Visual Analytics in Support of Secure Cyber-Physical Systems

David Dittrich
Pacific Rim Visualization & Analytics Center
University of Washington
dittrich@u.washington.edu

Mark P. Haselkorn
Pacific Rim Visualization & Analytics Center
University of Washington
markh@u.washington.edu

1. Introduction

Homeland Security Presidential Directive 7 (HSPD-7) [1], released in 2003, firmly established the term *critical infrastructure protection* and directed action be taken to identify, prioritize, and address the vulnerabilities to the systems and services that have relevance to the American way and quality of life. Cyber Physical Systems (CPS) – are integral to the functioning of not only critical infrastructure (CI) sectors, but extend all the way down to the scale of the human body. Two of the more commonly discussed types of CPS are the Supervisory Control and Data Acquisition (SCADA) devices that are the subject of much media attention, and Industrial Control Systems (ICS). However, CPS encompasses far more than just SCADA or ICS systems. Other CPS applications include: automotive and aeronautic control; border traffic monitoring and radiation detection sensing; wearable devices used in health care (e.g., pace-makers, glucose monitors, and bionics); automated manufacturing; electricity generation, distribution, consumption monitoring, and energy conservation; water and nutrient control in agriculture. In short, CPS can include any computing device used in sensing and/or manipulation of the physical world, in real-time, by way of an interface to a physical object.

HSPD-7 assigned specific government agencies with responsibility for securing specific critical infrastructures, responding to attacks and disasters, and initiating cooperative response through a number of information sharing mechanisms including sector-specific *Information Sharing and Analysis Centers* (ISACs). The report of the Obama administration's 60-day review of cybersecurity policy [2] discusses the limits of what has been accomplished by government and industry since HSPD-7, and cites reports by organizations such as the Government Accountability Office (GAO) who have been evaluating the effectiveness of laws and regulations aimed at improving cybersecurity. The report stresses the need to build new, more effective public/private partnerships to both raise awareness of security vulnerabilities and to develop an integrated, action-oriented approach to ensuring "a trusted and resilient information and communications infrastructure." The 60-day policy review itself drew in part from recommendations made by the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency. [3] The CSIS report also notes the limited success to date in securing critical infrastructures, and while it calls for actions to secure ICS and SCADA systems (recommendations 11 and 12), it also focuses on finding new ways to secure networks, increase response capacity, and develop new socio-technical solutions to the problems of securing cyberspace.

All three of these efforts call for *effective* public/private partnerships, investment of R&D funding, and implementation of a trustworthy networked foundation in order to provide critical services to the public. As the CSIS put it, "the United States has begun to take the steps needed to defend and to compete effectively in cyberspace, but there is much to do." So what are the special needs of CPS security, and more importantly what are the new "socio-technical" solutions?

This paper lays the groundwork for new strategies to secure cyber-physical systems that are more pro-active, holistic, and require more collaborative partnerships among researchers, designers, managers, operators, and policy makers. The task will not be easy, but achieving the highest goals requires the greatest effort and commitment. While we must guard against *scope creep* into areas that fall outside of our ability to affect change, what is clear is that the interdependencies of the various critical infrastructure sectors require a more inclusive model. It is incumbent on members of all CI sectors to work more closely and cross-functionally in order to respond in a systemic way to attacks on one or more CI targets The motivation for trying to achieve a more collaborative response capacity cannot be more clearly put than it was by the CSIS: "losing this struggle will wreak serious damage on the economic health and national security of the United States."

2. Themes in CPS Security

Some CPS devices were originally designed to be used only on closed circuits, not connected to the internet in any way. This assumed only trusted parties have access to CPS interfaces, and that CPS devices are isolated both physically and logically from all other computers. Today, pressures to decrease operational costs by providing remote access to both employees and third-party support, combined with an increase in the use of CPS have driven some devices to be made

accessible from the internet or from wireless (WiFi) network access control points within range of unsecured public roads or buildings.

This changing networked world requires a re-evaluation of the concept of a *perimeter* and the realization that in order to facilitate the business of government via the internet, we need to employ meaningful controls and strategies short of complete isolation. Preventive controls are a first line of defense, but often impractical given required functionality. Thus, detective controls and analytical capabilities become an increasingly important second line of defense. At a meta-level, this second line of defense requires a framework that enhances local solutions without limiting local action, yet works within a framework that is designed to scale up to the national level. This framework has to support a collaboration among the various localized solutions that can be harmonized both horizontally across enterprises, and vertically through regional and national protective entities.

The first step is developing a strategic framework to establish the collaboration and promote research and development of tools and techniques addressing the "socio-technical" problems. The framework is the enabler for fostering advancement. A fundamental problem remains, however, that is central to achieving a trustworthy internetworked environment in which cyber-physical systems are deployed: dealing with the vast scale and scope of the data involved with these networks. We propose that no timely and effective awareness of the security state of the network is achievable without visualization and analytic capabilities that match the scale and scope of the data involved. These visualization and analytic capabilities, then, are integrated into the framework to continue to evolve at pace with emerging challenges.

