Security in Cyber-Physical Systems

Wm. Arthur Conklin
Center for Information Security Research and Education
University of Houston
waconklin@uh.edu

Abstract

Information Security is a domain of IT that has a well developed body of knowledge, and a cadre of practitioners with significant experience in securing IT systems. Cyber Physical Systems (CPS) also has a well developed body of knowledge and a well trained cadre of professionals that have been successfully running systems for years. These are two separate groups that would benefit from working together rather than in a hierarchical management structure. Securing CPS is a new challenge as systems become interconnected. New technologies will be needed, but much can be gained from existing knowledge, if it is properly shared between these two groups. This paper examines this idea in light of previous security examples.

1. Introduction

Modern information technology systems act as a key integration element in today's information centric enterprises. Enterprises exist for the purpose of business related goals and the information technology systems enable efficient efforts in pursuit of those goals. Traditional IT security efforts have been defined around the triad of confidentiality, integrity and availability. What is often overlooked in this simplified view is that these three elements are neither mutually exclusive nor pursued in isolation, but exist in a particular balance as defined by the business needs of the enterprise. Cyber-physical systems have security needs as well, and the same triad can be used albeit with one cautionary note; the balance of the three elements may be different depending upon the nature of the information flow associated with the specific system being protected.

When one examines traditional security, confidentiality and integrity tend to take the front stage, with availability being afforded a role of lesser importance. This has led to the development of technology and controls that are driven by the need to protect confidentiality and integrity, even at the expense of availability. Simply trying to adapt these existing controls to the CPS environment is neither appropriate nor beneficial to the goals of organization.

The objective of an information security effort is to provide for the appropriate levels of protection of information and information systems based on their role in the enterprise. Just as an enterprise would not spend resources to protect information that has no value, they are expected to expend appropriate levels of resources to protect items based on their value to the enterprise. The protection is against specific threats for these information assets, threats which vary by asset. Confidentiality of secret military data has different protection profiles than the accounting system data in the same firm. One of these is based strongly on confidentiality and the other on integrity.

2. Cyber Physical Systems

Cyber-physical systems have very strong integrity and availability requirements. This tends to make these systems different than traditional IT systems in many enterprises. When the central IT security function attempts to protect these systems, the first response is to apply what they know and are good at, traditional IT security efforts. Unfortunately, this approach is laden with problems. First, it does not address the specific security needs of the CPS elements in the enterprise. Second, even if there is an attempt to communicate needs, the two communities, traditional IT and CPS, have different vocabularies and this hampers the passing of requirements and capabilities between the parties. Lastly, even if the central IT security function fully understood the needs and requirements, their traditional toolsets are

not equipped to provide solutions to achieve the desired levels of protection. This mismatch between central IT security efforts and CPS needs, whether properly communicated or not, has lead to a divide in which CPS does not trust security and security thinks CPS should "be reined in". This divide has created and fostered a gap in which the group with the best security knowledge is not communicating with the group that has specific security needs, i.e. the CPS group.

Cyber-Physical Systems (CPS) are systems where information technology is connected to, for the purpose of controlling, physical infrastructure elements. A recent NSF sponsored workshop on CPS brought together researchers from technology, business and social sciences to examine the future research needs in the areas of CPS [1]. One of the interesting findings and points of discussion was that the problems associated with the advancement, including security of, CPS rested not just in the technical domain, but in the people (sociological, political and psychological) and process domains. Solutions to security problems will also be impacted by these multiple domains.

3. Role of Training and Awareness

Training and education can address the differences between the two communities, security and CPS technical, and facilitate better communications. Awareness of this issue is beginning to spread, but comprehensive training and education programs to assist both communities in the communication of needs and capabilities is much more than simple awareness.

This issue has been previously addressed in most organizations, as central IT functions, including security, have had to learn to communicate with the business elements they support. When dealing with IT organizations, it is common to lose sight of the fact that they act in a supporting and enabling role in a business, but that the true goal is business related, not IT centric. When the financial aspects of brokerage and banks became online properties, this led to significant security and performance concerns from the business side of the enterprise. They viewed the business in very different term than the IT security folks and there were significant communication issues for most firms as they learned to integrate business critical systems into the IT realm. This same challenge exists with respect to CPS.

If one were to examine university programs in IS/IT/CS, one will find that the acknowledgement of the importance of business communications is a relatively new and growing topic, but that the programs are still significantly centered on IT/IS/CS principles without regard to the specifics of their enterprise objectives. Repeating the same survey, but looking for CPS specific information, would yield a much bleaker result. This needs to change as the age of IT Enterprise-CPS integration has arrived and education needs to properly prepare the future workforce. Development and dissemination of educational material is a time-consuming, expensive task, and much like typical project documentation – left as a casualty of budget and resource constraints. The result is a learn it as it happens path, one which has proven very expensive in enterprise ERP system integration efforts, and given the nature of CPS, would be wise to avoid in the future. So one clear effort required for secure CPS-enterprise integration is the development and dissemination of training and education materials. This will at least address future workers and management pursuing graduate education.

