6.9 Education.

Offer CPS cyber security education at the high school, trade school and university level.

5.7 References

IEC 62443-2-1 ED. 1.0 EN:2010, “Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program”, 2010. http://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

ANSI/ISA 99.02.01-2009, “Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program”, 2009. http://www.isa.org/Template.cfm?Section=standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=10243

IEC/TS 62443-1-1 ED. 1.0 EN:2009, “Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models", 2009. http://webstore.iec.ch/webstore/webstore.nsf/Artnum_PK/43215

ANSI/ISA 99.00.01-2007, “Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models”, 2007.

6.0 Buying the Black Box: Security in Acquisition and Implementation

Presenters: Mike Baldi, Honeywell Process Systems; Blaine Burnham, USC/ISI; Emile Monette, U.S. General Services Administration; and Scott Sanders, Sacramento Municipal Utility District (Author)

4 April 2013 in Gaithersburg, Maryland

Abstract

The traditional idea of a black box is one where knowledge of the inner workings is unknown by the acquirer. The acquirer is merely purchasing hardware and software that is preconfigured for a specific purpose. These systems have been traditionally referenced as appliance-based solutions or may be seen merely as a service. While the acquirer may be provided a limited interface to make settings changes, they will not be provided any details about the actual manufacturing, hardening, or build of the black box. During the workshop covering cyber-physical systems, the concepts and concerns regarding the acquiring and implementation of the black box was discussed with a wide variety of stakeholders. Participants identified six significant themes related to black box acquisition and implementation practices and processes.

6.1 Problem Definition

With the increase in concerns related to cyber security and supply chain manufacturing; the idea of a true black box may no longer exist. Vendors remain reticent to provide acquirers any details of their black box in fear that their intellectual property may be disclosed and ultimately their market share jeopardized. Many vendors only provide white papers or discussion about the functions of the black box.

In contrast to vendor concerns, a 2011 report from Symantec, a large antivirus and malware vendor, reported nearly 5,000 new publicly released vulnerabilities in that year. While this was a decrease from the 2010 number of nearly 6,300, industry remains vulnerable to exploitation. It is unknown how many vulnerabilities exist because not all are published [Symantec, 2012]. As part of efforts to implement President Barrack Obama's Executive Order on Cybersecurity, the U.S. Department of Homeland Security (DHS) will be making more vulnerability information available to industry representative owners and operators of critical infrastructure. However, in a recent article, security vendors like Qualys argue that DHS is not going far enough. The truth of the matter is that knowledge of vulnerabilities can be seen as a commodity and an upper hand in potential cyber

warfare. Qualys, a large vendor in the vulnerability assessment marketplace, argues that to play sufficient defense, there must be a wider release of known vulnerabilities. Additionally, since the DHS is planning to release this limited information only to the owners and operators of critical infrastructure that are deemed most important, there is a greater chance that smaller businesses will be adversely affected and become greater targets of attackers [CSO Online, 2013].

During the workshop covering cyber-physical systems, participants identified six significant themes related to black box acquisition and implementation practices and processes:

1. Lack of definition of what security is.
2. Lack of ability to quantify security and risk.
3. Lack of definition of composability and the ecosystem of security across a trusted system.
4. Lack of practices to assure integrity of components through conformance assessment practices.
5. Lack of understanding and participation between vendors and acquirers in terms of capabilities and secure configuration.
6. Concern with vendors who only provide secure solutions when a sufficient number of industry acquirers actually start requesting and paying for security.

The balance of this report examines each of these themes identified and discussed in the workshop.

6.2 Lack of Definition of Security

Participants agreed that there is no consistent definition of security. While there are many standards, guidelines and practices that are published by national and international authoritative sources, there still is no uniform understanding about "security." Consensus by participants was that industry, vendors, academia and government define for themselves what security means within their operational domains.

6.3 Lack of Ability to Quantify Security and Risk

Another strong discussion covered the lack of ability to quantify security and risk. Participants said that metrics are inconsistent for evaluating and quantifying security – and ultimately risk. In many cases, black box acquirers are blindly accepting unknown risk because their acquisition practices transfer expectation of security implementation to the vendor community. Metrics for businesses to quantitatively assess cyber risk are inadequate or unknown. Many businesses focus on the "business requirements"; these translate to functionality and do not weight cyber security as an equal component.

6.4 Lack of Definition of Composability and the Ecosystem

Composability is the idea that as you glue together multiple systems and interfaces, there is an ongoing requirement for the independent security architectures to remain trustworthy. During acquisition and implementation of new technology, many vendors will pitch a single "system" that is really a conglomeration of multiple vendors' products. Moreover, within the technology industry it is very common to see larger vendors acquire smaller niche product companies to enhance their overall product saturation. Both of these practices lead to security concerns about the integrated security model and the reliability of security posture factoring the newly acquired black box "system."

6.5 Lack of Practices to Assure Integrity through Conformance Assessment

While it is a recognized practice of security professionals to perform regular vulnerability assessments, the practice of assessing conformance of security requirements against recognized cyber controls may not be as common during acquisition. In many cases this is not done because vendors are responding to business requirements that relate to functionality and are not being presented with actual cyber security requirements for testing. One critical infrastructure owner and operator participant discussed their practices of requiring a "System Security Plan" as part of every technology project. However, it seemed this was less of a norm among different industry representatives. Some vendor participants said that adding conformance assessment as a component in acquisition will raise the cost of the acquisition to the acquirer.

