SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

SUTD-MIT INTERNATIONAL DESIGN CENTRE (IDC)

Innovation Ready Design

iTrust Centre for Research in Cyber Security

Secure Cyber Physical [SCy-Phy]

Systems Week

June 5 - 9, 2017

Singapore University of Technology and Design

About

SCy-Phy Systems Week 2017

Secure Cyber-Physical Systems Week has been an annual event held at the Singapore University of Technology University (SUTD) since 2015. It is organised by iTrust with support from the Ministry of Defence and the SUTD-MIT International Design Centre (IDC). This year, we have a widespread participation from both local and abroad expertise as well as several Singapore government and private organisations. The event focuses on (cyber) security for industrial control systems, general cyber-physical systems, and IoT. The SCy-Phy Systems Week 2017 includes a two-day Think-in event, the SUTD Security Showdown'17 (S317), and a number of technical in-depth talks, as well as a workshop on Cyber Security Essentials for students.

<table>
<tr><th>5 Jun
(Monday)</th><th>6 Jun
(Tuesday)</th><th>7 Jun
(Wednesday)</th><th>8 Jun
(Thursday)</th><th>9 Jun
(Friday)</th></tr>
<tr><td colspan="2">Think-in</td><td colspan="2">Invited Talks</td><td></td></tr>
<tr><td colspan="3">S317 Reconnaissance</td><td colspan="2">S317 Finals</td></tr>
<tr><td colspan="2"></td><td colspan="2">Workshop on
Cyber Security Essentials
(for students only)</td><td></td></tr>
</table>

Think-in (5 & 6 Jun): Think-in is a two-day event focusing on the theme "Securing Cyber-Physical Systems by Design" held as part of the Third SCy-Phy Systems Week 2017. Think-in will include a sequence of five panel sessions. Each session will be devoted to a specific sub-topic under the general theme led by a panel of experts. These experts will present key issues within the sub-theme and the state of the art techniques and tools to address these issues. Presentation by the panellists will be followed by a discussion involving event attendees focusing on the strengths and limitations of the existing tools and techniques. We hope that these discussions will lead to proposals for further research and potential international collaborations. This year we also included a Design Innovation Micro Experience session facilitated by the SUTD-MIT International Design Centre (IDC).

SUTD Security Showdown'17 (5 - 9 Jun): This is a by-invitation-only event. It consists of two phases: an online qualifier, and a live event held at SUTD. In the live event, qualifying teams from industry and academia team have been invited to attack or defend our Secure Water Treatment (SWaT) and Water Distribution (WADI) testbeds, with the goal to reach a number of defined challenges.

Technical Talks on Cyber Security (7 & 8 Jun): Four speakers with expertise in cyber security have been invited to give an in-depth technical discussion and sharing of insights on a specific area of special interest or their current work in progress. All are welcome to attend.

Workshop on Cyber Security Essentials (for students only) (7 & 8 Jun): This workshop is organised for students to excite and educate them on cyber security. As the younger generation is growing up with cyber-connected systems and devices around them, it is important for them to be aware of the threats they are susceptible to and how they can protect themselves from such threats.

Think-In

Issues of Interest

The five panel discussion for Think-in sessions are *Threats, Interconnected Systems, Models, Defences* and *Translating Research to Industry*. A list of suggested issues for panellists of each session is provided. In addition, panellists are encouraged to address issues, in addition to those listed below, that they consider important.

The overall context of the entire Think-in event is critical infrastructure that includes power grid, water treatment and distribution, transportation and flood control, and selected applications of Cyber-Physical Systems (CPS) such as digital manufacturing, and health care. Panellists are welcome to discuss the potential impact of IoT on the operation of large public infrastructure. While research already published is of interest, we hope that participants will primarily focus on the future aimed at identifying unsolved problems in a realistic context.

Session I: Threats

Current threats to ICS, goals that could be achieved, interest in attacking ICS systems, attacks of tomorrow; similarities and/or difference between attacks on ICS and traditional IT attacks.

Session II: Interconnected Systems

Security threats and potentially defences that are emerging in larger scale systems, systems-of-systems, interdependencies between systems, and similar.

