+ Law an der Hochschule Luzern – Wirtschaft. Zudem ist sie Dozentin für Informatikrecht an verschiedenen Nachdiplomstudiengängen, welche am Institut für Wirtschaftsinformatik der Hochschule Luzern durchgeführt werden. Die Autorin ist hauptsächlich im Bereich Informatikrecht und Datenschutz tätig.

Dagstuhl Manifesto

Schloss Dagstuhl is a place where computer science researchers and practitioners meet to discuss research outside the strict format of traditional conferences. Founded in 1990, it has earned an international reputation as an incubator for new ideas. Schloss Dagstuhl hosts over 50 seminars each year which are organized by leading researchers in a field. In this series, they present their results and visions.

SCHLOSS DAGSTUHL
Leibniz-Zentrum für Informatik

Network Attack Detection and Defense: Securing Industrial Control Systems for Critical Infrastructures

Marc C. Dacier (Qatar Computing Research Institute (QCRI), QA)
Frank Kargl, Rens van der Heijden (Universität Ulm, DE)
Hartmut König (BTU Cottbus, DE)
Alfonso Valdes (University of Illinois – Urbana Champaign, US)

From July 13–16, 2014, more than 30 researchers from the domain of critical infrastructure security met at Schloss Dagstuhl to discuss the current state of security in industrial control systems.

The last years have highlighted the fact that security precautions of information and communication technology (ICT) in many critical infrastructures are clearly insufficient, especially if considering targeted attacks carried out by resourceful and motivated individuals or organizations. This is especially true for many industrial control systems (ICS) that control vital processes in many areas of industry that are relying to an ever-larger extent on ICT for monitoring and control in a semi or fully automated way. Causing ICT systems in industrial control systems to malfunction can cause huge economic damages or even endanger human lives. The Stuxnet malware that actually damaged around 1000 Uranium enrichment centrifuges in the Iranian enrichment facility in Natanz is the most well-known reported example of an ICT attack impacting ICS[1], but many similar examples have been published. The proliferation of sophisticated Stuxnet-like malware (e. g., Duqu[2,3], Flame[4], or Gauss[5]) shows how imminent the threat is and how limited our detection and response countermeasures are.

This situation led to increased efforts in research which resulted in a number of related Dagstuhl seminars of which this seminar is a follow-up event, namely two Dagstuhl seminars on *"Network Attack Detection and Defense"* in 2008 and 2012 and one on *"Securing Critical Infrastructures from Targeted Attacks"* held in 2012.

The main objective of this seminar was to discuss new approaches and ideas on how to detect attacks on industrial control systems and how to limit the impact on the physical components. This is closely coupled to the question of whether and how reactive security mechanisms like Intrusion Detection Systems (IDS) can be made more ICS- and process-aware. To some extent it seems possible to adopt existing security approaches from other areas (e. g., conventional networks, embedded systems, sensor networks, robotics) and one of the questions is whether adopting these approaches is enough to reach the desired security level in the specific domain of industrial control systems, or if approaches specifically tailored for ICS or even single installations provide additional benefits.

The seminar brought together junior and senior experts from both industry and academia. It was kicked-off by a presentation from Gunnar Bjoerkman from ABB who presented *"Examples of cyber-attacks on SCADA systems for the electrical grid and their consequences"*. Based on results from the FP7 project VIKING[6], he described several scenarios of possible cyber-attacks on SCADA systems used for the supervision

[1] http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/
[2] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet_research.pdf
[3] http://en.wikipedia.org/wiki/Duqu
[4] http://en.wikipedia.org/wiki/Flame_(malware)
[5] http://www.securelist.com/en/analysis/204792238/Gauss_Abnormal_Distribution
[6] http://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/p/v

and control of the electrical grid, some of which were inspired by real events like Stuxnet, and underlined that some attacks could have really severe consequences. Furthermore, he explained how the CySeMoL method can be used to calculate attack probabilities.

On the second day, another plenary talk was given by Alvaro Cardenas from UT Dallas, who presented his work *"Towards Resilient Control of Critical Infrastructures"*. He argued that today's control mechanisms were designed for safety, fault-tolerance and robustness, but that future designs could be extended towards resilient control algorithms that also consider a strategic attacker. This can lead to new forms of ICS security mechanisms that effectively limit the negative impact that attacks on ICS can have and that can survive their mission critical objectives even when successful attacks have breached traditional security mechanisms. He also showed use-cases in industrial process control of anaerobic and chemical reactors, and in frequency control as well as demand-response control in the power grid to illustrate this concept.