6.6 Lack of Understanding and Participation by Vendors and Acquirers in Terms of Capabilities and Secure Configuration

There was a perceived disconnect between vendors and acquirers related to implementing security capabilities. Participants said that during the deployment stage, vendors may not implement secure configurations because the acquirer did not explicitly ask to have those settings enabled. The discussion returned to the issue that vendors are implementing functionality and not necessarily security. The acquirers said they have not implemented or required conformance assessments to verify that the implemented system is configured securely.

6.7 Vendors Only Providing Secure Solutions When Industry Actually Requests and Pays for Security

Vendors said there is a cost to providing security even if it is the right thing to do. Concerns were expressed that vendors risked potentially losing market share because acquirers may not be willing to pay a higher price for a more secure solution. Additionally, acquirers may not recognize the more secure solution because the supply chain analyst is looking at the scores associated with price separate from a "security" score. Industry

representatives countered that there are commonly known best practices that all vendors can implement that would at least remove the easily exploitable vulnerabilities. The costs associated with implementing these practices may not be as significant as some other security practices. If all vendors ascribed to their implementation, costs would be normalized.

6.8 Research Opportunities

As a result of the themes discussed in the workshop, participants identified the following short term, mid-term and long-term research opportunities:

6.8.1 Short-Term Research

Evaluate practices to engage the supply chain function to understand the role of security during acquisition and implementation. Within the supply chain function, there needs to be development of reusable security requirements and the inclusion of specific and evaluated security procurement language. Additionally, as a component of unified risk determination, researchers should attempt to develop and define a uniformed threat landscape that can be used to quantify the level of black box "security." Is security the same as resiliency? How much resiliency is enough to say the black box solution is secure?

6.8.2 Mid-Term Research

Using the definition of security and understanding of resiliency, evaluate the risks of ensuring a trustworthy and composable security ecosystem. Evaluate what practices can be used by vendors when they are presenting a system of systems and what practices can be used by acquirers to ensure that the whole system can be trusted as a single architecture. A report was issued in 2004 under the DARPA Composable High-Assurance Trustworthy System (CHATS) program that covered a portion of this concern [DARPA, 2004]. What factors of reliability, performance, survivability and assurance are necessary to ensure trustworthiness for black box systems?

6.8.3 Long-Term Research

The first phases of research should produce a consistent definition of security and resiliency, specific procurement language, and an understanding of what makes for a trustworthy composable architecture. The long-term research opportunity is to integrate conformance assessment as a core component of the procurement life cycle. The practices need to protect the intellectual property of the vendor, but still provide sufficient demonstrable evidence to the acquirer that the vendor’s black box solution is secure. Is the conformance assessment process something that is initiated by the acquirer? Is conformance assessment something provided by the vendor during the requirements analysis? What level of detail is provided to the acquirer?

6.9 References

[CSO Online, 2013] http://m.csoonline.com/article/733557/experts-ding-dhs-vulnerability-sharing-plan-as-too-limited?utm_content=bufferdaca9&utm_source=buffer&utm_medium=twitter&utm_campaign=Buffer&mm_ref=http%3A%2F%2Ft.co%2FUZAgx5JJbh

[DARPA, 2004] http://www.csl.sri.com/users/neumann/chats4.pdf

[Symantec, 2012]. http://www.symantec.com/threatreport/topic.jsp?id=vulnerability_trends&aid=total_number_of_vulnerabilities

7.0 Enabling Trustworthy Operational Readiness: Making it Easier for CPS to Keep Doing the Right Thing

Presenters: Steve Kester, AMD; and Sean Smith, Dartmouth College

5 April 2013 in Gaithersburg, Maryland

Abstract

Cyber-physical systems (CPS) play an important role in keeping real-world infrastructure and systems working as intended – which is their purpose. As with any system, ensuring that CPS remain secure against action by malicious adversaries and can recover from failures requires that we consider how CPS remain secure *while* operating, as well as throughout the system lifecycle. This workshop brought together industry representatives from the IT hardware, software, and systems industries, and government participants from NIST, DoD, and other agencies to consider of the core concept of "trustworthy operational readiness." Participants discussed how to design, build, field, maintain, and sunset CPS technology to make it easier for them to remain trustworthy in practice.

7.1 Summary of Key Findings

7.1.1 Challenges for Trustworthy Operations

- Lack of automated process driven models for design and verification.
- Lack of risk mitigation processes.
- Lack of effective collaboration mechanisms in design and assurance.
- Few mechanisms to collect evidence of trustworthiness.
- Imperfect architectures and baseline models for operational correctness.
- Lack of mechanisms to generalize context-based security approaches.
- Imperfect understanding of the source and nature of vulnerabilities.

7.1.2 Some Approaches to Greater Safety

- "Designed-In" security practices.
- Improved certification.
- Improved security assessments.
- Improved vulnerability reporting.
- Improved process to collect best practices.

- Improved architecture: stripping down unnecessary features.
- Improved interoperability and legacy system management.
- Improved run time testing.
- Little understanding of economics of CPS risk and threat mitigation.

7.1.3 Key Areas for Research

- Security vulnerability and threat taxonomy for CPS.
- Security metrics for CPS, including lifecycle metrics.
- New approached to certification and verification.
- Run time trust evidence.
- Trust languages to improve design of secure components and protocols.
- Cross-domain security in CPS.
- Economics of security for CPS.
- Usability and use cases for CPS.