The second aspect of training and awareness is associated with the currently existing workforce, already in place and working on CPS. Waiting for a critical mass to either enter graduate school where they may be exposed, or waiting on new hires to bring new ideas – takes way too long to effect meaningful change in the near term. The solution is again awareness on the part of senior executives, which drives in-house training efforts designed to open the lines of communication and bridge the differences. This is not classroom training, but rather focused meetings designed to address this educational shortcoming of both sides; CPS and security personnel.

The content of these materials is twofold, foundational and then specific. The foundational elements are meant to address vocabulary differences between the communities and assist in the understanding of the rearranging of the priorities in the application of the triad. The specific elements are the "how do I secure it steps" which will depend on the best practices that have yet to be fully developed. These best practice elements are a challenge because 1) CPS elements are not designed to be secured across open networks, 2) the imbedded base is huge, preventing sweeping change-outs, and 3) the life of CPS elements is in decades, not years like traditional IT elements. This makes securing these systems challenging and makes the economic decision on security placement on the enterprise/network side of the house. What is stopping this from rapidly occurring is that the technology to provide the appropriate levels of protection does not exist, and

where it does it is still in its infancy when compared to other IT security elements in the enterprise. Just as there are no single silver bullet solutions in traditional enterprise IT security, there will be no silver bullets in CPS security solutions. A collection of tools, techniques, processes and procedures will aggregate over time providing the desired levels of protection depending on each system need.

Most of the current tools and systems used in traditional IT security systems were at one time a research project at either a corporate lab or university. The development of point solutions to particular problems began as niche solutions, which then grew into larger solutions through expansion of capabilities or aggregation of components. The same lifecycle can be repeated in CPS environments, there just has to become a recognized need and market to drive the innovation.

4. Government Roles and Responsibilities

Government can play a role is assisting all of the players in achieving CPS security goals. There are several steps needed to assist in the transition from today's weaker than desired security to more appropriate levels of security. First, is a recognition of the scale and scope of the problem. Like a morbidly obese patient, it is easy to identify the fact that the patient is too fat. The challenge lies in determining a safe pathway to achieve a healthy lifestyle without killing the patient. One cannot just cut out all the fat and expect the patient to survive. Even if you could, there were lifestyle choices that led to the condition and would result in a return to this condition. Four elements are needed to achieve this change.

1) Identify the scope, scale and cause of the current condition.
2) Identify the desired outcome in measurable terms.
3) Determine a path from the current to the desired condition.
4) Determine how to measure progress along the path.

These are huge policy related issues, for each has economic implications that are interrelated with other aspects of the systems that CPS operates in. Dictating an immediate solution, quick and "relatively painless because of time", may end up costing more to secure the system than the risk that the system was suffering under, leading to a suboptimal solution. Taking too long or ignoring the issue leads to the inevitable risk coming to bear on the system, again suffering avoidable losses. Finding an appropriate middle ground will be a herculean task, as many of the risk management elements are not well understood or properly rewarded in today's environment.

Government is quick to want to offer, one size fits all solutions to problems, including IT security. And this approach has rarely proven successful, and in the case of IT security, and acts such as FISMA, have proven not to lead to the desired results in broad scale. Addressing the four previous points cannot be done in one sweeping document. The scope, scale and cause of the current security condition of CPS will vary greatly by CPS system, and even within industries by element. NERC has spent considerable resources on defining standards for the electrical system, as has API for oil and gas and other industry groups. Each of these standards is tailored to the needs and vocabularies of an industry vertical.

5. Industry Roles and Responsibilities

Approaching this problem with blissful ignorance, one may wish to just go do it and get it over with. The challenge here is that determining the appropriate desired end state for CPS security is not easy and is hampered by lack of metrics in this area that can assist in the determination of appropriate levels of security.

We have been down this road before in traditional IT security. In many cases, the firms operating in the CPS space may not have had the luxury of this journey as experienced by their financial firm friends, but none the less, they would do well to learn from the lessons learned from the financial firms. I know of many people involved with CPS who have openly stated that CPS is different, and I agree that CPS systems are different and have different needs than other IT systems. Financial based IT systems are different as well, and yet they have managed to close the communication gap and find the solutions. Recent attacks against US Government and commercial websites offer evidence of the resilience of the financial sector [2].

As the web became part of business processes, it started with systems not being secured, with IT and business on different tracks, with communication issues between business and technologists. Business and IT have learned to work through those challenges. We have learned to secure our enterprise IT systems, and although we are not at the desired end-state, we are making progress towards those goals. We need to replicate this process, it is proven

to work and most have experience in it as it is an ongoing effort in most firms.