What, then, are the major themes in CPS security that our proposed framework must address? The North American Electric Reliability Council (NERC) outlined the *Top 10* vulnerabilities commonly found in control systems. [4] They detailed foundational, intermediate, and advanced means of remediating these vulnerabilities. According to NERC, several major themes in CPS security must be addressed to minimize risk to control systems in the energy sector. Together, they illustrate how networked control systems differ significantly from normal IT networks. Some of these themes include:

2.1. Insufficient separation of CPS from other systems (defense-in-depth)

CPS devices too often share networks with systems unrelated to device control (such as general use desktops, laptops, print and file servers, etc.) If these general purpose computers become infected, they can begin to transmit hostile traffic that can disrupt control devices. This problem becomes even more acute when cost efficiencies drive organizations to switch from wired to wireless communications for all networking. This also increases the exposure of control devices to potential unauthorized use by the control interfaces being accessible from general purpose computers that may be infected by *drive-by download* attacks resulting from spam or malicious web sites. As more and more CPS devices are deployed, the challenge of supporting this highly-distributed network becomes ever greater.

2.2. Insufficient monitoring of access and use

While intrusion detection and intrusion prevention systems (IDS and IPS) are commonly used on large corporate networks, they are underutilized or their capabilities immature as deployed in the control system environment - especially those under public-sector management. The prevailing culture in the sectors with strong organized labor representation that employ CPS is *anti-monitoring*. That culture, combined with a lack of strong oversight and system management that might identify attacks or unauthorized access, increasing the window of vulnerability to attack. Mechanisms that enhance security oversight and controls, improve the ability to detect and respond early to threats against critical infrastructure, while also protecting privacy rights, are sorely needed.

2.3. The need for better coordination, education/training, and workforce enhancement

There is a general problem of a cultural gap between those who design control systems, those who operate them, and those who manage the networks to which they are connected. Without a shared sense of responsibility and shared goals, there are problems with creating workable policies, audit and enforcement mechanisms, and sensible procedures to involve employees in ensuring a trustworthy network overall. There is a clear need to foster research, workforce enhancement, and the education of tomorrow's professionals.

The issues above illustrate how CPS networks differ significantly from normal IT networks: they are less resilient to unexpected or unwanted traffic that occurs on the open internet, require greater isolation of their control interfaces from normal computer systems, and are not as actively paid attention to. NERC's report describes many ways in which a more sophisticated *defense in depth* strategy can be used, but as the President's 60-day review and the CSIS both stress, technical defenses are not enough: there *must be* a complementary focus on producing an agile, action-oriented approach to securely operating networks, combined with education and training to foster better engineering in the future and to build and enhance the existing workforce. These issues may be addressed through a creative combination of three elements: (i) the application of distributed access control and intrusion prevention technologies; (ii) the use of visualization and analytic capabilities, and; (iii) the integration of operations, R&D, and education/training. [5] This combination has never before been attempted on a national scale, yet has tremendous potential to be a *game-changing* strategy that scales well nationally (or even internationally.) One of the key aspects of this proposed new paradigm is moving beyond basic information sharing

into a more collaborative and dynamic mode by creating action-oriented alliances that leverage limited expertise across resource-constrained federal, state, and local government IT organizations in partnerships with the private sector.

The type of collaborative, action-oriented alliance proposed in this paper builds on the successful model established in 2004 by DHS with its Regional Visualization and Analytic Centers (RVACs), also known as Centers of Excellence (COE), at research universities across the United States. The charter calls for: R&D leadership [6]; technology evaluation and implementation; training and education, and; coordination and integration. The recently-formed Visual Analytics for Command, Control & Interoperability Environments (VACCINE) COE is an evolutionary result of the initial RVACs.

3. The Research Problems

The research problem is to identify the key relationships between the sources of operations data, and use them for both *daily functional operations* and *security operations.* By using the same visual analytic capabilities for both types of operations, the utility and efficiency of both functions are enhanced; when two separate systems are used, communication and coordination of activities breaks down, effectiveness of the system as a whole decreases.

Take the application of radiation and traffic monitoring at international borders as an example. The goal is to detect attempted breaches of border controls, or illegal import of nuclear materials, and interdict. Border agents rely on constant monitoring of the sensor network to alert them to breach attempts, or to control traffic barriers that seal vehicle ingress points. A reasonable engineering requirement is to alert if a sensor fails, communication is lost, or power is disrupted. But what if an attacker can temporarily disable or bypass the sensors by taking control of computing devices that share the same logical network, but are not part of the sensor network per se? Other computers, possibly unrelated to the CPS network, are often found on the same networks. They are none the less potentially capable of initiating connections to the CPS devices or control interface, and are thus potentially an avenue for attacking the CPS network. By expanding the concept of *system* to not only include the specific CPS devices and control interface, but to also include these computers and network devices that are in logical proximity, a more holistic sense of integrity and trustworthiness in the complete system can be achieved.