7.2 Background

Participants in the workshop noted that increasing threats and vulnerabilities for CPS in the defense, industrial and critical infrastructure space require new approaches to system and component-level design to enable trustworthy operational readiness. Owner-operators must have a high level of trust and assurance from suppliers, service providers and their supply chains that CPS infrastructure is designed to the required specifications and will operate as expected. In this case trust and assurance includes protections against targeted attacks, such as the infamous Stuxnet attack in Iran that can exploit vulnerabilities and cause substantial damage or otherwise compromise operations. It also includes protections against malware or other vulnerabilities including counterfeits. These may be introduced into a system or component during the design, manufacturing or distribution phases, as well as after CPS is deployed and maintained in the field. We need to focus on producing systems that are “secure,” and can generate evidence of their trustworthiness at run time and support trust evidence as a multi-way conversation between systems, infrastructure and stakeholders.

Given the increasing reliance on CPS in a wide range of industries and critical infrastructure services, such vulnerabilities and threats are unacceptable when measured in terms of safety and the potential economic, environmental and societal impact.

If we believe that complexity is the enemy of security, so the ever-expanding and evolving installed base of CPS for national security and critical infrastructure presents a challenge. How do we support global design, manufacturing and sourcing with trust and assurance at the levels necessary to protect CPS and ensure that the operators and computing environments can trust and rely upon them? While it is clear that there is no single “silver bullet” that can address all the threats and vulnerabilities facing CPS, there are models for traceable evidence of trustworthiness in the component and system design, manufacturing and deployment of CPS that can be improved upon to provide enhanced

assurance, verification and resiliency. The key is to identify the gaps and seek practical and extensible ways address them throughout the CPS lifecycle, from design, to manufacturing, field deployment and end-of-life management.

This report identifies challenges in ensuring trustworthy operations of CPS. It also defines areas of research and related topics that will enhance the security and resiliency of CPS for national security and critical infrastructure. Specifically, the paper considers practical, cost-effective means to "design-in" security-related verification and test processes, as well as product features or elements that can enhance assurance for product integrity and operation. Because timing is critical for securing CPS, this paper also establishes research priorities and identifies the specific next steps required to operationalize the research priorities for particular projects, funding options, and associated timelines. Finally, this paper also seeks to recognize the complexity of the global supply chain and realities of the global economy and workforce. A guiding principle for proposed research topics is that any potential solutions that are explored should consider the technical, financial and logistical challenges to enable practical solutions that can be economically produced and are likely to be widely adopted.

7.3 Defining Challenges to Secure CPS: Where Is the Attack Surface?

One of the challenges with securing CPS is defining where systems begin and where they end. Does the electricity grid begin at the point of energy generation, or the myriad of systems, subsystems, fuels, networks, and other elements that comprise a generation facility? Does it end with the electricity users, or are the countless others who are connected via computer networks, sensors, and distribution channels the end of the line? And what about maintenance? Power systems can't be "rebooted" without significant disruption, and an effective "hot patch" solution[2] may require more careful engineering. The productivity gains, service improvements and other enhancements created by interconnected CPS systems have delivered significant benefits, but they also create a complexity that is inherently unsecure.

The same is true for the global supply chains for CPS systems and components. Cost, manufacturing and distribution efficiencies have enabled large-scale adoption of complex CPS systems and the benefits they deliver, but they have also introduced considerable vulnerabilities at numerous points throughout the system or component life-cycle. CPS infrastructure is comprised of sub-systems and elements sourced across the world, often with a mix of commercial and custom parts, and sometimes without thought or record of provenance and verification. Even when assurance through tracking and verification are prioritized within a CPS supply chain, the veracity of that assurance is uncertain given the complexity of system components, dependence on third-party intellectual property, and proliferation of global design, manufacturing and distribution. Some, including recent

[2] See S. Bratus, J. Oakley, A. Ramaswamy, S.W. Smith, and M. Locasto, "Katana: Towards Patching as a Runtime Part of the Compiler-Linker-Loader Toolchain," International Journal of Secure Software Engineering, 1(3):1-17. 2010.

actions in the U.S. Congress, have pointed to domestic sourcing as an effective proxy for trust. Others have answered that even if it were possible to fully source CPS domestically, which it is not for most systems that depend on a wide array of electronic components, domestic location is not inherently secure. Recent events bear this out.

The relatively simple act of developing a comprehensive list of the potential risks to CPS is elusive as the risks are expanding and evolving as rapidly as new CPS technologies, use-cases, and interconnections and dependencies on other systems and subsystems. Further, the widespread and persistent reliance on legacy systems in CPS is a practical reality that cannot be overlooked. In short, the challenges are great, and are made even more so due to the pervasive complexity of CPS and increasing interconnectivity and dependency of other systems, networks, and supply chains.

It is important to also consider the contributing and supporting technologies. For example, secure source code can be undermined by insecure version control or by vulnerabilities in libraries and build tools (Who audits their libc code?). It's also important to not let the vendor perspective lead us to focus exclusively on the *production process* of the technology, and overlook the challenges that arise when it is *used*.

7.4 Characteristics of CPS

It is important to define the scope of the problem by delineating the characteristics of CPS that make them distinct from other areas where similar security techniques can be applied. We can distinguish several such characteristics:

7.4.1 Lifecycle.

In many cases, CPS security features are intended to last for the lifetime of the system, which can span a few years or even 2-3 decades. During this period, technologies and nature of the attacks change, and it is important when designing a trust mechanism for CPS to ensure that it is compatible with the lifetime of the system and that it could be replaced or recovered if a catastrophic event takes place. Differences in context between different classes of CPS make it difficult to design security features that apply across the board.