Session III: Models

Bridging formal modelling in security community and physical process models as well as more complex system and attacker models. Verifying the correct operations of an industrial plant, realistic next steps and long-term plan.

Session IV: Defences

Different ways to increase cybersecurity in the ICS context: protocols, industrial embedded devices, process monitoring, including attestation, hardening of legacy devices, intrusion, anomaly detection, and more.

Session V: Translating Research to Industry

Discussion of how to translate academic research into industrial products, success stories (or educational failures), business side of this, specific needs of industry that is not met by academia.

Attendees

Panellists

- Neil Hershfield, ICS-CERT, US Department of Homeland Security
- Alvaro Cardenas, University of Texas at Dallas
- Mauro Conti, University of Padova
- Jorge Cuellar, Siemens AG
- Dieter Gollmann, Hamburg University of Technology
- Gerhard Hancke, City University of Hong Kong
- Robert Kooij, TNO Singapore
- Marina Krotofil, Honeywell Cyber Security Lab
- Matthieu Lec'Hvien, Secure-IC
- Soon Chia Lim, Cyber Security Agency of Singapore
- Sjouke Mauw, University of Luxembourg
- David M. Nicol, University of Illinois at Urbana–Champaign
- David Ong, Excel Marco
- Sahra Sedigh Sarvestani, Missouri University of Science & Technology
- Biplab Sikdar, National University of Singapore

Short biographies of the panellists can be found on page 8.

Moderators

- Aditya Mathur, SUTD
- Nils Tippenhauer, SUTD
- Martin Ochoa, SUTD
- Jianying Zhou, SUTD
- Sudipta Chattopadhyay, SUTD

Think-In

Agenda

5 June 2017 (Monday)		Multi-Purpose Hall
8:00 am	Arrival and Registration	
9:00 am	Welcome Address	Prof Aditya Mathur, Centre Director, iTrust
9:15 am	Keynote Address	Neil Hershfield
10:15 am	Coffee/Tea Break	
Panel 1: Threats Moderator: Nils Tippenhauer		
10:45 am	Managing Cyber Risk: Current Threats and Defensive Strategies for Protecting Industrial Control Systems of Critical Infrastructure It's Time to Face the Truth: Realistic, Real and Unlikely Threats to ICS Threat landscape in Singapore Discussion	Neil Hershfield Marina Krotofil Lim Soon Chia
12:00 pm	Lunch	
Panel 2: Interconnected Systems Moderator: Aditya Mathur		
1:30 pm	Assessing Risk to Physical Sytems through Interconnected Cyber Systems Interdependencies and Fault Propagation in Cyber-Physical Systems Assessing the Impact of Cyber-attacks on Interdependent Critical Infrastructures Discussion	David Nicol Sahra Sarvestani Robert Kooij
3:00 pm	Coffee/Tea Break	
Panel 3: Models Moderator: Sudipta Chattopadhyay		
3:30 pm	Challenges in Security Modelling of Cyber-Physical Systems Adversary Models in Industrial Control Systems Model-based Security Analysis for CPS Discussion	Sjouke Mauw Alvaro Cardenas Dieter Gollmann
5:00pm	End	

Think-In

Agenda

6 June 2017 (Tuesday)	Multi-Purpose Hall	
Panel 4: Defences Moderator: Jianying Zhou		
9:00 am	Device Attestation, Software Updates, and Data Protection Hardware Platform Security for IIoT Anomaly Detection in Cyber-Physical Systems: The Physical Law Approach Discussion	Mauro Couti Gerhard Hancke Biplab Sikdar
10:30 am	Tea/Coffee Break	
Panel 5: Translating Research to Industry Moderator: Martin Ochoa		
11:00 am	Securing IoT: Not an Easy Task Data Mining for efficient physical attacks on Cyber Physical Systems ICS Security Discussion	Jorge Cuellar Matthieu Lec'Hvien David Ong
12:30 pm	Lunch	
1:30 pm	**IDC Micro-Design Experience**	
3:00 pm	Tea/Coffee Break	
3:30 pm	Results of BATADAL, and Lightning talks on iTrust Research Projects • Advancing Security of Public Infrastructure using Resilience and Economics • Cyber Physical System Protection • Research & Security Innovation Lab for IoT	
4:15 pm	Open discussion	
5:15 pm	Closing note	

Biographies

Session 1: Threats

Neil Hershfield is the Deputy Director of the U.S. Department of Homeland Security's (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). ICS-CERT operates within the National Cybersecurity and Integration Center (NCCIC), to bring a control systems focus to the mission of protecting the Nation's critical infrastructure from physical and cyber threats.

