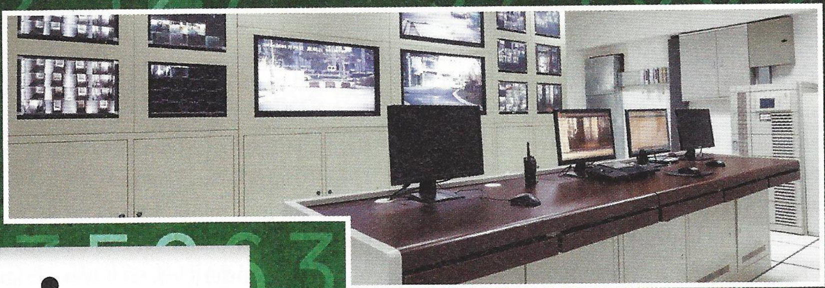

Cybersecuring Building Control Systems

By Michael Chipley, PhD, GICSP, PMP, LEED AP

Building control systems with embedded communications technology—as well as those enabled via an Internet Protocol (IP) address—provide critical services that allow a building to meet the functional and operational needs of building occupants. Unfortunately, they also can be easy targets for hackers and people with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities; use as an entry point to traditional information technology (IT) systems and data; cause physical destruction of building equipment; and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber-event. Cyber attacks, such as the Target and Home Depot data hacks, have directed increased attention to the network connectivity of facility/building operations and maintenance vendors, an organization's business IT systems and facility/building control systems.

Facility/building control systems, such as building automation systems (BAS), energy management systems (EMS), physical security access control systems (PACS) and fire alarm systems (FAS), now are considered potential hacking points into an organization. Such control systems often are referred to as operational technologies (OT) and use a combination of traditional IT protocols—transmission control protocol (TCP) or user datagram protocol (UDP)—and control systems with unique protocols (such as Modbus, BACnet, LonTalk and DNP 3) to communicate with sensors, devices and actuators.

IT is about data; OT is about controlling machines *(see the "Explanation of IT and OT" table, below, for more detail)*. Increasingly, OT is becoming more IP-based. The Internet of Everything, smart grids, smart cities, smart buildings and smart cars are redefining the boundary between IT and OT. As IT and OT systems converge, so are the risks and vulnerabilities of hacking OT systems as a point of entry. Once a hacker enters a system, it's just a matter of pivoting up the network and taking control of other system assets.

The National Institute of Standards and Technology (NIST) Special Publications (SPs) are a primary source for IT cyber standards and guides. Both government and industry have used *NIST SP 800-37—Guide for Applying the Risk Management Framework to Federal Information Systems* and *NIST SP 800-53—Security and Privacy Controls for Federal Information Systems and Organizations* publications, as well as the SANS Institute's top 20 critical security controls and standards from the International Organization for Standardization (ISO), as IT best practices for a number of years.

Control System Cyber Exploits Increasing in Number and Complexity

On the OT side, the International Society of Automation (ISA) ISA 99 and *NIST SP 800-82 Revision 2 Industrial Control Systems Security Guide* provide the standards and guides for industrial control systems (ICS).[1] Traditionally, neither ICS nor OT received the same level of cyber scrutiny as IT systems. However, malware, such as Stuxnet, Duqu or Flame, now are specifically designed to infect OT components and devices at the firmware or project-file level. They inject false commands to spoof an operator's human machine interface console, establish a command and control channel to exfiltrate data (technical specifications, floor plans, drawings, etc.), create Botnets or physically destroy the equipment and other IT systems.

Earlier this year, Cylance released the Operation Cleaver report (**www.cylance.com/operation-cleaver/**), which details the work of a group of international hackers, primarily from Iran, who are attacking multiple companies from diverse

Explanation of IT and OT

	Information Technology	Operational Technology
Purpose	Process transactions and provide information	Control or monitor physical processes and equipment
Architecture	Enterprise-wide infrastructure and applications (generic)	Event-driven, real-time, embedded hardware and software (custom)
Interfaces	Graphical user interface (GUI), web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays and hand-held devices
Ownership	Chief information officer, IT	Engineers, technicians, operators and managers
Connectivity	Corporate network and IP-based	Control networks, hard-wired twisted pair and IP-based
Role	**Supports people**	**Controls machines**

industries in 16 different countries. The tactics, techniques and procedures they are using in what is considered to be an ongoing campaign include:

- Targeting and compromising transportation networks and systems.
- Fully compromising active directory domains, along with entire switches, routers and internal networking infrastructure.
- Fully compromising Virtual Private Network (VPN) credentials, meaning an entire remote access infrastructure and supply chain are under control under permanently compromised credentials.
- Achieving complete access to airport gates and their security control systems.
- Gaining access to PayPal and Go Daddy credentials in order to make fraudulent purchases and allow unfettered access to a victim's domains.

