



A Survey and Taxonomy for Roots of Trust in Cyber-Physical Systems

Summary of Results

November 2014

About the Project

This pilot research project, sponsored by the Cyber Security Research Alliance, was designed to survey research connected to defining roots of trust for Cyber-Physical Systems (CPS) and draft a taxonomy and ontology of terms and relationships for hardware, software or firmware Roots of Trust in CPS. Results were provided for the domains of energy systems, transportation, and medical devices.

Roots of Trust are security functions in a CPS device or system that are implicitly trusted and constitute a foundation for integrity. CPS are devices used to physically manipulate critical infrastructure and a wide range of systems vital to well-being of citizens, businesses, cities, states and the nation. Roots of Trust are fundamental elements underpinning the dependability and trustworthiness of CPS, which are susceptible to cyber security breaches due to vulnerabilities in firmware and software and specific nature of their design and operations. One of the inhibitors of research in this area is the lack of common terminology and assessment of work in adjacent fields. This is due to the diversity of CPS contexts and the multidisciplinary nature of the field. As a result, best practices and research advances are not always shared and applied across relevant CPS contexts. The public availability of the CRSA project results will help ameliorate this situation and promote a community of practice in CPS security and privacy.

For each domain, the project surveyed the field, prioritized technologies, identified gaps, and defined taxonomy on the basis of this analysis, while also defining a common vocabulary and cross-cutting context for CPS, as well as a mechanism to detect gaps, promising technology developments, and the relationships among diverse domains. Results are made available in subsequent phases of research in this area addressing research gaps, research results, test and evaluation, and transition, adoption and commercialization. The outcome of this project will lead researchers to form multidisciplinary teams to investigate the best solutions in perspective of real-world trade-offs for protection, detection and response to cyber attacks on CPS.

Participants

In response to a Request for Proposal in 2013, the CSRA selected teams at George Mason University and Drexel University to conduct research for this study. Their findings are summarized below.

Results by Drexel University

Area of Focus: Energy Systems Security

Team Members: Spiros Mancoridis (PI); and Marcello Balduccini (co-PI)

As a critical infrastructure, the security of energy systems has received considerable attention in recent years, including new technology development, implementations, large scale deployments of technologies, and new regulations. Smart grid and smart metering represent important components, so issues related to their security and privacy have spawned considerable interest in the research community.

The Drexel team elected to leverage the considerable amount of research in smart energy, including domains of security and trust. Its research re-used approaches to security and privacy that have emerged within advanced areas – particularly to evaluate them for possible applications to other CPS contexts. The team believed it would be helpful to gauge work done in a very active field of CPS to understand relationships with other areas of knowledge, technology roadmaps, and potential gaps in previously adopted approaches.

The Drexel team built an ontology that permits technologists to look at the active domain of smart grid and smart energy in a structured way. The ontology also highlights connections within the domain and outside the domain to key technology areas. Further, the ontology helps identify potentially missing elements that should be added to short and long term research priorities.

The resulting materials were loaded into the Protégé ontology tool to create a working instrument for answering queries about the relationships and structures within the smart energy domain.

In summary, the Drexel team's approach used to build this ontology is extensible and can be re-used for other domains in CPS. The ontology provides a robust picture of technologies, tools, and actors in the smart energy domain as well as requirements for security and privacy in different CPS contexts.

Results by George Mason University

Areas of Focus: Transportation and Medical Device Security

Team Members: Arun Sood, Co-PI; Duminda Wijesekera, Co-PI; and Bo Yu, Research Assistant

The GMU team focused on the transportation and medical device domains, and implementations of roots of trust in these areas. The work entailed two stages: Defined structures forming domains of knowledge addressed in the report; and used these structures to build taxonomies and ontologies.

The GMU report describes methodologies used during the two stages of the work and presents findings. The resulting materials were loaded into the Protégé ontology tool to create a working instrument for answering queries about the relationships and structures within each domain.

Ontology descriptions highlighted key elements across diverse CPS models of top level structures in transportation domains. Examples of these elements include:

- Models of top level structures within the two domains
- Areas of use for root of trust terminology among the elements of device architectures
- Key requirements for security in CPS

Definitions are included for common elements in CPS security requirements and architectures. The researchers concluded that the views on security were substantially different in the transportation and medical device domains. Although similar objectives were intended, the focus and approaches had few similarities.

The resulting ontology permitted GMU team to answer queries on the implementation of secure elements of architecture. The ontology covers both security and functional objectives in the chosen domains and represents a template for a useful tool that could be used for enterprise engineering of CPS as well as strategic technology development roadmaps. A logical extension of the work could be the inclusion of coverage for metrics associated with CPS design and operations, and a proposal for such extension is included in the report.

In summary, the GMU report and the ontology provide a first look at cross-cutting security requirements and architecture features in two diverse and very different domains. The work produced by the research team is highly extensible and has multiple uses.

About the CSRA

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.

Our mission is to foster the research and development of game-changing solutions to critical cyber security challenges through effective partnerships among government, industry, and academia. For more information, visit our website at cybersecurityresearch.org.