Cyber-Physical Security Engineering for Grid and Transportation Networks

Electrical and Computer Engineering

Michigan Technological University

In the context of today's adversary, the term "security" can be redefined in a broader sense both in terms of resilience, adequacy, and safety of an integrated cyber-physical system, as well as its relational dependencies crossing multi-domains of nation's critical infrastructures. Between the power grid and transportation system, the tie has never been closer. In power utility businesses, advanced sensors have been ubiquitously deployed. On the other hand, the transportation system, such as quasi-real-time traffic information can be established to optimize the complex system of interconnected systems. The traditionally established communication infrastructure in critical infrastructures can now be collaboratively extended with ubiquitous mobile devices.

The objectives of this workshop:

1. Cultivate cross-disciplinary research and to bridge the gap of cultures between the two professional communities.

2. Promote awareness of emerging research subjects related to optimality of transportation and power delivery.

3. Relate correlations of geographically overlapped specifics that can be spatiotemporally established

4. Critical issues of privacy on the individuals corresponding to electrical load consumption and human mobility in geographical locations.

5. Adaptation of cybersecurity technologies with countermeasures against malicious intent of the potential foul play.

6. Provide a ground of preliminaries in actuarial science that can be systematically assessed based on intentional catastrophe.

7. Bridge the gap between industry practitioners and academic researchers in these two critical domains.

Who should attend: Industry practitioners in power and transportation industries, policy makers and influencers.

This workshop represents a curated mix of industry and academic speakers, presenting up-to-date practice and state-of-the-art research. The two-day events are programmed with experienced speakers who have years of practice in cybersecurity, power operations planning, and transportation engineering. All involved faculty are research-active and working in this emerging space. The niche will provide unprecedented access to industry engineers with hands-on experience in the emerging world. This workshop satisfies continuing education requirements for professional engineers.

Presentations

Secure Operations Technology

Speaker: Andrew Ginter, Waterfall Security Solutions (andrew.ginter@waterfall-security.com)

Abstract: Secure Operations Technology (SEC-OT) is a perspective, a methodology, and a set of best practices used by the most secure industrial sites, in addition to classic Information Technology Security (IT-SEC) practices. SEC-OT focuses on information flows: since all cyberattacks are information, a comprehensive inventory of both online and offline flows of information entering a control-critical network is also a comprehensive inventory of all cyber-attack vectors for the network. SEC-OT sites systematically discipline all such inbound information/attack flows, preferably physically. Disciplines range from physically blocking information/attack flows and substituting other mechanisms to achieve essential business needs, to limiting, inspecting, transforming and testing incoming information for impacts on safe, reliable, continuous, correct and efficient industrial operations. This presentation introduces and surveys SEC-OT concepts and practices.

Biography: Andrew Ginter is the VP Industrial Security at Waterfall Security Solutions, leading a team of experts responsible for industrial cyber-security research, contributions to standards and regulations, and security architecture recommendations for industrial sites. Before Waterfall, Andrew led the development of software products for SCADA systems, IT/OT middleware, and OT security at Hewlett-Packard, Agilent Technologies and Industrial Defender. Andrew holds IT/OT middleware and industrial cybersecurity patents, is a co-author of the Industrial Internet Consortium Security Framework and is the author of the books SCADA Security - What's broken and how to fix it and Secure Operations Technology" He holds a BSc. in Applied Mathematics and an MS in Computer Science, both from the University of Calgary.

Bottom-Up Electrical Vehicles (EV) Forecasting

Speaker: Pedram Jahangiri, National Grid (pedram.jahangiri@nationalgrid.com)

Abstract: EV charging load is expected to have one of the largest potential impacts to National Grid's electric system in the next 15 years. Therefore, accurate future charging demands needs be forecasted for better planning. Given the complex issues associated with EV driving and charging, the interactions with regular vehicles, and options in deploying different charging infrastructure, there is a need to explore the future charging load demand profiles in space and time dimensions. Existing studies are limited on forecasting EV charging and infrastructure needs. Some studies use travel survey data to get the sampled daily travel pattern to estimate the driving energy consumption and simply scale up to the entire simulated EVs. Some other studies use optimization methods to maximize the electric vehicle mile travelled (eVMT) to fully utilize the current charging stations. Given the challenges of the problem and the limitations of existing studies, the objective of the present study is to provide a comprehensive agent-based traffic and energy simulation method for the EV charging load demand in accelerating EV market growth. The proposed method considers the interactions between EVs and regular vehicles based on dynamic activity-based travel demand models in POLARIS, an open-source agent-based simulator for large-scale transportation systems. The presented method combines the electric grid with the transportation network in simulations and post-processes the EV charging power profiles traffic simulation results with feeder load profiles.

