MIT MANAGEMENT SLOAN SCHOOL
INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY
(IC)^3

Newsletter

Newsletter #13: March-April 2017

(IC)^3 Spring Workshop held on April 5, 2017

The Spring (IC)^3 workshop was at full capacity this past April. The agenda included sessions on cybersecurity impact on the adoption of new technologies, cyber-insurance as a risk mitigation strategy, blockchain benefits and vulnerabilities, security versus usability, defeating hackers of IoT devices, and international trade impacts of cybersecurity. A panel session on cybersecurity risk metrics, featuring five cybersecurity leaders, and a table-top exercise to teach board and C-level executives about cybersecurity rounded out the content. A poster-session reception provided for lively discussion following the content of the day. The (IC)^3 Annual Conference will be held on July 10-11. Save the date!

Spring Workshop showcasing latest research was at capacity!

Photos from Spring Workshop

Top left: MIT Student Juan Carrasocsa presents to the workshop. A full house of members and guests engage in discussion. Bottom left: The Cybersecurity Risk Metrics pane (left: Michael Siegel (MIT) Moderator, John Herd (Limelight), Andrew Stanley (Philips Healthare), Jim Cupps (Liberty Mutual), Michael Siechrist (State Street) and Jerry Grochow (MIT), shares expertise, graphic recording of session highlights and key ideas.

(IC)^3 Participated in the Financial Times CyberSecurity Summit

Professor Madnick Spoke at the FT Cyber Security Summit

Financial Times Live held their summit "Is America Losing the Cyber War?" in Washington DC., on March 15, 2017. Professor Stuart Madnick from the (IC)^3 participated in the panel session on “The Internet of Things – Attack Vulnerabilities and Solutions.” See the video of this session here: http://bit.ly/IC3FTCyberPanel

FT
FT CYBER SECURITY SUMMIT USA
Is America Losing the Cyber War?

Save the date for the (IC)^3 summer conference: July 10-11

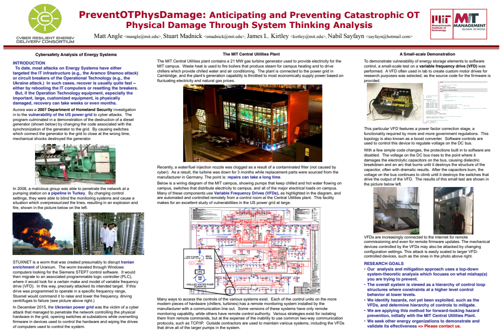
About Cybersecurity at MIT:

The MIT Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity, (IC)^3, is one of three cybersecurity programs at MIT. It is focused on the managerial, organizational, and strategic aspects of cybersecurity. The other two programs are the Internet Policy Research Initiative (IPRI), focused on policy, and Cybersecurity@CSAIL, focused on improved hardware and software. More information on (IC)^3 can be found at http://ic3.mit.edu or by contacting smadnick@mit.edu

(IC)^3 Team Participated in CREDC Workshop

(IC)^3 team: Keman Huang, Keri Pearlson, Michael Siegel, and Matt Angle

The Cyber Resilient Energy Delivery Consortium (CREDC) is a five-year, $28.1 million research and development initiative that is funded by the Department of Energy and is focused on cybersecurity and cyber-resiliency of energy delivery systems for the electric power and oil & gas industries. In March 2017, the Consortium workshop highlighted many of the projects funded by this initiative, including a project from (IC)^3, *Preventing OT Physical Damage: Anticipating and Preventing Catastrophic OT Physical Damage Through System Thinking Analysis* (poster image shown to the left). MIT Student Matt Angle represented the research team (which includes Stuart Madnick, James Kirtley, and Nabil Sayfayn) at the Consortium and presented a poster of the project (Visit http://bit.ly/IC3CredCPowerPoster for larger version of the poster).



CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

PreventOTPhysDamage: Anticipating and Preventing Catastrophic OT Physical Damage Through System Thinking Analysis

Matt Angle <mangle@mit.edu>, Stuart Madnick <smadnick@mit.edu>, James L. Kirtley <kirtley@mit.edu>, Nabil Sayfayn <sayfayn@hotmail.com>

Cybersafety Analysis of Energy Systems

INTRODUCTION

To date, most attacks on Energy Systems have either targeted the IT infrastructure (e.g., the Aramco Shamoo attack) or circuit breakers of the Operational Technology (e.g., the Ukraine attack.) In such cases, recover is usually quite fast – either by rebooting the IT computers or resetting the breakers. But, if the Operation Technology equipment, especially the important, large, customized equipment, is physically damaged, recovery can take weeks or even months.

Aurora was a **2007 Department of Homeland Security** investigation in to the vulnerability of the US power grid to cyber attacks. The program culminated in a demonstration of the destruction of a diesel generator (shown below) by changing the code associated with the synchronization of the generator to the grid. By causing switches which connect the generator to the grid to close at the wrong time, mechanical shocks destroyed the generator.

In 2008, a malicious group was able to penetrate the network at a pumping station on a pipeline in Turkey. By changing control settings, they were able to blind the monitoring systems and cause a situation which overpressurized the lines, resulting in an explosion and fire, shown in the picture below on the left.

STUXNET is a worm that was created presumably to disrupt Iranian enrichment of Uranium. The worm traveled through Windows computers looking for the Siemens STEP7 control software. It would then migrate to an associated programmable logic controller (PLC), where it would look for a certain make and model of variable frequency drive (VFD). In this way, precisely attacked its intended target. If this drive was programmed to operate in a specific frequency range, Stuxnet would command it to raise and lower the frequency, driving centrifuges to failure (see picture above right.)

