Challenges in Security for Cyber-Physical Systems

Dr. Clifford Neuman
Center for Computer Systems Security
Information Sciences Institute
University of Southern California
bcn@isi.edu

Abstract

The design of security for cyber-physical systems must take into account several characteristics common to such systems. Among these are feedback between the cyber and physical environment, distributed management and control, uncertainty, real-time requirements, and geographic distribution. This paper discusses these characteristics and suggests a design approach that better integrates security into the core design of the system. A research roadmap is presented that highlights some of the missing pieces needed to enable such an approach.

1. What is a Cyber-Physical-System?

The term cyber-physical system has been applied to many problems, ranging from robotics, through SCADA, and distributed control systems. Not all cyber-physical systems involve critical infrastructure, but there are common elements that change the nature of the solutions that must be considered when securing cyber-physical systems.

First, the extremely critical nature of activities performed by some cyber-physical systems means that we need security that works, and that by itself means we need something different. All kidding aside, there are fundamental system differences in cyber-physical systems that will force us to look at security in ways more closely tied to the physical application. It is my position that by focusing on these differences we can see where new (or rediscovered) approaches are needed, and that by building systems that support the inclusion of security as part of the application architecture, we can improve the security of both cyber-physical systems, where such an approach is most clearly warranted, as well as improve the security of cyber-only systems, where such an approach is more easily ignored.

In this position paper I explain the characteristics of cyber-physical systems that must drive new research in security. I discuss the security problem areas that need attention because of these characteristics and I describe a design methodology for security that provides for better integration of security design with application design. Finally, I suggest some of the components of future systems that can help us include security as a focusing issue in the architectural design of critical applications.

2. Characteristics

Among the characteristics that may be present in cyber physical systems are:

1. Input and possible feedback from the physical environment
2. Distributed management and control
3. Uncertainly regarding readings, status, and trust.
4. Real-time performance requirements
5. Wide-distribution geographically, with components in locations that lack physical security.
6. Multi-scale and systems of systems control characteristics.

Feedback and input from the physical environment means the existence of communication channels not typically considered, which need to be “secured”. This characteristic is one that is specific to cyber-physical systems. An attacker does not need to break into the computer to affect such a system, but could cause a coordinated series of physical actions that are sensed and which cause the system to respond in an unexpected manner. How one protects such systems from this kind of attack requires an understanding of the system and its response, not the typical computer security defense mechanisms.

While not unique to cyber-physical systems, large scale cyber-physical systems such as the power grid [2], involve management by multiple parties. The utilities manage their own parts of the grid (e.g. the local distribution network to their customers). Network operators such as CAL-ISO (the California Independent System Operator) may control interconnections between utilities, but the decisions made by CAL-ISO affect the power that is available and the actions that must be taken by the utilities, and failures or load imbalances by independent producers and local utilities will affect what needs to be done by CAL-ISO. Many of the changes that need to be made across the system as whole must occur increasingly on small time-scales, meaning automation of local actions based on input from other organizations in other parts of the system. The structure of such systems is one of federation, systems are interconnected and control is distributed, yet the final authority on local resources remains with the participant owning the resource.

Cyber-physical systems have real-time requirements. In the power grid, actions must be taken in distant parts of the grid to compensate for generation or transmission failures elsewhere. Failure to react in a timely manner will result in cascading failures and possible permanent damage to equipment. Over time, these interactions have become more complex, and require reaction on smaller time-scales, and this requires automated response, sometimes based on distant inputs from sensors and commands originating with other members of the federation (creating a requirement to assess trust in the input from other federants). The real-time requirement also presents a requirement for performance isolation: that overload of the system due to other system functions, not impact the availability of bandwidth or system capacity needed to meet the time-critical function.

Cyber-physical systems are often geographically dispersed, with components in the field where they lack appropriate physical security. Such physical dispersion also makes it difficult to physically reset, or reload the software on a compromised device. Security solutions in such an environment must be tied in part to resilience of the application in spite of such compromise, rather than focus solely on preventing compromise of the component in the first place.

Finally, cyber-physical systems may be multi-scale systems and systems-of-systems. The home automation network within a home is one system, with local control and monitoring of appliances, and power input and output (consider the nascent distributed generation model with solar panels and local energy storage from plug-in hybrid vehicles). It is also part of a utility wide system, where the utility can turn off a meter for non-payment, or safety reasons, and even send requests to home appliances to defer energy use (e.g. disabling air-conditioning during a power emergency for those customer that accept such control in exchange for lower rates, or less directly by communicating demand based rates to appliances and home automation controllers that make decisions locally about when to use power).

Since components in the systems of systems are necessarily part of multiple systems, with different ownership, management, and security requirements, what we once thought of as non-critical infrastructure can have critical consequences. Consider the home automation network again. More and more end users are connecting their home automation capability to the internet (myself included). While it might seem foolish to manage the control functions of the power grid through a low security internet connection, in some sense this has already happened through these home automation controllers, and it is unavoidable. Consider the bot-net composed of unsecured home-automation controllers that simultaneously cycle the power on major appliances (or even entire houses). Such a bot-net can generate traffic on inputs to the larger scale power grid and even control (though its stimulus) the response that will occur.