The goal of the ICS-CERT is to guide a cohesive effort between government and industry to reduce the cyber risk to industrial control systems. The ICS-CERT provides guidance and reduces risk to critical infrastructure control systems by: leading the Common Strategy to Secure Control Systems; operating the ICS-CERT for control systems related vulnerabilities, threats and incidents; creating informational products and tools to assist vendors and owners/operators in designing, procuring, installing, and operating controls systems to mitigate risks; and performing outreach activities and improving awareness in the control system community through training and education.

Neil received a BS in Chemistry from the University of Wisconsin – Eau Claire and an MBA from Northwood University. Away from work, Neil enjoys golf and cycling.

Marina Krotofil is a Cyber Security Researcher at the Honeywell Industrial Cyber Security Lab in Atlanta, USA. Her previous experience includes working as a Senior Security Consultant at the European Network for Cyber Security, Netherlands and as a Research Assistant at Hamburg University of Technology, Germany. Her research over the last few years has been focused on discovering novel attack vectors, engineering practical cyber-physical attacks and on the design of process-aware defensive solutions and risk assessment approaches.

Marina is the author of more than 15 academic papers and several whitepapers on cyber-physical security. She is also the author of the Damn Vulnerable Chemical Process framework – an open-source platform for cyber-physical security experimentation based on the realistic models of chemical plants. Marina teaches workshops on cyber-physical exploitation and is a frequent speaker at the leading security stages around the world. She holds a MBA in Technology Management, MSc in Telecommunication and MSc in Information and Communication Systems

Lim Soon Chia is Director (Technology) of Cyber Security Agency. In his current role, he is responsible for capability development, evaluation and certification, technology management, and R&D for cyber security.

Mr Lim started his career with the Ministry of Defence and the Republic of Singapore Airforce (RSAF) where he held several senior leadership appointments. He was the Deputy Chief Research and Technology for Operations, and C4 (Command, Control, Communications and Computer) of Defence Research and Technology Office (DRTECH), from 2004-2013. Before retiring from the Airforce, he was Deputy Head Air Operations, responsible for driving Command, Control, Communications and Cyber (C4) ops developments in the RSAF.

Session 2: Interconnected Systems

David M. Nicol is the Franklin W. Woeltge Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign, and Director of the Information Trust Institute. Previously he held faculty positions at the College of William and Mary and at Dartmouth College.

David's research interests include high-performance computing, simulation modeling and analysis, and security. He was elected Fellow of the IEEE and Fellow of the ACM for his contributions in those areas. He is co-author of the widely used textbook Discrete-Event Systems Simulation and was the inaugural awardee of the ACM Special Interest Group on Simulation's Distinguished Contributions Award, for his contributions in research, teaching, and service in the field of simulation.

Sahra Sedigh Sarvestani Dr. Sahra Sedigh Sarvestani is an Associate Professor of Electrical and Computer Engineering and a Research Investigator with the Intelligent Systems Center at the Missouri University of Science and Technology. Her current research centers on development and modeling of dependable networks and systems, with focus on critical infrastructure. She received the B.S. degree from the Sharif University of Technology and the M.S. and Ph.D. degrees from Purdue University, all in electrical engineering. She is a Fellow of the National Academy of Engineering's Frontiers of Engineering Education Program and held a Purdue Research Foundation Fellowship from 1996 to 2000. She is a member of IEEE-HKN and ACM and a senior member of the IEEE.

Robert Kooij has a background in mathematics: he received his PhD degree cum laude at Delft University of Technology, in 1993. From 1997 until 2003 he was employed at KPN, the largest telecom operator in the Netherlands. Since 2003 he is employed at TNO, the Netherlands Organization of Applied Scientific Research. In 2011 he became Principal Scientist, conducting and managing research on Critical ICT Infrastructures.