7.4.2 Accessibility.

In many cases, security mechanism in CPS cannot be replaced (or replaced completely) by users, including administrative users, and the manufacturers or technology vendors may retain a role in managing some of the trust anchors.

7.4.3 Computing Resources.

In many cases, only limited computing resources are available to support trust features; these limitation need to be taken into consideration for design and management of trust features.

7.4.4 Priorities and Tradeoffs.

CPS often exist to serve a particular real-world, non-cyber context – and this context can lead to different decisions about what system behavior are important, and what the relative trade-offs are between security properties. For example, in the power sector, *availability* may trump *confidentiality*, and returning a somewhat-correct answer within 3ms may be far more valuable than returning a completely correct one in 10s. A stress on reliability might also lead to requiring the system to work in low-probability extreme cases (e.g., a major blackout), not just the average expected cases.

7.4.5 Invisibility.

Another characteristic of CPS is that the "cyber" portion is often invisible. We have seen cyber security network assessments be surprised at encountering a fleet of unsecured Linux machines that were cable TV appliances (hence not considered "computers"). We have also seen analysis of a CPS overlook how that the potential damage, if compromised, could reach far beyond that CPS. For example, attacks on smart meters with SDR could potentially reach beyond the power grid and bring down the cell phone network.[3]

7.5 Security Challenges in CPS

The goal of this section is to identify challenges that could form the inspiration for research projects to help compensate for current weaknesses, and close gaps that exist by designing CPS with trustworthy operations potential.

7.5.1 No Automated, Process-Driven Models for Design, Verification and Evaluation.

Many verification models employed by technology companies today do not fully consider the level of interconnectivity and inter-dependency of the modern computing environment. Some types of verification tools, design checking software, and other quality assurance tools, for example, may be well-suited to ensure adequate functionality, but they may not have been optimized to identify possible security vulnerabilities. This is particularly true for CPS systems and components with an extended life-cycle and those that are dependent on legacy systems and infrastructure that may exacerbate vulnerabilities. New verification models that can be adapted to technology and security challenges in CPS environments need to be developed. Because the context is so diverse and the technology space is so dynamic, these models need to be automated. Additional attention should be focused on identifying potential vulnerabilities and "threat-access points" in the design, verification and evaluation phases and addressing them with tailored solutions that can be

[3] Critical Infrastructure Providers Need to Consider Smart Meters Attack Risks (April 23, 2103). http://www.continuitycentral.com/news06735.html

automated. An automated process can introduce vulnerabilities, so the development of such processes should also involve a series of internal controls to reduce associated risk.

7.5.2 Effective Risk Mitigation Processes.

When a security issue is found in a CPS, the nature of cyber-physical systems makes it difficult to address mitigation, due to specific characteristics of CPS described above. Given the design of CPS and their need for certain levels of longevity, it is important to develop both risk analysis tools and risk mitigation approaches that are compatible with various context of the use of CPS. There is significant diversity in CPS, and some contexts have shorter lifecycles. But addressing design issues for systems with greater longevity remains a significant challenge that requires more research.

7.5.3 Collaboration in Assurance Processes.

Diversity of CPS contexts makes collaboration among the technologists from different areas important as they have different experiences and technology approaches that could be complementary across segments. Today, there are no mechanisms for such collaboration. The lack of knowledge about common design patterns to address shared security concerns is a challenge that will benefit from additional research.

7.5.4 Trust Evidence Collection.

How do we know that a CPS can be trusted? Examination of this problem needs to consider the various ways to garner evidence of trustworthiness at production time and at run time. There is a limited inventory of trust technologies in this area. What is evidence of trust in CPS? Could it be generalized or will it remain context-driven? What components are needed to prove that a CPS system can be trusted? Trusted computing has provided early approaches for certain classes of systems and security issues, but it is not always easily applicable[4] to CPS. Due to the architecture and limited computing resources available on many CPS systems, trusted computing approaches cannot be applied without adaptation. The Trusted Computing Group (TCG) is developing specifications to address implementations in new areas such as embedded systems, but this work is context specific, currently focusing on automotive applications. Greater participation of the CPS community representatives in TCG can help remedy the issue and create usable and interoperable standards faster.

7.5.5 Architecture for Easy Operational Correctness.

Can we develop architectures for CPS that intrinsically contain evidence of operational correctness and trustworthiness? What components do such architectures need to contain? One promising line of inquiry is using the developer intent semantics in standard executable/loader formats to constrain code and data actions to their correct, intended behaviors. These will inform technologists making changes or engaged in deployments on intended operations, making it harder for an adversary to bend operation in ways not

[4] E.g., see http://seclab.illinois.edu/trustworthy-cyber-infrastructure-for-power-tcip/attested-metering

intended. Defining common architectures for trustworthy operations is a challenge requiring attention.

7.5.6 Context-Driven and General Approaches.

A generalized approach is desirable from many points of view, but the reality is that there is no single solution at this time that works across contexts. The challenge in CPS is to develop a list of canonical design features for security in CPS and general purpose approaches to apply this library of features in different contexts. The development of such a standard requires collaboration among different expertise areas in CPS, and such collaborative mechanisms remain a challenge.