The important element to remember is that CPS is not the current business element and the relearning of many of the initial lessons of coming together with the business will need to be repeated. IT and CPS need to be given the time and resources to go through the same courtship process that occurred between business and IT. Just because one relationship was developed does not mean the second one will be any easier – in fact, it will be harder. And the matter is further complicated by the fact that some of the firms involved, including the people, have not been through the IT and business need courtship ritual, hence they are embarking on a new set of blind dates.

6. The Need for Balance

Trying to decide the specific technical solutions today, given what is known now is premature. The IT security industry needs to learn more about the specifics of CPS environment, the threats, requirements and drivers before we can assist in securing the environment. Successful information based security will only arise when all three key aspects of a system are secured; the technical, the people and the process sides. It is common for IT people, and academics to want to reach for a technical solution, and without some of the technical solutions that have been developed, there would be no hope. But in the immortal words of Bruce Schneier, "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

From a practical point of view, the four questions mentioned earlier provide a pathway. The first question, identify the scope, scale and cause of the current condition, is the starting point for action. This is a variation of "where are you now" and requires one to take a good look at the current threat level, anticipated threat levels of the future, what asset is at risk, and what is the exposure to the enterprise. Some assets may be of minor value and of no consequence, but the may expose the rest of the enterprise to catastrophic loss. A good way to begin answering this question is, for each asset you can identify, answer the following questions:

1) What are the risks/threats associated to this asset?

2) What security resources are in place to protect the asset, and how do they line up against #1?

3) What residual risks remain associated with the asset?

4) What overall level of risk remains accounting for all #3's?

Answering these questions will take considerable time, but when complete, you will have a solid idea of where you stand with respect to securing specific CPS systems, both individually and in the aggregate. It is important to consider not just technical issues ans solutions to the above questions, but to consider how people and processes play a role in CPS.

After determining where you are with respect to securing your systems, the next of the four questions comes into play. Question #2, identify the desired outcome in measurable terms, is a form of "where do you want to go". The qualifier, measurable terms is important, for merely stating I wish to be secure is not something that a team can go accomplish. To state I wish to achieve a level of security the prevents unauthorized entities for manipulating controls systems is measurable – simple count the number of unauthorized control system events per unit of time. Employing a form of intrusion detection system targeted to measure this specific aspect will do the trick. Measurements are both easy and difficult. It is relatively easy to pick operational metrics that can guide operators to measure effectiveness of a specific control. The challenge is in aggregating a collection of operational metrics and creation of a management metric that reflects the overall health of a section of the enterprise. This is one area of active research still in need of solutions.

Once you know where you are and where you want to go, what remains are the management functions of determining the correct path to follow and a means to measure progress. These aspects are just like the previous aspects, specific to the particular aspects of the problem at hand, in context with the environment of the enterprise.

7. Conclusions and Future Directions

The good news is, this is not our first child, we have already begun raising one, the finance industry, and have learned valuable lessons in the process. The bad news is, this is not our first child, and like many parents we will want to replicate what we did with the first one again. This might work at first, but as the child grows and discovers that blue is their favorite color, not pink, and that hand me down clothes from their older sister doesn't work when they are a boy.

This might seem trite and obvious, yet it is how many are approaching the CPS and IT security relationship. The security industry may know a lot about security, but there will be new technical lessons

from real world issues associated with CPS and ignoring them will not make them go away.

One key element that will mark success or failure will be in how the parties approach the relationship process. If the process is viewed as getting a second spouse, where affection will need to be split from the previous spouse, then competition and turmoil and favoritism will spoil the results. If the process is undertaken like having a second child, then as any parent understands, love is not a zero sum game, love for the second child does not come at the expense of the first, but in addition to it. Yes, time and resource constraints will always be an issue, but they can be managed. All it takes is awareness and leadership for this aspect of the problem.

Applying this philosophy to the CPS problem is relatively easy. Apply previous knowledge of security best practices to the new environment of CPS. And just as in security for enterprise systems requires that actions be applied to all three aspects of the system, people, processes and technology, this same requirement holds true in CPS. In enterprise systems, although there may be differences in terminology between financial systems, e-commerce and service based systems, commonalities and efficiencies have been discovered and capitalized upon. This same process will occur in the CPS realm as well.

Just as security metrics are a challenge for enterprise security efforts, they are a challenge int eh CPS realm as well. This represents an area that active research can be effective in advancing the state-of-the-art. Best practices have yet to be specifically determined and as CPS efforts advance, these will be determined through efforts of industry actions to secure their systems.

8. References

[1] Missouri University of Science & Technology and The Great Plains Network, in *Bridging the Cyber, Physical and Social Worlds*, Kansas City, MO, 2009.

[2] AP, "Federal Web Sites Knocked Out by Cyber Attack," in *Fox News .com*, 2009.