In December 2015, the Ukranian power grid was the victim of a cyber attack that managed to penetrate the network controlling the physical hardware in the grid, opening switches at substations while overwriting firmware in devices used to control the hardware and wiping the drives of computers used to control the system.

The MIT Central Utilities Plant

The MIT Central Utilities plant contains a 21 MW gas turbine generator used to provide electricity for the MIT campus. Waste heat is used to fire boilers that produce steam for campus heating and to drive chillers which provide chilled water and air conditioning. The plant is connected to the power grid in Cambridge, and the plant's generation capability is throttled to most economically supply power based on fluctuating electricity and natural gas prices.

Recently, a water/fuel injection nozzle was clogged as a result of a contaminated filter (not caused by cyber). As a result, the turbine was down for 3 months while replacement parts were sourced from the manufacturer in Germany. The point is: repairs can take a long time.

Below is a wiring diagram of the MIT campus, showing pumps that keep chilled and hot water flowing on campus, switches that distribute electricity to campus, and all of the major electrical loads on campus. Many of these components use Variable Frequency Drives (VFDs), as highlighted in the diagram, and are automated and controlled remotely from a control room at the Central Utilities plant. This facility makes for an excellent study of vulnerabilities in the US power grid at large.

Many ways to access the controls of the various systems exist. Each of the control units on the more modern pieces of hardware (chillers, turbines) has a remote monitoring system installed by the manufacturer with a communication line out. Some versions of these systems have only remote monitoring capability, while others have remote control authority. Various strategies exist for isolating them from remote commands, but at the expense of the inability to use common two-way communication protocols, such as TCP/IP. Outside contractors are used to maintain various systems, including the VFDs that drive all of the larger pumps in the system.

A Small-scale Demonstration

To demonstrate vulnerability of energy storage elements to software control, a small-scale test on a **variable frequency drive (VFD)** was performed. A VFD often used in lab to create custom motor drives for research purposes was selected, as the source code for the firmware is provided.

This particular VFD features a power factor correction stage, a functionality required by more and more government regulations. This topology is also known as a boost converter. Software controls are used to control this device to regulate voltage on the DC bus.

With a few simple code changes, the protections built in to software are disabled. The voltage on the DC bus rises to the point where it damages the electrolytic capacitors on the bus, causing dielectric breakdown and an arc that burns until it destroys the structure of the capacitor, often with dramatic results. After the capacitors burn, the voltage on the bus continues to climb until it destroys the switches that drive the output of the VFD. The results of this small test are shown in the picture below left.

VFDs are increasingly connected to the internet for remote commissioning and even for remote firmware updates. The mechanical devices controlled by the VFDs may also be attacked by changing configuration settings. This attack is easily scaled to larger VFD-controlled devices, such as the ones in the photo above right.

RESEARCH GOALS

- **Our analysis and mitigation approach uses a top-down system-theoretic analysis which focuses on what mishap(s) you are trying to prevent.**
- **The overall system is viewed as a hierarchy of control loop structures where constraints at a higher level control behavior at lower levels.**
- **We identify hazards, not yet been exploited, such as the VFDs, and determine hierarchy of controls to mitigate.**
- **We are applying this method for forward-looking hazard prevention, initially with the MIT Central Utilities Plant.**
- **We seek other energy organizations to demonstrate and validate its effectiveness => Please contact us.**

Upcoming Events

MIT Sloan CIO Symposium will be on May 24, 2017. There will be two sessions on cybersecurity being organized by the (IC)^3 ."Measuring ROI for Cybersecurity: Is It Real or a Mirage?" moderated by Dr. Michael Siegel and "You Were Hacked—Now What?" moderated by Dr. Keri Pearlson. For our (IC)^3 members, you can get discounted $99 registration fee by using the code IC3-VIP-17. Use this URL to register: http://www.mitcio.com/

The (IC)^3 Annual Conference will be held July 10-11, 2017 at the MIT Sloan School of Management. **Save the date**! Last year's conference was a favorite of members and attendees. We welcome up to 3 participants from attending organizations making this an excellent opportunity to involve colleagues and generate discussion around building a cyber resilient organization. Sessions will highlight recent (IC)^3 research and include speakers on key topics of interest to our members. THIS IS AN INVITATION ONLY EVENT, so if you are not a member of (IC)^3, please join soon so you can attend. Details about the agenda are coming soon.

(IC)^3 in the News

Financial Times MBAs vs hackers: leaders of the future learn to fight cyber crime (April 2017) featured Stuart Madnick's comments on the importance of flexible management thinking to manage cyber security. (See article here: http://bit.ly/IC3MBAvsHackers)

> Stuart Madnick says the high-level consequences of cyber attacks mean that they must be handled by executives who direct the company's strategy, rather than to the technical staff. Madnick taught network security in the college's MBA program, saying that companies need extremely flexible management thinking because hackers may be more unpredictable than natural disasters. "The hurricane will not change the direction because you know you are coming, but the network attacker can."
>
> This article was also published in Chinese at FT China: 应对黑客攻击从MBA抓起 (See Chinese article here: http://www.ftchinese.com/story/001072309)

Rolling Stone WikiLeaks' CIA Document Dump: What You Need to Know (March 2017) interviewed Stuart Madnick for comments about the continued government breaches. (See article here: http://bit.ly/IC3RollingStoneApril2017)

> Cybersecurity expert Stuart Madnick, head of the Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity at MIT, says the CIA is conflicted: "How dangerous is it to you if the vulnerabilities persist, or how valuable are the vulnerabilities if the CIA can use them? We need to decide as a nation."