7.5.7 Domain-Specific CPS Constraints.

Solutions for real-world CPS require accounting for real-world constraints such as legacy networks (e.g., slow serial links for SCADA), limited computing resources, diversity of platforms, harsh environmental conditions, lack of physical security and lengthy refresh cycles. The challenge is applying new technology approaches in this diverse environment.

7.5.8 Origins of Vulnerabilities and Ways to Reduce Incidence of Threats.

Vulnerability analysis and associated threat and vulnerability metrics are considered, in all areas, as important foundations of building more secure features and safer computing environments. It has been difficult to create a framework that could dynamically capture and incorporate changes in technology, usage models and security environment. CPS, their diversity notwithstanding, represents a potential testing ground for new ideas in metrics and analysis. That’s due to their greater longevity and, in many cases, smaller inventory of available trust features as well as low computing resources.

In particular, the contrast between the quick emergence of new technologies and the relative stability of CPS engineering can lead to trouble. For example, security techniques that worked fine when SCADA had a dedicated serial line may fail when that line is moved to the Internet; moving from a well-understood platform to something where “hackability” is relatively untested (e.g., Zigbee) can also be problematic. The challenge is to marry the predominant architectures in CPS with the dynamic nature of threats in a public computing environment, or modify architectures in a way to make them more agile.

7.5.9 Understanding the Economics of CPS.

The pace of development of secure and trustworthy features and trust / security infrastructure depends heavily on economics in the environment. Part of the challenge is to ensure that the right incentives and right economic models are in place to support the development of trust and security. For CPS, the economic analysis is a new area beyond the elementary cost analysis, and there are few studies, other than simple risk analysis, that focus on the economic modeling for CPS security features and their long-term influence. Without such a body of work, it is difficult to approach the applications and understand the incentives necessary to spur growth of trust and security. Study of the

economics of security in the CPS context is crucial for the success in the adoption of CPS features.

7.5.10 Managing Third-Party Intellectual Property.

Introducing third-party intellectual property (IP) into a technology product comes with an element of risk, depending on the source, nature of the product, and supply chain of the third-party IP, and other security-related factors. In many cases, the purchaser or user of the third-party IP may not have access to the source code or design elements of the product, which means they may not know if it is tamper-free or if it is susceptible to certain threats or vulnerabilities. The so-called “black box” is a common feature in many Information and Communication Technology components and subsystems, and it means that the potential for risk is widespread. Currently, there are few solutions that can address the tension between the owner / producer of the third-party IP to restrict access to source code or specific design elements and the need for the purchaser to have assurance that a third-party IP product does not introduce, knowingly or unknowingly, new vulnerabilities or back-doors.

7.5.11 Realistic Trust Expectations for All Stakeholders.

Government, industry, end-users and general consumers need to have realistic expectations for trust as it relates to the risks, threats, and potential impact of cyber-attacks and intrusions. Stakeholders are right to expect that products, applications and services include reasonable measures to address common threats and vulnerabilities and metrics to represent these measures, but as higher levels of assurance are required, expectations must also be realistic. Creating realistic, but concise and broadly applicable metrics in the CPS space is a serious challenge. With the complexity of IT systems, applications and networks comes considerable security risks, but a difference between the risk expectations and the ability for security measures to meet those expectations may negatively influence system design, economic viability and other important factors. Therefore, it would be helpful for research to be performed to measure levels of trust that are expected by different stakeholder groups, and assess how these expectations may correlate with realistic levels of assurance and trust.

7.5.12 Cross-Talk Between CPS.

We need to make sure that a silo-focus on one CPS domain does not lead to overlooking how two or more domains may interact. Enhanced information sharing and collaboration are required to identify and manage cross-domain threats and vulnerabilities.

7.5.13 Trustworthiness in CPS is Difficult to Specify in Terms It Will Be Understood and Analyzed.

Stakeholders need to specify what “trusted” means, and translate between machine-generated “trust evidence” and their mental models of correctness. However, the lack of effective of tools for this process leaves much room for improvement.

7.6 Solutions for Improving Trustworthy Operational Readiness of CPS

This section proposes solutions to improve trustworthy operational readiness of CPS. Elements of solutions already exist, but they are not sufficient without closing the technology gaps. But some progress could be facilitated with existing technology and approaches. Solution ideas that could be implemented relatively easily or have been implemented are presented below.

7.6.1 Improved Certification Approaches.

A federal repository for leveraging certifications by others could be helpful. It could reference secure standards developments and certifications that companies would leverage to verify trustworthiness of vendor or code (ASA, ISO). Different contexts in CPS use different certification models. Could ideas for improvement be gleaned from certification schemes and best practices in other CPS areas? CPS is an interesting area for certification where we need to build durable systems that can resist new generations of attacks. A combination of certification and self-certification in tandem with new technologies could improve the general levels of security. In addition to certifications, audits are useful in some CPS contexts. The highly structured and collaborative International Standards Organization (ISO) approach of standards development could be used as a starting point, and new ideas could be collected to improve it in the context of CPS certification that would involve multiple industries and stakeholders.

7.6.2 Common Criteria Protection Profiles, Used as Building Blocks to Evaluate Third-Party IP.

The new approach outlined by NIAP and others for Common Criteria takes into consideration the context and expertise that goes into creating Protection Profiles and associated tests. Common Criteria evaluations could be one of the assessment tools for design features in CPS, but run time assessment as well as other aspects of trust are also important. Tools to create a lifecycle-based assessment of CPS, including third-party evaluation and self-testing, among other components, remain one of the strongest challenges to support trustworthy operations of CPS.