Since 2005 Robert is part-time affiliated with the Delft University of Technology, at the faculty of Electrical Engineering, Mathematics and Computer Science. Since 2010 he is a part-time full professor with the chair “Robustness of Complex Networks”. In 2016 prof. Kooij relocated to the TNO South-East Asia office in Singapore.

Session 3: Models

Sjouke Mauw is full professor in "Security and Trust of Software Systems" at the University of Luxembourg in the Computer Science and Communications Research Unit. He was associate professor (UHD) in computer science at the Eindhoven University of Technology, with a part time secondment as senior researcher at CWI (Center of Mathematics and Computer Science) in Amsterdam. He received his master's degree in Mathematics (1985) and his PhD degree in Computer Science (1991) from the University of Amsterdam. He graduated on the Ph.D. thesis PSF - A process specification formalism under the supervision of Prof. J.A. Bergstra and Dr. J.C.M. Baeten.

His research focuses on the application of formal methods in the area of information security. Keywords: security protocols, security assessment, privacy, attack trees, DRM, RFID, Trust. Sjouke Mauw has performed research in other areas, such as visual specification languages, concurrency theory, algebraic specification, term rewriting, domain specific languages, testing, distributed algorithms, internet applications. He was member of many scientific committees and organized a number of workshops.

Alvaro Cardenas is an Assistant Professor at the Department of Computer Science at the University of Texas at Dallas, where he is a member of the Cyber Security Research and Education Institute. He holds M.S. and Ph.D. degrees from the University of Maryland, College Park. Before joining UT Dallas he was a postdoctoral scholar at the University of California, Berkeley, and a research staff at Fujitsu Laboratories of America in Sunnyvale California.

His research interests focus on computer security, cyber-physical systems, network intrusion detection, and wireless networks. He is the recipient of the NSF CAREER award, best paper awards from the IEEE Smart Grid Communications Conference and the U.S. Army Research Office, and a Graduate School Fellowship from the University of Maryland.

Dieter Gollmann received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria, where he was a research assistant in the Department for System Science.

He was a Lecturer in Computer Science at Royal Holloway, University of London, and later a scientific assistant at the University of Karlsruhe, Germany, where he was awarded the 'venia legendi' for Computer Science in 1991. He rejoined Royal Holloway in 1990, where he was the first Course Director of the MSc in Information Security. He moved to Microsoft Research in Cambridge in 1998. In 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology, Germany.

Dieter Gollmann is an editor-in-chief of the International Journal of Information Security and an editor of the IEEE Security & Privacy Magazine. His textbook on 'Computer Security' has appeared in its third edition.

Session 4: Defences

Mauro Conti is an Associate Professor at the University of Padua, Italy. He obtained his Ph.D. from Sapienza University of Rome, Italy, in 2009. After his Ph.D., he was a Post-Doc Researcher at Vrije Universiteit Amsterdam, The Netherlands. In 2011 he joined as Assistant Professor the University of Padua, where he became Associate Professor in 2015. In 2017, he obtained the national habilitation as Full Professor for Computer Science and Computer Engineering. He has been Visiting Researcher at GMU (2008, 2016), UCLA (2010), UCI (2012, 2013, 2014), TU Darmstadt (2013), UF (2015), and FIU (2015, 2016). He has been awarded with a Marie Curie Fellowship (2012) by the European Commission, and with a Fellowship by the German DAAD (2013).

His main research interest is in the area of security and privacy. In this area, he published more than 170 papers in topmost international peer-reviewed journals and conference. He is Associate Editor for several journals, including IEEE Communications Surveys & Tutorials and IEEE Transactions on Information Forensics and Security. He was Program Chair for TRUST 2015, ICISS 2016, WiSec 2017, and General Chair for SecureComm 2012 and ACM SACMAT 2013. He is Senior Member of the IEEE.

Biplab Sikdar received his B. Tech degree in electronics and communication engineering from North Eastern Hill University, Shillong, India, M. Tech degree in electrical engineering from Indian Institute of Technology, Kanpur and Ph.D in electrical engineering from Rensselaer Polytechnic Institute, Troy, NY, USA in 1996, 1998 and 2001, respectively.

