Secure plug and play architectures for cyber-physical systems

A Position paper for the NSF workshop on cyber-physical systems
Prepared by
Jyh-Charn (Steve) Liu
Computer Science Department, Texas A&M University
College Station, TX 77843-3112

Summary
This position paper advocates research investment on the area of holistic security management for plug and play based cyber-physical systems (CPS). Plug and play plays a key role in the success of the personal computer industry, and numerous modular electronics systems. With well defined standards at each system layer, vendors can create hardware and software modules independently, and be plugged together to form a large system. From the functional design viewpoints, it is fairly straightforward to expand the plug and play concept from the computing software and hardware to CPS. However, contemporary plug and play architectures do not have security management designs, but only focus on resource management issues, e.g., resource type discovery, performance features, available services, etc.

With the increasing sophistications and functionality integrated into computing modules of CPS, they can perform computations and even execute decisions based on simple commands received from some high level sources. When the physical systems are the computing devices are tightly integrated in the new generation of CPS, it is of great importance that a CPS module can determine whether or not plug and play requests/demands are permissible. When a system is disintegrated, individual modules should also be able to take independent actions safely. Otherwise, high performance, high capacity CPS modules can be easily misused and result in significant harms.

Research in CPS security requirements
1. What are the three fundamental limitations of today’s cyber-physical systems?
   Limitation 1: There are no established threat models to characterize the security needs and the level of acceptable risks. The ad hoc assumptions made by various research efforts made it very difficult and costly to develop useable technologies that can obtain predictable effects.
   Limitation 2: Little is understood about the authorization and access control requirements in the current cyber-physical systems that can be readily expanded to the future generation of CPS that are expected to have much more distributed computing and management architectures.
   Limitation 3: Most existing public-private crypto algorithms still require significant computing power for embedded microcontrollers.

2. What are the three most important research challenges?
   Challenge 1: Develop versatile modeling techniques that can characterize the security threats of a broad range of CPS applications.
   Challenge 2: Establish benchmarking criteria and the “case bases” to support development, evaluation and testing of technologies.
**Challenge 3:** Identify the technology roadmap to support holistic design processes that incorporate functional and security designs in one framework.

3. **What are promising innovations and abstractions for future cyber-physical systems?**
   Many valuable lessons learnt from the fault-tolerant computing technologies are applicable to secure system designs. In fact, security and safety are two closely related issues, albeit they rely on very difficult solution technologies. The notion of “inherently safe/secure” design principle could be a permissible investigation approach for development of security requirements for the future generation of CPS.

4. **What are possible milestones for the next 5 to 10 years?**
   - Year 3: Reference security requirements, proof of concept benchmarks.
   - Year 6: Standardization of security requirements, “mature case bases.”

---

**Research in security management architecture of CPS**

1. **What are the three fundamental limitations of today’s cyber-physical systems?**
   - **Limitation 1:** Most current systems are based on separation of computations from sensors and actuators. Yet, one can foresee that much more computing power will be available to CPS modules due to tighter integration of sensing, actuation computations, and mechanical parts is expected in the near future. The existing hierarchical management architecture will be inefficient and inadequate.
   - **Limitation 2:** Most security management schemes are designed for large software systems. They become unusable or extremely inefficient for CPS types of applications.
   - **Limitation 3:** Lack of crosscutting analysis and design of different system attributes, including security management, to support plug and play, reconfigurable operations.

2. **What are the three most important research challenges?**
   - **Challenge 1:** Development of modular security management functions that can be interfaced with other modules, with their security attributes and behaviors reliably inherited and migrated.
   - **Challenge 2:** Light weight crypto methods (asymmetric key systems) with low computing costs, and minimal requirements for central authorities.
   - **Challenge 3:** Efficient key management techniques (with minimal central authority requirements.)

3. **What are promising innovations and abstractions for future cyber-physical systems?**
   Off-line authentication methods that have been developed by the crypto methods can be a viable approach to attack this problem. Most existing solutions are aimed for high value, high security requirement applications. They can be tailored for the security management of future CPS applications.

4. **What are possible milestones for the next 5 to 10 years?**
   - Year 3: Reference security management architectures, proof of concept algorithms.
   - Year 6: physical prototypes for simple CPS applications
   - Year 8: expansion to other applications
   - Year 10: broad deployment/commercialization