Defending Building Control Systems

Within the U.S. Department of Homeland Security (DHS), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) maintains a list of vulnerabilities and alerts for control systems and publishes the Cyber Security Evaluation Tool (CSET), which is free of charge to any organization. CSET contains standards, guides, references, networking diagram tools and compliance evaluations, and can generate system security plans and other key documents (*learn more* at **http://ics-cert.us-cert.gov/**).

In addition, the National Institute of Building Sciences WBDG Whole Building Design Guide® now hosts a new Cybersecurity Resource Page (*see at* **www.wbdg.org/resources/cybersecurity.php**). This resource, primarily for use by the buildings community, includes cybersecurity information, as well as links to other control systems, workshops and training. All facility/building owners, property managers and engineering and security staff are highly encouraged to understand the basic principles of *NIST SP 800-82 R2*; know how to use the DHS CSET tool; understand how tools (such as Shodan, Kali Linux and SamuraiSTFU) work for penetration testing; and prepare to adopt new acquisition and procurement processes into their organizations. Whereas the IT community has had almost two decades to learn and implement cybersecurity, the OT community will require an accelerated learning curve and will need to work closely with senior management, IT and other stakeholders to properly cybersecure their assets.

Every building owner should have a building cybersecurity strategy with the following key documents to cover both IT and OT assets:

- System security plan (SSP);
- Plan of action and milestones (POAM);
- Information technology and concept of operations plan (ITCP);
- Incident communications procedures (ICP); and
- Security auditing plan (SAP).

In 2015, the DHS Interagency Security Committee released the "Securing Government Assets through

Continued on page 30

Key Cyber Issues/Actions for Facilities

Most building control system protocols, such as Modbus, BACNet and LonTalk, are not encrypted or authenticated. Building security teams need to put in a DMZ, firewalls, VPNs, fiber and wireless that support front-end encryption and authenticate their building control systems.

Many system integrators do not employ basic cyber hardening of the IT front-end of control systems. Building security teams need to harden the front-end of their IT control systems.

Many of the operator log-ins for web portal access use **htpp** (port 80) and not https (port 443). Building security teams need to make their portal access secure.

Many facilities have minimal precautions to prevent social engineering and phishing, or to even identify an exploit. By setting up even basic security levels, facility operators can greatly reduce the potential for harm.

The *NIST SP 800-82 R2 Industrial Control Systems Security Guide* can provide guidance and best practices.

Building security teams should make tools, such as Kali Linux, DHS CSET, Shodan, Sophia and Diggity, an important part of their facility's tool bag.

Building security teams should include continual monitoring and conducting **monthly** security audits of building control systems on their critical tasks list.

Combined Traditional Security and Information Technology White Paper" (*see at* **www.dhs.gov/sites/default/files/publications/ISC-CVS-White-Paper-2015-508.pdf**). This document outlines the risk management framework process that can be applied to physical security systems, such as closed-circuit video equipment or video systems, intrusion detection systems and electronic PACS. Key to these recommendations is bringing physical security specialists, facility engineers and managers, IT, system integrators and property owners to the table to conduct assessments and develop an SSP. Another consideration in the procurement process is to initiate the converged systems' baseline risk assessment in planning and design phases, and conduct factory acceptance testing in the construction phase and full-site acceptance testing (including penetration testing) for system turnover.

An underlying fundamental concept of the *NIST SP 800-82 Rev 2 Industrial Control Systems Security Guide* is the concept of "inbound protection and outbound detection." All control systems should be on a separate network with multiple levels of demilitarized zones (DMZs)[2] and sub-networks. Control systems behave in very predictable ways with data frequency, packet size and other attributes fairly constant and amenable to white listing. New OT firewalls able to perform deep packet inspection and OT passive monitoring tools that identify anomalous traffic provide inbound protection. Continuous monitoring provides an outbound detection capability. Control systems generally do not send megabit or gigabit files to remote servers, either in an organization's known network or connected vendors. Exfiltration of

Clarification

In the August 2015 issue of the *Journal of the National Institute of Building Sciences*, an article on pages 28-32 by Patricia Andrasik, "Building Performance Analytics," incorrectly identified Dr. Don McLean's place of work. In this instance, IES should have been noted as Integrated Environmental Solutions, Ltd.