3. A Design Methodology

We frequently hear security experts (and the victims of cyber-attacks) calling for us to design applications for security, rather than adding it later. This call is often misunderstood, or perhaps it is misstated. What does it mean to design an application for security? To many it means we must think about the security requires of the application during the design, so that we include the necessary data and interfaces up front that will enable the application to use myriad security mechanisms such as encryption, authentication, authorization, intrusion detection, and firewalls. Unfortunately, that misses the point. Yes, providing the ability to use such mechanisms is important, but true security requires an even more fundamental integration of security in a way that will permeate the basic design and structure of the application itself.

The first step in designing a secure application, and this will be especially critical in the design of cyber-physical applications, is to understand what it means for the application to be secure. One needs to define the authorized and unauthorized information-flow, control-flow, and availability requirements of the application, taking into account the physical as well as the cyber consequences of a breach of any of these requirements.

These requirements should be stated explicitly as part of the design documents, and the data and communication architecture for the application must be designed to meet the requirements.

During the design, all communication channels within the application should be enumerated and analyzed to ensure that the information, control, and communications constraints are met. In cyber-physical systems, this enumeration must take into account a domain specific understanding of the physical and external-process channels that are part of the system. By physical channel, I refer to physical inputs from sensors, and external-process channels include the reactions by human operators of the system, or control activities initiated by outside parties based in part on data from the system under design.

Security failures in such a system will result either from an incorrect specification of the information flow, control, and availability requirements, or errors in the implementation (including software bugs) of the system based on such requirements. If we have the existence of an explicit specification of security requirements, it would be useful to develop better network, operating system, and middleware components that can enforce the specified constraints automatically as a second line of defense in depth behind the application specific enforcement of such constraints, and the traditional security mechanisms used by the developer.

4. Research Roadmap

There are several areas where research is needed to improve the security of such systems. Attention is needed on the hard problems, rather than on simply plugging holes, fixing bugs, and adding new defenses that react to new vulnerabilities. Security for such systems needs to be considered architecturally, not as a separate "security architecture", but as a secure architecture for the deployment of such applications.

Among the critical topics needing attention is security for federated systems. Critical cyber-physical systems are federated, and we require tools to model, assess, and enforce security and trustworthiness of system components that are managed in different organizational security regimens. We need is to better understand issues of trust in distributed computing systems, and in particular, to develop models of trust that support segregation of dependence for different functional components of a system. These trust models must not be monolithic, or even hierarchical, as different parts of a system must be able to achieve protection and provide availability for themselves, without a central point of failure or vulnerability. These trust models must also be understandable to designers and users cyber-physical systems, providing simple abstractions that parallel the physical and organizational dependencies that apply to such systems.

Work is needed on modeling the security implications of physical interactions in cyber-physical systems. Physical interactions with components of a system must be modeled as control and data channels. Security testing on testbeds such as DETER [1], and through other means, should model these physical interactions in addition to the purely cyber attacks. Such modeling of physical interactions is likely to be application domain specific, e.g. modeling the effect of phase imbalance on the power grid, or flow constraints within an oil or gas pipeline. A framework for integrating such modules and visualizing the effects of the physical aspects of such a system would be useful.

Security for sensors and actuators in the field (including components in the home) needs to be considered. Techniques for detecting tampering, and validating the inputs provided by these sensors is important to prevent these control inputs to the cyber-physical system from being recruited by adversaries (e.g. bot-nets). If we can't do this, a cyber-physical bot-net is a frightening possibility (I believe it is actually possible already).

Finally, we need to consider security as part of system architecture and application development. This is more than applying security solutions to the problem. The structure of data placement, system control, and monitoring of the system as a whole must consider the security implications.

Finally, we should be developing system architectures and system development tools that can take a specification of these control flows and apply them at the hardware, O/S, and network layers to provide strong isolation (both data isolation, control isolation, and performance isolation) within virtualized distributed systems that will run such applications [3].

5. Conclusion

Cyber-physical systems have additional security requirements due to the addition of physical control and communication channels, real time requirements, and their common application to critical infrastructure. If we are to achieve secure cyber-physical systems we must take security into account at the very start of the design

process for such systems, by enumerating the specific information flow, control, and availability requirements and ensuring that those requirements are met through all parts of the design of the system, rather than attempting to meet them only with add-on security mechanisms. We should develop design tools that will force developers to specify and meet such requirements. We should also develop operating system, networking, and middleware components that can separately enforce such constraints as underlying invariants within the system on which such cyber-physical systems are implemented.

6. References

[1] Terry Benzel, Bob Braden, Dongho Kim, Clifford Neuman Anthony Joseph and Keith Sklower Ron Ostrenga and Stephen Schwab, *Experience with DETER: A Testbed for Security Research.* Second IEEE Conference on testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2006), March 2006, Barcelona.

[2] Massoud Amin (EPRI), *Security Challenges for the electricity infrastructure.* IEEE Computer (Security and Privacy Supplement) Volume 24, Number 4, pp 8-10. April 2002.

[3] Arun Viswanathan, Clifford Neuman, *A Survey of Isolation Techniques* Information Sciences Institute, University of Southern California. February 2009.