Biography: Pedram Jahangiri is a Manager at Advanced Data and Analytics team in National Grid. He received the B.S., M.S. and PhD degrees in electrical engineering, power System in 2006, 2008 and 2014, respectively. His PhD work at Iowa State University was focused on modelling smart distribution systems and distributed Volt/Var control by Photovoltaic inverters. Currently at National Grid, he leads the modelling and planning of advanced analytics initiatives, such as developing quantitative models and analyses associated with electric distribution system forecasting. He has been previously employed as a researcher by Electric Power Research Center at Iowa State University, Electric Ship Research and Development Consortium at Mississippi State University, and by the Automation of Complex Power Systems Center, RWTH University, Germany. He also worked on enhancing Volt/VAr management models as an electrical engineer in the summer of 2012 by Energy Automation Solutions, Cooper Power Systems Company (Eaton).

Assessing and Evaluating Risk of Passenger Rail Transportation Systems

Speaker: Joel Langill, AECOM (joel.langill@aecom.com)

Abstract: Acts of terrorism continue to rise as malicious actors continue to find new ways to inflict mass casualty in ways that were not previously considered as credible threats. Flying a plane into a building was only the beginning. From titrating liquids to make inflight explosives, to using vehicles to ram crowds of innocent bystanders, threat actors continue to pose significant risk to the safety and security of local, regional, national and global communities. In 2017, Americans took 10.1 billion trips on public transportation with more than 34 million times each weekday. More than 6,800 organizations provide public transportation in the United States today. In New York City, more than 5.7 million people take the subway each day. This brief will take a look at a typical rail transportation system. The cyber attributes of each major component will then be discussed focusing on two key attributes. How could this be weaponized to cause physical harm; and how could this be compromised using cyber techniques, tactics and procedures to cause this harm. Risk management forms the foundation for both physical and cyber security, as well as long-term resilience. Risk is not only measured in terms of the likelihood and impact a threat poses a particular asset, but also the attractiveness of this asset to the adversary. With transportation organizations representing very attractive targets to a malicious actor, local, state and federal governments are working diligently to protect passengers and offer a safe and secure environment. This brief is meant to induce new ways to look at risk management in terms of a converged world that leverages both cyber and physical weapons, and why current regulations and frameworks can only serve as a foundation to initiating change.

Biography: Joel Langill is a part of the Critical Infrastructure Protection team at AECOM where he serves as the Director of Industrial Cybersecurity Services. In his role, he leads and develops teams within AECOM's global organization focusing on the identification of cyber-physical threats, how they could potentially exploit system and operational weaknesses across cyber, physical and spectrum domains, and how this could impact essential business and manufacturing operations. Cybersecurity services span multiple sectors including defense, transportation, commercial facilities, sporting and entertainment venues, smart cities, to name a few. Prior to joining AECOM, Joel founded SCADAhacker.com – a site devoted to industrial cybersecurity. He has worked for over 30 years exclusively in the industrial automation and control industry where he was involved in designing, implementing and supporting automation solutions for infrastructure projects spanning the globe. His experience was developed working in control system architectural design, product development, project implementation, and system migration in a variety of roles having exposure to most industry sectors. Having worked on both greenfield and brownfield projects around the world, Joel has rare and insightful insight into the risks and mitigation of cyber threats in industrial control systems as they have been designed, deployed, and maintained. Joel offers one of the leading training courses on ICS cybersecurity, and was the co-author of the popular book on the subject "Industrial Network Security". Joel is a member of the ISA 84 and ISA99 committees on functional safety and industrial security for control systems. His certifications include: Certified Ethical Hacker (CEH), Certified Penetration Tester (CPT), Certified SCADA Security Architect (CSSA), and TÜV Functional Safety Engineer (FSEng). Joel has also obtained extensive training through the U.S. Dept. of Homeland Security FEMA Emergency Management Institute having completed ICS-400 on incident command and crisis management. He is a graduate of the University of Illinois – Champaign with a BS (Bronze Tablet University Honors) in Electrical Engineering.

Cyber Insurance for Power Grids

Speaker: Chee-Wooi Ten, Michigan Tech (ten@mtu.edu)

Abstract: As evidenced by the recent cyberattacks against Ukrainian power grids, attack strategies have advanced and Stuxnet-like malware agents will continue to emerge. Currently, the measures to audit the critical cyber assets of power infrastructure do not provide a quantitative guidance that can be used to address security protection improvement in the audit process. Investing in security protection is often limited to compliance enforcement on the reliability standards. Technologies could provide more security logs to automate the assessment of the ongoing health of cyber systems. The cyber risk management in utilities can be quantified but the auditors and investors must understand the implications of hypothetical worst cases and how they can affect their neighboring control areas within an interconnection if a cyberattack ever occurs. The talk of this collaborative effort accumulated over the past years is to promote the ongoing development for an actuarial framework of enterprise risk management for power grid cybersecurity. The generation of comprehensive vulnerabilities and reliability-based knowledge based on extracted security logs, cyber-induced degradation of operational reliability, and hypothetical implications can establish risk portfolios for utilities in term of their preparedness level to protect their power communication infrastructure against cyber manipulation.