7.6.3 Challenge to Implement and Use the FIPS Mode.

The FIPS 140-2 certification process provides several levels of assurance, and applies to several types of devices (e.g., standalone vs. software-only). In practice, we have seen how the validation process can catch dangerous flaws before products are released. However, the FIPS process has several limits. The variations are insufficient to address all products we care about, but are too many for managers to comprehend. The FIPS process addresses only the “cryptographic module” and not the larger system in which it is embedded. And the process also only talks about the end product, and not the engineering and tool-chain lifecycle.

Turn “on” the FIPS mode for applications that need an easy quick solution. Many real-world vendors and users find that FIPS 140 validation can have the advantage of adding

assurance to many aspects of system security – but with the disadvantage of requiring features that don't match customer needs. This can lead to FIPS-validated products with a "non-FIPS mode" that customers actually use. (For example, one of us had to add DSA signature support to a product in order to get validation, but had to give the customer the ability to use RSA because that's what they wanted.) FIPS mode enables creating a more trusted environment for operations of a system. However, FIPS model doesn't exist for all environments and applications, and doesn't cover all operations that need to be trustworthy. Architecture and available computing resources in many CPS systems make it a difficult to turn off FIPS mode under current architectures and technology environments.

7.6.4 Improved Security Assessments.

Security assessments associated with some classes of CPS such as aviation are mature and have a time-tested history, but they have not fully addressed specific issues of trust associated with electronic systems in airplanes. The assessments focus on the correctness of implementation and do not address trust – even in the core systems with crucial dependencies. In other areas, such as smart grid, the need for security assessments is well understood but there isn't yet a shared view about the approach to be adopted in this area. The emergence of guidance documents in the US and European countries, as well as in Asia, is a testimony that the work is well under way. Similarly, in the automotive industry, interest in security has grown during the last several years. In some other contexts associated with CPS, work is just starting. Security assessments can include requirements for trusted elements in CPS, leading to a greater security levels. These assessments need more elements related to secure operations.

7.6.5 Improved Reporting of Vulnerabilities.

Third-party organizations (for a fee) could help identify vulnerabilities and help mitigate them. Academia could join forces with industry to create and conduct innovative tests to discover vulnerabilities. What can we do when vulnerability is discovered? A good process for mitigation in CPS could help in many ways. For example, threats evolve. Today's solution won't necessarily work two or three years from now. From the times of stationary clients with static IP addresses to the situation today, with the great diversity of technologies available as end-points and networks, new threats appear with new technologies, whether or not they are related to trust and security. CPS is relatively slow changing compared to other computing system, with a lifespan of 12-18 months and decreasing. But CPS is also a source of innovation in many of the contexts that are experiencing fast progress. The evolution of threats for systems that are innovative, but are designed to last longer than the average technology replacement cycle, is an area that needs careful study. It should consider different approaches to verification from initial design through operational phases.

7.6.6 Improved Process to Collect and Implement Best Practices.

Are suppliers and manufacturers following best practices for development and security testing? There are some best practices in assurance that apply across the board and some context-driven best practices. They are voluntary and frequently formulated as high-level approaches that could be interpreted in a different way. What could be done to ensure that best practices are understood in a consistent way, that they are followed, and that they are matched between various contexts of use in CPS, where applicable? Can we establish levels of security? CPS are composed of diverse technologies and trust contexts. The usage models and security models are also different. There are few initiatives where technologists associated with different types of CPS are exchanging information on best practices developed in their specific areas. Similarly, the technology community is only beginning to consider the need and feasibility of a coordinated standards framework that could cover trust issues in different areas of CPS. A few documents raising this issue, such as an ENISA report published in late 2012[5] have started to address this opportunity, but are limited to some aspects that are relevant to CPS.

7.6.7 Stripping Down Unnecessary Features to Eliminate Vulnerabilities.

As systems develop (especially in new areas), proliferation of features outside of the core functionality and interoperability requirements create potential for new vulnerabilities that are not thoroughly analyzed and well understood. Stripping unnecessary features creates an opportunity to eliminate some vulnerabilities. Analyzing security and trust outside of the core functionality, but among the features necessary to fulfill the requirements will increase the security and trustworthiness of CPS.

For example, standard engineering principles dictate that it is better to use an off-the-shelf, well-tested component than build one from scratch. However, we have seen how that principle can lead to using vastly overpowered kernels in CPS – which became insecure due to the vulnerabilities present in this extra, unneeded functionality. Developing robust off-the-shelf kernels that can be easily stripped down to the minimum required functionality is a promising research area. Indeed, some observers have touted that, for security, the smarter grid needs dumber components.

7.6.8 Improved Interoperability Beyond Authentication.

Interoperability among various components of CPS is important. So is their connectivity and interoperability with adjacent systems – management, backup, regulatory control, updating, and other depending on the context in which CPS are used.

What kind of attestation could be implemented, what kind of data can be exchanged to narrow the field of vulnerability and filter out “noise”? Research in this area could help tease out future paradigms early in the development of Trusted Computing technologies, attestation protocols and approaches created to exchange proof that a system is

[5] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/sci

trustworthy. Although the vision includes exchanging significant information about the health of system during operation, in practice, only limited information could be exchanged, due to the diversity of systems and availability of resources. Today, new ideas have emerged to permit the technologists to consider such an approach for complex data exchanges. CPS that are relatively static in some contexts provide an opportunity to evolve the field to produce, exchange and consume trust evidence that will improve trustworthy operations of mission critical systems.