In terms of CPS, Human Machine Interface (HMI) displays provide a means for humans to understand the operational state of mechanical systems, and to allow them to monitor and mediate changes in the system when required. HMI displays are often designed to represent the physical system being monitored or manipulated as clearly and simply as possible. As the components of the physical system itself – the pipes, the pumps, the pressure gauges, the valves, etc. – do not change, the HMI display may simply be a static representation of the physical system. The only thing that changes within many HMI displays are indications about the state of the components and the system as a whole. In terms of the *security state* of the system – its availability for remote access and control, its integrity, and the confidentiality of the data contained within the system – there are multiple levels of logical structures that do not have direct analogs to the physical structures, and cannot be viewed using the same static HMI display. This results in a significant problem in terms of monitoring and controlling all aspects of the system's state in a coherent manner.

If existing HMI displays are an incomplete visual analytic solution, an effective solution must be able to handle multiple perspectives. It must allow the operator to seamlessly change perspective as needed to address different, but interrelated tasks. We will briefly look at some of these perspectives.

3.1. Physical relationships

CPS devices are edge nodes in a normal computer network. While they historically were connected via serial communications links similar to phone modems on early personal computers, today many of them use standard TCP/IP networking protocols that rely on standard ethernet, WiFi, fiber-optic, or other radio-frequency protocols (e.g., Blue Tooth or RFID.) These communication links may be normal authorized communications, or they may be hostile. The links themselves are almost as static as the physical system's connections as described in the last section. An HMI can show them in a similar way to display of the physical components, but the diagrams will be distinctly different in appearance. A research problem is bridging these two types of physical connection networks in ways that allow operators to understand how failure or compromise of devices external to the system being monitored (e.g., a network router) could affect the availability of the CPS device (e.g., the valve) and to act accordingly.

3.2. Logical communication relationships

As CPS devices are being controlled, there are implicit communication links from the HMI display (i.e., the control interface) and the CPS devices. If the HMI control interface is accessible from the internet, an attacker may be able to bypass the normal authentication mechanism and communicate directly to the control interface or CPS device through back-doors. Network flow monitoring can make these communications visible, but external information about which users are both authorized to access the system, but also which ones *should be currently working*, can help identify potentially hostile access to the system. A research problem is integrating external physical security authentication information, work schedules, task orders, etc., to help augment determinations about authorized vs. hostile access to CPS components.

3.3. Organizational relationships

Remote access to CPS control interfaces implies that systems within one network are allowed by policy to make

connections. These policies are typically implemented by network firewalls or virtual private network (VPN) proxies. These are typically static policy settings that change very rarely once they are established. But what if the end node that is authorized to connect is compromised and is now under control of a hostile actor? Or worse, what if *another node* is compromised, and then a connection is proxied through that authorized host? This is known as a *stepping stone* attack, and can be imagined similar to a member of a family being diagnosed with the H1N1 virus.

Data exists about authorized login relationships between computers in an organization, the same way that familial relationships are known within a household. If one member of the household is known to be infected with a contagion, quarantine of the entire family is often used to isolate further infection. Within a network that involves CPS devices, where remote access is authorized by policy, a similar type of quarantine is possible. A research problem is to identify the networks of networks that could potentially result in unauthorized access to CPS control interfaces, to detect infections of nodes in those networks, and to implement meaningful containment of potentially harmful pathways to the CPS control interfaces.

These are just three examples of different meta-networks of logical entities that must be understood and manipulated in a similar way to how CPS devices must be understood and manipulated to control the physical world. The use of visual metaphor, and the application of analytic tools, can be accomplished using a familiar display similar to existing HMI displays.

4. A New Way Forward

Since much research today is performed in isolation, apart from daily operations in working environments, there is a huge disconnect and time lag between development of new concepts and their successful integration into commercially available technologies. A more agile and effective model would focus on immediate *operational needs*, with an emphasis on *applied research* complementary to basic research and education, all working together *in parallel*. This not only provides a more agile response model, but it leverages limited expertise across resource-constrained organizations at a reasonable cost.

Visual analytics is central to achieving this goal. Its strength lies in applying analytic methods to vast amounts of data and using the high-bandwidth visual system of the human brain to take in the results. The result is better awareness of what is expected in normal conditions, and faster recognition of the unexpected, leading to reasoned conclusions and judgments about appropriate actions to take *now*. At the same time, privacy and trust by the citizens who are to be protected is paramount. Visual analytics can support privacy protection through data minimization, data anonymization, or simply communicating about data in aggregate through visual means.