Biography: Chee-Wooi Ten is an Associate Professor of Electrical and Computer Engineering at Michigan Technological University. He received the BSEE and MSEE degrees from Iowa State University, Ames, in 1999 and 2001, respectively. He later received the Ph.D. degree in 2009 from University College Dublin (UCD), National University of Ireland prior joining Michigan Tech in 2010. Dr. Ten was a Power Application Engineer working in project development for EMS/DMS with Siemens Energy Management and Information System (SEMIS) in Singapore from 2002 to 2006. His primary research interests are modeling for interdependent critical cyber-infrastructures and SCADA automation applications for a power grid. He is a Senior Member of the IEEE. He is an active reviewer for IEEE PES transactions and was a member of IEEE PES computer and analytical method for cybersecurity task force. Dr. Ten is currently serving as an Editor for IEEE Transactions on Smart Grid and Elsevier Journal Sustainable Energy, Grids and Networks (SEGAN). He recently published a textbook entitled "Distribution Emergency Operation," addressing the reconfigurability (a notion of resilience) of distribution feeders and promotion of large-scale data extraction of topologies from geographic information systems (GIS) for advanced distribution engineering course.

"Securities" for System-Wide Power Control and Protection

Speaker: Koji Yamashita, Michigan Tech (kyamashi@mtu.edu)

Abstract: Aligning with the theme of this workshop, this presentation emphasizes the evolving security context, both in terms of reliability and cybersecurity. Traditionally, a protective relaying is armed with a local control mechanism that is set up against the faulted current. However, cascading events can aggravate grid operation if remedial actions are not well coordinated in an interconnected area. Since there has been a tremendous number of renewable energy sources (RES), the intermittency of alternative RES can complicate the planning and operational environment. On the other side, the control systems have now been integrated with the current trends of Internet protocol (IP)-based solutions. This talk will brief through the fundamentals of system control based on event types where how preventive or remedial actions can improve overall security. In addition, disruptive switching events may initiate a detrimental event that can cascade to other areas within an interconnection. These issues of RES, cybersecurity will be discussed from the industry and academic perspectives.

Biography: Koji Yamashita has more than 20 years of work experience with the Central Research Institute of Electric Power Industry (CRIEPI), which is the Japanese Electric Power Research Institute (EPRI). He had access to projects involved in protective relaying and simulation models for wind, solar, battery on the Japanese power transmission/distribution grid. His passion for power system dynamics and stability was infected by his ongoing CIGRE/CIRED working group (WG) activities from around the world where he started to engage since 2009 and led the WG for the past 5 years. He now remains active as a participant to attend the regular meetings each year. He has recently published a 300-page technical report entitled "Modeling of Inverter-Based Generation for Power System Dynamic Studies." Koji received the B.S. and M.S. degrees both in Electrical Engineering from Waseda University, Tokyo, Japan, in 1993 and 1995, respectively. He was a Visiting Researcher with Iowa State University from 2006 to 2007. He is currently a full-time researcher at Michigan Technological University and finishing the Ph.D. degree in ECE department.

Emerging Cybersecurity Threats with Case Studies

Speaker: Yu Cai, Michigan Tech (cai@mtu.edu)

Abstract: Cyberattacks are becoming more common, sophisticated and damaging with new threats emerging almost daily. Recent cyber breaches indicate that cybersecurity is not just an IT and cybersecurity issue, and likely won't be solved by IT and cybersecurity people alone. The need to have well-trained and well-prepared cybersecurity professionals with domain-specific knowledge is a pressing issue. This talk has two parts. In part I, we will review some recent high-profile cyber breaches, look into the technical details of these attacks, and learn how the attacks could have been prevented or mitigated. In part II, we will summarize lessons learned from past breaches, and study emerging cyber threats and new defense mechanisms.

Biography: Yu Cai is a professor and chair of the Computer Network and System Administration (CNSA) program at the College of Computing, Michigan Technological University. His current research interests include cybersecurity, computer network, and IT education. He is particularly interested in applying his research and techniques to real-life applications. He has been a consultant to many companies including IBM and Ford. Dr. Cai serves in editorial boards of several international journals. He also serves in the program committees of many international conferences. Dr. Cai is an IEEE senior member, ACM member, ASEE member, and ABET evaluator.