7.6.9 Improve Run Time Tests and Accumulate Helpful Data; Ensure TPM Could Work in a Specialized Environment with CPS.

A major challenge is to create useful baselines that will provide critical information during the operations at run time without impeding the normal core functionality of a system. Creating and implementing trust parameters during run time is a very complex problem. Additionally, it will be necessary to produce, store, and exchange information acquired during operations in a trusted manner. The new generation of Trusted Computing technologies can provide one approach to addressing this issue. TPM 2.0 released in early 2013 is an inventory of commands that could be adjusted for different environments, including CPS, if technologists in CPS contribute to Trusted Computing work in their area.

Implement Trusted Computing Group IF-MAP. IF-MAP is one of the solutions used for control systems. Technically it works well, although there are some issues. It maps some aspects of device to device communication, defines the machine's security related metadata and can support an (optional) TPM. IF-MAP is a standard client/server protocol for accessing a Metadata Access Point (i.e. IF-MAP server). The IF-MAP server has a database for storing information about network security events and objects (users, devices, etc.). The IF-MAP protocol defines a powerful publish / subscribe / search mechanism and an extensible set of identifiers and data types.

7.6.10 CPS Security Models Developed on the Idea of DO178B – Certification of Avionics Software.

DO178B requires that software will perform reliably in an airborne environment, that it does what it says it will do and not anything else. It is approached from a functionality perspective, requires two-way traceability, provides for a secure, traceable design and production process, and is based on a risk management approach that seeks to capture every element of the supply chain, as well as every stage from design, production, implementation, maintenance, to end-of-life management.

7.7 Research Opportunities

As a result of the themes discussed in the workshop, participants identified the following research opportunities:

7.7.1 Define Security for CPS Programmers: Focus Security at Programmer Level So It Can Serve as Backstop for Those Who are Experts in Security.

In order to understand whether a program or a system operates as expected and can be trusted, it would be helpful to understand its intended functionality. With this information, one can compare software execution with the intentions of the authors, administrators who installed and configured the software or systems, or users who chose to operate the software for various purposes. Potentially, intention semantics could become an important element of user controlled privacy and security, providing a link between development and usage requirements that is missing today. However, this ideal state is far from reality. With no standard way to understand or express intended functionality, defining and measuring trust and integrity of the computing environment remains difficult.

Large scale efforts to define ontologies or expert systems demonstrate that complexity and ambiguity in semantic definitions are difficult to overcome. Thus, capturing intention semantics for consumer use of multi-functional devices and systems is likely to be too complex and too diverse to warrant a quick solution. But reducing the problem to the intentions of program developers is easier and may help.

If intention semantics could be defined, captured and used to annotate computer software, both the users and the developers can benefit. This approach might be applied to user interface designs, systems integration problems, communication protocols, and other domains. Moreover, the use of intention semantics can help overcome cross-domain trust problems and lead to decisive developments in this area. Finally, intention semantics could help resolve the composition problem for trust and security.

Intention semantics could lead to the emergence of a new language or set of expressions or an XML schema for describing such intentions. Such a language or schema could be used for cross-domain electronic processes and applications, as well as other areas like software verification. In order to be useful, a new language expressing intention semantics needs to be standard and simple. Alternatively, expressions of intention semantics could be added to existing programming languages, policy languages and communications protocols.

7.7.2 Developing Taxonomy of Risk and Policy Related to CPS.

Taxonomy would provide common terms and understanding related to CPS vulnerabilities and threats, as well as help identify specific risks and associated security levels needed for CPS from the national security, critical infrastructure and commercial / public enterprise perspectives. Including an economic analysis of the threats and associated security measures that might mitigate those risks would be useful in prioritizing mitigation efforts.

7.7.3 Define and Implement Evidence of Trustworthy Operations, Programming Languages, and Research to Determine Current Programming Language Paradigms.

A programmer's knowledge can significantly improve the identification of key program sequences requiring baselining and the manner in which baselines are constructed. In addition to describing an expected program control-flow, a baseline might include additional information defined by the programmer. Such information may act as "guard rails" to define the expected path of execution as it moves forward.

The question to be explored is how to empower the programmer in the baseline construction process. One can imagine a hierarchy of possible layers that might be considered in building program instrumentation: application organization and code structure, specialized libraries, programming language features, compiler features and binary annotation.

Of particular interest is programming language extensions or modifications. To illustrate, perhaps programming languages could be extended to include "hooks" for inserting custom control points to designate the start and finish of a baselining sequence, specialized support for particular language constructs, or assertions that are examined at runtime to generate trust evidence. High-level programming languages could require simplifications to reduce control-flow complexity and make runtime baselining more practical to implement. What are the limits of control-flow baselining approach for different program language constructs, programming paradigms and workload types?

Another possible approach to program instrumentation might be logic based. Applying concepts from linear temporal logic, or another runtime verification formalism, it may be possible to create a new language of trust for use in instrumenting program code. Logic statements could be used to construct baselines, to evaluate program execution within the runtime environment, and to generate trust evidence in various forms. Scoping rules and conflict resolution may be applied by conspiring runtime mechanisms or by the consumer of the generated trust evidence.