BUILDING SCIENCES
Hazard Mitigation and Risk Assessment
BUILDING SCIENCES
Resilience in the Built Environment
BUILDING SCIENCES
Up Close and Professional

Ad Index

AIA Contract Documents	www.aia.org/JNIBS	9
ARCAT	www.arcat.com	CV4
Bentley Systems	www.bentley.com/yiiconference	3
	www.bentley.com	20
Bluebeam Software, Inc.	www.bluebeam.com/decidefaster	7
	www.bluebeam.com/institute	20
Building Innovation 2016: The National Institute of Building Sciences Fourth Annual Conference & Expo	www.nibs.org/conference2016	17
CENTRIA	www.CENTRIAperformance.com	21
Cosella-Dörken	www.cosella-dorken.com	20
Dow Corning	www.BuildaBetterBarrier.com	CV2
	www.dowcorning.com/construction	20
Flood Control of America	www.FloodControlAM.com	13
GeoShack	www.geoshack.com	21
	www.geoshack.com/BIM	CV3
ICC-International Code Council	http://premiumACCESS.icc.safe.org	4
INVIEWlabs-Unifi	www.discoverunifi.com	34
National Institute of Building Sciences Cybersecurity Building Control Systems Workshop	www.nibs.org/cybersecurity	21
NSSA-National Storm Shelter Association	www.nssa.cc	16
Parsons Corporation	www.parsons.com	29
VaproShield	www.vaproshield.com	21
VP Buildings	www.vp.com/ad/JNIBS	31

data and covert command and control channels to unrecognized IP addresses are key signs of compromise. *NIST SP 800-82 R2* also has new controls for acquisition, life-cycle software development and penetration testing. New continuous monitoring tools have been created specifically to evaluate and manage control system protocols.

Facility owners and operators also will need to add penetration testing tools to their tool bag. Traditional hacking tools now have add-on packages with OT exploits. Other tools can expose any IP device and provide a wealth of information about the device, system, organization and other data.

Security Auditing

The security team should perform a monthly security audit, including documentation. Such an audit verifies that an organization's software and hardware are functioning as intended; reviews event and audit logs; identifies and addresses potential vulnerabilities; confirms that patch management is current; notes whether continuous monitoring is functional; identifies indicators of compromise or exploitation; and ensures that appropriate action is taken in a timely manner.

When conducted on a monthly basis, a security audit process compares baseline and previous configurations to identify any systemic changes. This document is used in conjunction with IT policies and procedures, ITCP and ICP documents.

The security team, consisting of members listed within the ITCP, should include, at a minimum, the information system security officer, system administrator and security coordinator(s). Among the tasks are the following:

- Situate all building control systems into a DMZ and properly configure them so the human machine interface and building controllers cannot be found on Shodan.
- Register the team with ICS-CERT to receive alerts and advisories.
- Exercise the ITCP at least annually.

With the number of hacks on the rise, it is no longer a question of if a building controls system will be exploited. It is only a question of when. JNIBS

ABOUT THE AUTHOR: Michael Chipley, PhD, GICSP, PMP, LEED AP *is a consultant to multiple federal agencies and private-sector clients; contributor to the NIST SP 800-82 R2 and the DHS CSET tool; and creator of the National Institute of Building Sciences' "Cybersecuring Buildings Control Systems Workshops." He can be reached at* **mchipley@pmcgroup.biz**.

References:

[1]The NIST definition of ICS includes a wide range of control systems; an emerging term to categorize these converged systems is cyber-physical systems (CPS).

[2]In computer security, a DMZ (demilitarized zone) is a physical or logical sub-network that separates an internal local area network (LAN) from other untrusted networks, usually the Internet. External-facing servers, resources and services are located in the DMZ so they are accessible from the Internet, but the result of the internal LAN remains unreachable. This provides an additional layer of security to the LAN as it restricts the ability of hackers to directly access internal servers and data via the Internet (**http://searchsecurity.techtarget.com/definition/DMZ**).