If we try to envision the components of a new way of thinking about CPS security, some key elements come to mind.

4.1. Secure overlay network for isolation and a trusted foundation

Computer devices today have shrunk to the point where fully-functional computers with multiple network interfaces, small enough to fit in the palm of a hand and costing just a few hundred dollars, can be used to form an overlay network of filtering-bridges between CPS devices and remotely accessible networks. This creates the foundation from which a distributed system can be built that provides all the functions of a trustworthy system. An HMI as described in Section 3 can be used to facilitate monitoring and control of these devices just like any other CPS device.

4.2. Integrated access control, command and control hardening, and monitoring

Given a device that is capable of acting as a firewall, an IPS, a network traffic capture system, and a programmable general-purpose computer, there is tremendous flexibility. Secured VPN tunnels are possible, as are fine-grained and dynamic access control rules that limit the ability to connect to and communicate with control devices. Traffic can be filtered at the ethernet level, and flow records generated and sent to a central collection repository for analysis. Using visualization and analytic capabilities, containment strategies can be implemented through dynamic adjustment of the communications links described in Section 3.2

4.3. Visualization and analytics for improved oversight

The power of visualization techniques and applied analytics gives network operators, security operators, and CPS system operators a shared picture of the health of their networks. Comparisons can be made of the type of traffic and connection patterns between CPS devices and normal computer systems in an organization, between CPS devices at different sites or different organizations, and historical patterns of activity can be evaluated to provide ongoing multi-faceted situational awareness. Any availability or performance problems can be observed in real-time, and more timely alerts sent out. The same visualization and analytic capabilities can also serve as a foundation for research, education, and training activities. New techniques can be immediately applied back into the operational framework.

4.4. Integration of operations, research and development, and education/training

Boyd used the concept of the *Observe, Orient, Decide and Act (OODA) Loop* (http://en.wikipedia.org/wiki/OODA_Loop) to describe how one can be alert to attacks and agile in responding and reacting to them. Central to the OODA Loop is a deep understanding of attacker weapons and tactics, and

the right tools and training to enable defenders to *get inside* the attackers' OODA Loop. Visual analytics is central to the Observation and Orientation phases of the OODA Loop, while knowledge repositories and decision support systems can support the Decide and Act phases. The integration of operations with R&D can provide the missing ingredient that accelerates transit through the OODA Loop, while the strategic framework described earlier enables integration of data fusion, data analysis, decision support, even providing a means of training users and running regular exercises to achieve peak performance in time of crisis.

5. Conclusions

The challenge put forward by the President's 60-day review and the CSIS is to come up with new ways – *out-of-the-box thinking*, or *high-risk, high-reward* projects – to achieve a trustworthy internetworked world. As stated in the President's review, "The government needs to integrate competing interests to derive a holistic vision and plan to address the cybersecurity-related issues confronting the United States. The Nation needs to develop the policies, processes, people, and technology required to mitigate cybersecurity-related risks... Research on new approaches to achieving security and resiliency in information and communications infrastructures is insufficient. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while also meeting our economic needs and national security requirements."

It is not sufficient to simply share information reactively. Rather, we need to collaborate in action-oriented alliances to better understand threats and design effective systems and procedures that counter those threats as a part of normal operations. As these alliances must span thousands of municipalities and private-sector organizations, from the local level up through state and federal agencies, visual analytics becomes central to addressing the scale and scope of the data involved. There is no better foundation for collaborative awareness and reasoning, which will drive analysis, prevention, and response activities.

References

[1] Executive Office of the President, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," Department of Homeland Security, December 2003. [Online]. Available: http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm

[2] Executive Office of the President, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure," The White House, Tech. Rep., May 2009. [Online]. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

[3] CSIS Commission on Cybersecurity for the 44th Presidency, "Securing Cyberspace for the 44th Presidency," Center for Strategic and International Studies, Tech. Rep., December 2008. [Online]. Available: http://www.csis.org/media/csis/pubs/081208_securingcyberspace_44.pdf

[4] North American Electric Reliability Council Control Systems Security Working Group, "Top 10 Vulnerabilities of Control Systems and Their Associated Mitigations – 2007," December 2006. [Online]. Available: http://www.controlsystemsroadmap.net/pdfs/NERC_2007_Top_10.pdf

[5] D. Dittrich, "On Developing Tomorrow's "Cyber Warriors"," in *Proccedings of the 12th Colloquium for Information Systems Security Education*, June 2008. [Online]. Available: http://staff.washington.edu/dittrich/misc/cisse2008-dittrich.pdf

[6] J. J. Thomas and K. A. Cook, 2005. [Online]. Available: http://nvac.pnl.gov/agenda.stm