Cyber Security and Optimization in Smart "Autonomous" Buildings

Michael Mylrea
George Washington University, Executive Leadership - Cyber Security Doctoral Program,
michaelmylrea@gmail.com

Abstract

The cyber-energy nexus threat is complex, non-linear and rapidly evolving as "smart" energy technology continues to transform our energy infrastructure. Cyber-attacks have been used to exploit smart building controls and breach corporate networks, manipulate drill logs, cause pipelines to explode and generators to fail. In the last two years there has been a major increase in cyber-attacks targeting the energy sector. In the six months ending in May 2013, there was a significant increase in cyber incidents, accounting for 53% of all incidents reported to the Department of Homeland Security (DHS). Most registered attacks appear to have targeted systems connected to the energy value chain or generation, transmission and distribution. A new and growing phenomenon appears to be attacks targeting building automation systems (BAS) and associated and interconnected enterprise networks. Target was hacked through the retailer's "Smart" HVAC system, giving hackers access to corporate networks and over 40 million customer's credit cards and other sensitive information.

Introduction

Smart building automation systems have opened smart buildings up to "Internet of Things" and present many opportunities to network and control key aspects of organization run out of these buildings. Pressure on building owners and operators to adopt smart building systems is being driven by economic and environmental factors. As a result they are quickly moving towards autonomous smart systems that integrate IT infrastructure with multiple electronic systems supporting building management functions and business applications. In smart buildings, this has led to major increases in process visibility, energy efficiency and conservation, cost savings, interoperability and the integration of systems. However, sharing of IT infrastructure and the integration of corporate IT and industrial control systems (ICS), including building systems, in an intelligent building also poses a number of design and operational cyber security challenges as well as opportunities. Despite these challenges and the increasing trend among critical infrastructure owners and operators to adopt networked building automation systems, this particular area of cyber security has not been examined thoroughly and related literature is at a nascent stage.

Building automation sensors can range from passive infrared motion detectors, to the CCTV motion detection and the use of radio frequency identification (RFID) technologies. By allowing sensors that are usually applied to a single sub-system to be used by other systems, the building can be made more intelligent: For example, the use of RFID tokens to control access to the building or building zones, to provide access to the corporate network and to retrieve documents on communal printers. Another example is the use of building security sensors and CCTV motion detection to operate and control lighting and in conjunction with environmental monitoring systems to manage heating, cooling, etc. Future smart buildings supported by the combination of artificial intelligence and building automation systems may enable a more flat or even leaderless structure inside organizations.

Historically, industrial control systems (ICS), including the subset that comprise building systems, and corporate IT systems have been managed by operations teams and IT teams respectively, with different operational processes, practices and governance. The combination of these organizational boundaries coupled with systems integration and interconnection can introduce significant operational complexity and cyber risk into intelligent buildings. For one, removing a virus or malware from a building management system may be significantly more complex as some electronic sensors or components will be embedded in many different major components and sub-systems. The problem may be further exacerbated by the potential age of the systems and the need to maintain building operations (Pullen, 2014).

Moreover, a combination of limited resources, different definitions, and competing priorities among smart building decision makers is one of the major reasons why there is a lack of cyber security. For example, if you ask different decision makers that own, operate or occupy a smart building their goals you will most likely get very different answers. Generally speaking, chief sustainability officers aim to reduce energy and natural resource consumption and costs. BAS presents an opportunity to increase visibility and interoperability of sensors, not cyber security. Similarly, chief finance officers want to maximize revenue and cost savings and may be opposed to cyber security measures that reduce interoperability and efficiencies. Chief security officers tend to focus on gates, guards and other physical building safety and access issues as opposed to information assurance. Even chief information officers tend to focus on securing corporate networks and devices to protect the confidentiality, integrity and availability of information. They are not accustomed or familiar with many of the new threats that are emerging as enterprise and industrial controls system networks converge in smart buildings.

Conclusion and Future Research

Today, United States' and other developed economies are increasingly shifting from manufacturing to services. Our factories, customers, distributors, suppliers have become increasingly distributed as have our leadership models (Conger and Pearce, 2003). Adding to the complexity, artificial intelligence is increasingly being used in robots and other automated systems to lead these distributed systems. The image of top-down leadership at the helm of the C-suite has been replaced by one of a computer or smart system sending and receiving commands to trade millions of dollars, collecting data on building occupants movements and interactions to optimize an organization's innovation and production, and smart adaptable intrusion detection systems that filter malware and spam while analyzing traffic for productivity and compliance.

In Pentland's recent book *Social Physics* he highlights how sensors gather behavioral data that enable scientists to develop "a causal theory of social structure" and ultimately establish "a mathematical explanation for why society reacts as it does" in all manner of circumstances. I'm interested in building on Pentland's research to examine how artificial intelligence can be used to enable building automation systems to collect and even send data that will optimize the innovation and productivity potential of organizations operating out of smart buildings. For example, if innovative organizations are characterized by significant cross-functional interaction then sensors will collect movement and communications patterns and provide suggestions on individuals that need to increase their collaboration (Pentland, 2014). A smart human machine interface could leverage that data to send an automated calendar invite to the individuals that need to communicate better. A smart intrusion detection system will be more agile and adaptable and learn to recognize patterns that suggest bad cyber hygiene practices and respond instantly with the appropriate threat remediation.

These new opportunities raise a number of questions worthy of future research: could smart automated buildings and processes take an increasingly important role in mitigating insider cyber threats, both intentionally and unintentional? Or will smart buildings increase the cyber threat to organizations? Will smart building controls one day take and increasingly important leadership role in future organizations? Artificial intelligence has already crossed critical thresholds such as self-learning and dynamic conservation, raising the prospect of smart buildings spurring leaderless or more autonomous organizations. Building controls area already replacing a wide gamut of workers inside organizations from guards to middle management, operations to analytic staff as building automation systems increasingly collect, monitor, control, and direct the activities inside organizations.

As behavioral researchers better understand what makes an organization successful will they be able to program building controls to better lead an organization (Pentland, 2014). Will doing make human leaders irrelevant? What are the limitations of automated systems in complex, distributed and non-linear organizations that increasingly define and drive our globalized economies? All of these questions present an interesting and timely avenue to examine issues at the nexus of cyber security and autonomous systems.

References

Conger, J. A., & Pearce, C. L. (2003). A landscape of opportunities: Future research on shared leadership. In C.L. Pearce & J.A. Conger (Eds.), *Shared leadership: Reframing the hows and whys of leadership* (pp. 285-303). Thousand Oaks, CA: Sage.

Pentland, A. (2014). Social Physics: How Good Ideas Spread-The Lessons from a New Science. Penguin.

Pullen, D. (2014)."Smart Buildings Research for the Future." Science in Parliament