His research interests include wireless MAC protocols, transport protocols, network security and queuing theory. His research has been funded by the National Science Foundation, DARPA, Intel Corporation and WiMAX Forum.

Sikdar is a member of Eta Kappa Nu and Tau Beta Pi and served as an Associate Editor of the IEEE Transactions on Communications from 2007-2012.

Gerhard Hancke obtained M.Eng and B.Eng degrees from the University of Pretoria (South Africa) in 2002 and 2003, and a PhD in Computer Science with the Security Group at the University of Cambridge's Computer Laboratory in 2008. He subsequently worked at Royal Holloway University of London, first as researcher with the ISG Smart Card Centre and later as Fellow with the Information Security Group. In 2013, he joined the City University of Hong Kong as Assistant Professor.

Gerhard's broad research interests are in system security and distributed sensing, with his particular focus at the moment being the Internet-of-Things and its industrial/cyber-physical applications. He is the Chair of the IEEE Industrial Electronics Society's Technical Committee on Cloud and Wireless Systems for Industrial Applications, and Associate Editor of the IEEE Transactions on Industrial Informatics. He is a registered Chartered Engineer (CEng) with the UK Engineering Council, and a senior member of the IEEE.

Session 5: Translating Research to Industry

Jorge Cuellar is a principal research scientist at Siemens AG. He was awarded the DI-ST Award for the best technical Achievement for his work on modelling of operating systems and transaction managers.

He has worked in several topics, including performance analysis, on learning algorithms, hand-writing recognition, formal verification of distributed system design, and security and he has co-authored 50 publications. He has done technical standardization work on privacy and security protocols at the IETF, 3GPP, and the Open Mobile Alliance. He has worked in several EU funded research projects, mostly on security topics. He regularly serves in Program Committees for international conferences and he has held many short term visiting teaching positions, in different Universities around the world.

Matthieu LEC'HVIEN graduated with a Master of Engineering in Computer Science from ECAM Rennes (France) and a Master of Science in Signal Processing from Rennes 1 University (France). He has been working 6+ years in Hardware Security in Secure-IC, one of the world's leader in the Security of Embedded Systems and Connected Objects. Since 2013 he leads the R&D lab in Singapore. He is also Product Line Manager on a software solution bringing Data Mining and Machine Learning techniques to Embedded Systems Security Evaluation.

Working alongside the top scientists in the field, Secure-IC provides security technologies and expertise for any electronic embedded system to protect them against attacks and guarantee at each stage of the design process that the security level reached is optimal.

David Ong has over 20 years of professional experience and is widely recognized as an active professional in process automation safety industries. He is a CFSE (Certified Functional Safety Expert) and has obtained his MBA from the University of Louisville. He is also a member of the advisory board of CFSE Governance Board and is the Founder of both companies - Excel Marco and Attila Cybertech. During the course of his career, he has executed many major projects in the Oil & Gas industry both onshore and offshore on Process Automation Safety & Control. Having involved with many major Oil companies such as Esso, Shell, Sinopec, PetroChina, Total, Mobil, Unocal, he is well versed with the corporate standards and practices of these companies and has also helped to develop key product marketing specifications for safety PLC and SIS (Safety Instrumented Systems) in general. Over the years, he has maintained focused on Safety PLC related application and was involved in conducting training on Functional Safety Standards and Practices.

David also developed a strong interest in Cyber-Physical Systems (CPS) and he setup Attila Cybertech – an affiliated company of Excel Marco, focusing on Critical Information Infrastructure (CII) sectors. His principal work responsibilities include business development, marketing, major project management/advisor, training on safety and reliability standards and applications.