Challenges and Opportunities of Transportation Electrification: A Perspective from Power Systems Engineers

Speaker: Wencong Su, Michigan Tech (wencong@umich.edu)

Abstract: We live in an increasingly urban world with abundant transport and electricity infrastructure. Recently, advances in electrified transportation systems and smart grid technologies offer great promise to widely popularize electric vehicles (EVs), and have the potential to revolutionize urban transportation systems and power systems. An ever-increasing number of EVs will radically change the traditional views of the power and transportation industries, the social environment, and the business world. The electrification of transportation brings both opportunities and challenges to existing critical infrastructures. The successful rollout of EVs depends highly on the affordability, availability, and quality of the associated services that our nation's critical infrastructures (e.g., power and transportation systems) can provide. In this talk, we will present a comprehensive overview of the planning, control, management, and economic operation aspects of grid integration of EVs from an power systems engineer's perspective. We will also discuss our ongoing research work at the University of Michigan-Dearborn and future research trend.

Biography: Wencong Su is an Associate Professor in the Department of Electrical and Computer Engineering at the University of Michigan-Dearborn, USA. Prof. Su received his B.S. degree (with distinction) from Clarkson University, Potsdam, NY, USA, in 2008, his M.S. degree from Virginia Tech, Blacksburg, VA, USA, in 2009, and his Ph.D. degree from North Carolina State University, Raleigh, NC, USA, in 2013, respectively, all in electrical engineering. He is a registered Professional Engineer (P.E.) in the State of Michigan. He worked as a Research Aide at Argonne National Laboratory in IL, USA, in 2012. He also worked as a R&D engineer intern at ABB U.S. Corporate Research Center in NC, USA, in 2009. His current research interests include power and energy systems, energy internet, electrified transportation systems, and cyber-physical systems. He is a senior member of IEEE. He is an Editor of IEEE Transactions on Smart Grid and an Associate Editor of IEEE Access.

Summer workshop by Michigan Tech
Cyber-Physical Security Engineering for Grid and Transportation Networks

Tuesday, July 30, 2019

	From	To	Hours	Events	Speakers
Day 1: Industry Practise	7:00:00 AM	8:00:00 AM		**BREAKFAST**	
	8:00:00 AM	**8:15:00 AM**	**0.25**	**Michigan Tech's ECE Tradition (Opening)**	**Prof. Glen Archer, ECE Interim Chair**
	8:15:00 AM	8:45:00 AM	0.50	Workshop overview and potential synergies	Prof. Chee-Wooi Ten, Associate Professor of Electrical Engineering, MTU
	8:45:00 AM	10:15:00 AM	1.50	**Secure operations technology**	Mr. Andrew Ginter, Waterfall Security
	10:15:00 AM	10:30:00 AM		15-MINUTE BREAK	
	10:30:00 AM	12:00:00 PM	1.50	**Bottom-up electrical vehicle forecasting**	Dr. Pedram Jahangiri, National Grid
	12:00:00 PM	2:00:00 PM		**LUNCH**	
	2:00:00 PM	3:30:00 PM	1.50	**Assessing and Evaluating Risk of Passenger Rail Transportation Systems**	Mr. Joel Langill, AECOM
	3:30:00 PM	3:45:00 PM		15-MINUTE BREAK	
	3:45:00 PM	4:30:00 PM	0.75	**Discussion of today and how to connect tomorrow**	Panelists
	4:30:00 PM	4:45:00 PM		Prepare for dinner	
	4:45:00 PM	6:45:00 PM		**DINNER**	
		Total PE Hours	6.00		

Wednesday, July 31, 2019

	From	To		Events	Speakers
Day 2: Emerging Research	7:00:00 AM	8:00:00 AM		**BREAKFAST**	
	8:00:00 AM	9:30:00 AM	1.50	Cyber insurance for power grid	Prof. Chee-Wooi Ten, Associate Professor of Electrical Engineering, MTU
	9:30:00 AM	9:45:00 AM		15-MINUTE BREAK	
	9:45:00 AM	11:15:00 AM	1.50	"Securities" for system-wide power control and protection	Mr. Koji Yamashita, Senior Research Scientist, Electrical and Computer Engineering, MTU
	11:15:00 AM	1:15:00 PM		**LUNCH**	
	1:15:00 PM	2:45:00 PM	1.50	Emerging threats and case studies	Prof. Yu Cai, Associate Professor, College of Computing, MTU
	2:45:00 PM	3:00:00 PM		15-MINUTE BREAK	
	3:00:00 PM	4:30:00 PM	1.50	Interdependency between grid and transportation	Prof. Wencong Su, Associate Professor of Electrical Engineering, UMich-Dearborn
	4:30:00 PM	5:30:00 PM	1.00	Concluding remarks for the workshop	Panelists
		Total PE Hours	7.00		