There needs to be a role for policy in program instrumentation. Can the expression of programmer intention include generalized policies that are examined within the runtime environment framework? What types of policies might be useful, how would they be expressed, and what are the scoping rules that govern their application? Research in the use of logic (e.g. Belmap logic) in defining conflict free policies, together with similar approaches to run-time logic-based evaluation could help overcome limitations in control-flow approaches.

These approaches leave room for the use of intention semantics in a variety of areas, from policy to resource allocation. The precise nature of the notation for intention semantics can vary with the different environments where it is used, but the standard representation is essential to ensure interoperability and facilitate the development of tools and ontologies.

These ideas need to be adapted for the CPS environment that has limited computing resources to expend on security and baselining. Such an adaptation could constitute a viable research project.

7.7.4 Define Ways to Obtain Evidence of Trust at Run Time.

In most cases, the user is not equipped to make a full judgment regarding the operating characteristics of CPS. "Trust evidence" defined in this context can play an important role in filling this gap. Trust evidence, as the term suggests, provides a canonical set of information and parameters for demonstrating trustworthiness during interactions with other components or systems in the computing environment. As an addition to authentication, trust evidence may provide a more nuanced approach to demonstrating trustworthiness that includes a potentially wide variety of factors surrounding a system and its operational software context. By assessing trust evidence provided by a system during operations, an appropriate threat posture can be formulated and maintained.

We can use the term *baseline* to refer to the expected control-flow behaviour for software executing on CPS. *Baselining* is the process of creating a baseline reference using a controlled execution environment. The key idea underlying system baselining is that while the system can be complex and the number of possible states and execution paths can be exceedingly large, in practice, critical execution sequences often follow predictable patterns. The baselining approach asks the question, “Can such predictability be captured and used to generate trust evidence for runtime environments?” A key challenge is the development of a framework for use in generating baseline information.

7.7.5 Generate CPS-Driven Trust Evidence and Analyze It for Decision Making.

By improving programming language instrumentation, we can turn trust evidence into a decision support mechanism, either in a machine-to-machine fashion, or with human assistance. Identify mechanisms to generate trust evidence without interrupting CPS operations and permit real time response. If we could create mechanisms for versatile and resource-economic baselining and generation of trust evidence in real time, we could also improve operational trustworthiness of systems.

7.7.6 Determine the Extent of Security Threats and Vulnerabilities Driven by Legacy Systems, the Economics of Replacement and Recommendations for Action.

The prevalence of legacy systems in CPS present significant vulnerabilities in that security is often piecemeal, non-interoperable or lacking entirely. Economics, of course, plays heavily into replacement schedules for CPS systems, as well as the prioritization of CPS updates and even routine maintenance. Assess the potential impact and associated vulnerabilities and recommendations for action.

7.7.7 Define “Safe Mode” for Critical Infrastructure.

CPS often operate in an “always on” environment, such as electric, water, transportation and communications systems. If attacked, shutdowns may come at an immense cost in terms of safety, economics, or operational efficiency. Developing a “safe mode” that would

permit means operations to continue safely while an attack is being addressed may be the optimal solution for certain CPS facilities or infrastructure.

7.7.8 Evaluate Consequences of Global Nature of the IT Supply Chain in CPS.

The global nature of the IT supply chain is well-known but the implications are not always well understood from a risk perspective. Additional research on the global IT supply chain as it relates to security threats and vulnerabilities would be useful. Understanding these implications is a serious challenge. Such research might include assessments of threat and vulnerability assumptions relating to the Advanced Persistent Threat viz. current capabilities, as well as threats and vulnerabilities that may not have been anticipated.

7.7.9 Predict Broad Vulnerabilities in CPS: Cross Talk Between CPS Contexts.

We can't look at just one CPS in its own domain, but must also consider security-relevant interaction between CPS owner-operators, suppliers and users, and how an adversary may get a CPS to cause malfeasance in areas other than its intended domain of applicability. We need to Identify interdependent, affiliated or otherwise connected CPS and the specific threats and vulnerabilities that cyber-attackers may exploit. Once the parties are identified, determine ways to support technical exchanges, such as the SAFECode model for software that could be applied using a consortium of companies that share information and develop solutions and common approaches.

7.7.10 Economics of CPS

Projects to define economic models and economics of CPS deployment as well as study of CPS economic issues in contexts where CPS are used are essential for achieving success in this area. Adjacent fields developed economic approaches as well as basic understanding of the incentives needed for success, but CPS lags behind in this area.

7.7.11 Usability and Usage Constraints of CPS

In order to successfully define technical features of future CPS, usability and usage pattern issues need to be studied, in context-specific and more general projects**.**

7.7.12 Define Metrics of Security or Trustworthiness in CPS.

Consider current industry standard measurements of security or trustworthiness to determine if they are adequate to provide assurance for CPS and components, or if new metrics or improvements need to be developed to better determine the levels of security or trustworthiness to address CPS-specific vulnerabilities or threats.

About the Cyber Security Research Alliance

The Cyber Security Research Alliance, Inc. (CSRA) is an industry-led, non-profit consortium focused on research and development strategy to address evolving cyber security environment through partnerships among government, industry, and academia. This effort was established in response to the growing need for increased public-private collaboration to address R&D issues in cyber security. The founding members of the CSRA are Advanced Micro Devices, Inc. (AMD), Honeywell International, Inc., Intel Corporation, Lockheed Martin Corporation, and RSA, the Security Division of EMC. To learn more, please contact us at (781) 876-8860 or visit www.cybersecurityresearch.org.