Technical Talks

June 7, 2017

Venue: LT3, Building 2, Level 4

09:30 am ***Privacy and Security with Green Computer Interfaces***
Prof Dieter Gollmann
Hamburg University of Technology

10:30 am Refreshments

11:00 am ***Privacy-preserving publication of social network graphs***
Prof Sjouke Mauw
University of Luxembourg

June 8, 2017

Venue: LT3, Building 2, Level 4

09:30 am ***Prepare to be Exploited: The End of Perimeter Protection***
Ms Marina Krotofil
Honeywell Cyber Security Lab

10:30 am Refreshments

11:00 am ***Model-Based Fortification of Large-Scale Cyber-Physical Systems***
Dr Sahra Sarvestani
University of Science & Technology

Workshop on Cyber Security Essentials

June 7 & 8, 2017

Venue: LEET Lab, Building 1, Level 6

09:00 am Introduction

09:15 am Advanced Computing

10:45 am Introduction to Ciphers

12:15 pm Lunch

13:30 pm Cyber Attacks

15:30 pm Tea-break

16:00 pm Testbeds Tours

Advanced Computing

Participants will be introduced to Command Line Interface of the PC that gives them important information of their computer/devices they are using. They will also learn how to setup their own Local Area Network using a simulation programme.

Introduction to Ciphers

With the transmission of data from personal devices, personal data could easily be eavesdropped. Participants will learn to create their own ciphers and pair up to "break" others. They will also understand how modern ciphers are implemented in the digital world.

Cyber Attacks

Participants will be introduced to common cyber attacks (e.g. Denial of Service, Password Attacks, SQL Injection, XSS and Ramsonware) and how to guard themselves against such attacks and minimise the impacts.

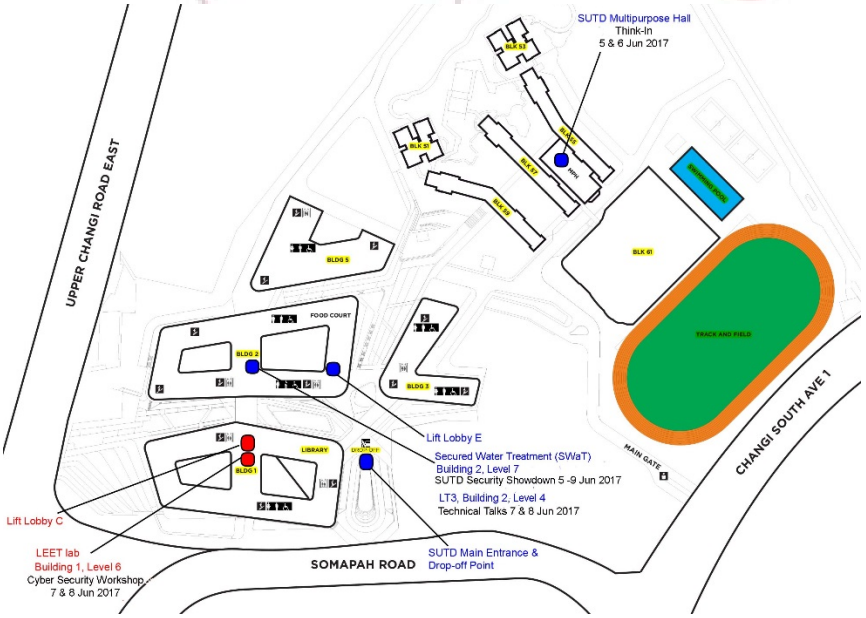
Testbeds Tours

Participants will tour the four testbeds of iTrust and observe the impacts of Industrial Control System (ICS) attacks in such systems (SWaT, WADI, IoT and EPIC).

Acknowledgement

Organising Committee

General Chair	*Aditya Mathur*
Programme Chair	*Nils Ole Tippenhauer*
S317 Chairs	*Nils Ole Tippenhauer* *Martin Ochoa*
S317 Contributors	*Daniele Antonioli* *John Henry Castellanos Alvarado* *Juan David Guarnizo Hernandez* *Sandra Siby* *Ahnaf Siddiqi* *Hamid Ghaeini* *Ragav Sridharan* *Francesco Scandola* *Amit Subhashchandra Tambe* *Randolph Wong* *Sridhar Adepu* *Kaung Myat Aung* *Muhamed Zhaffi Bin Mohamed Ibrahim*
Local, Travel Arrangement & Publicity	*Angie Ng* *Mark Goh* *Priscilla Pang*
Cyber Security Workshop	*Ivan Lee* *Francisco Furtado*



For any enquiries, please email to ***iTrust@sutd.edu.sg***

Please check out our website for the latest update on the programme.