The final plenary talk was devoted to the *"Security of Train Control Systems"* and was given by Stefan Katzenbeisser from TU Darmstadt. He used the train system to illustrate a more unusual form of a control system that not many security researchers have analyzed in details. He gave an overview of the technical systems providing safe train operations in Germany and discussed safety and security problems raised by these deployed systems. He also reported on an ongoing work he is involved in that attempts to provide IT security recommendations for the railway industry, ranging from risk analysis and security-aware design up to security management aspects, while also providing a survey of open research problems in this domain.

Short talks were given by Ulrich Flegel from Infineon (*"ICS Security – Challenges, State of the Art and Requirements"*), Dina Hadziosmanovic from TU Delft ("*Secure Our Safety: Building Cyber Security for Flood Management*"), Marina Krotofil from Hamburg University of Technology (*"Are you threatening my Hazards"*), Heiko Patzlaff from Siemens (*"Forensics in Industrial Control Systems"*), Andreas Paul and René Rietz from BTU Cottbus (*"Security Assessment and Intrusion Detection for Industrial Control Systems"*), and Konrad Rieck from University of Göttingen (*"Automatic Analysis of Unknown Network Protocols"*).

All talks were followed by extensive discussions on the respective topics. Furthermore, participants formed four working groups to address specific topics. One of these groups focused on "*Forensic Analysis in ICS*", others on "*Security Consequences and Quantified Risk Analysis*", the role of security in future forms of industrial control systems, often termed "*Industry 4.0*", and finally one on the "*Detection of Cyber-Physical Systems (CPS) attacks (in Real-Time)*".

The forensics group discussed how forensic analyses in the ICS context can be made more efficient, or even feasible in the first place. One option is to employ methods from machine learning to automate certain steps of the forensics process, which helps especially initially to filter out data. The WG also found that the central difference in terms of forensics between conventional ICT systems and ICS can also be seen as an opportunity: Context aware analysis makes it feasible to take semantics of operational data into account. However, ICS components, especially programmable logic controllers (PLCs), are often not able to support forensic analysis.

In the security consequences group, participants discussed how classical security and risk analysis applies to ICS and the various approaches that are available in literature today. In the Industry 4.0 group, researchers first tried to clarify and distinguish between ICS, cyber-physical production systems and what is recognized as Industry 4.0. Also other more unorthodox forms of ICS, e. g., dyke control systems or industrial farming, were discussed. Many of such systems pose additional security challenges, such as security scalability arising from greater decentralization, which results in data replication and synchronization issues requiring distribution of an increasing number of inexpensive embedded systems spread over a wide area. A potential reduction of production is an impact that is often overlooked when focusing only on critical infrastructures and treating availability as a binary characteristic. Finally, the detection group focused on the question whether detection of semantic attacks on ICS is still a matter of IT security or rather a matter of more resilient safety and robustness. It was also identified that ICS often fail to implement even the most basic security best practices and that often what is needed in real-world systems is security consulting rather than security research. Still, on-going research is required to address more sophisticated security threats.

In the end, this seminar led to a number of important conclusions and open research challenges that participants agreed should provide important directions for the future of ICS security research and practice:

1. Can Intrusion Detection Systems actually provide better security by becoming "process-aware", i. e., have detailed information about the process that the ICS controls? While this seems intuitive, others argue that everything done in this direction is simply replicating the control system and provides redundancy but not necessarily better security.
2. The interaction between safety and security mechanisms is an important aspect and needs further analysis. While today often treated separately, we think that both areas should work more closely together to work on unified mechanisms.
3. ICS, also those beyond Critical Infrastructures, should generally have "last-line-of-defense" monitoring and safety mechanisms that are not connected and not coupled with the potentially attackable ICS. Those mechanisms should provide a ground truth to operators and prevent the system from entering clearly forbidden states.
4. Proper reactions to attacks are often very hard to determine for ICS, as a sudden shutdown or disconnection may not be a viable option. ICS security mechanisms like Intrusion Detection and Prevention Systems should therefore be able to provide a flexible reaction to detected security breaches to allow a form of "graceful degradation". So as in the case of safety mechanisms, ICS should enter more robust and fail-safe states when attacks are detected, perhaps to the detriment of efficiency and output of the controlled process.
5. More attention should be paid to user interfaces of security mechanisms to allow operators and security experts appropriate analysis and reaction if attacks cause critical situations.
6. Security systems should provide more fine-grained output to allow better forensics and proper reaction to incidents.
7. We identified a huge gap between ICS security research in academia and industrial practice. While research targets highly sophisticated attacks and countermeasures, many real-world deployments fail because of lack of even the most simple security best-practices. Closing this gap will require a huge effort that should start with identifying which best-practices have to be applied and which do not fit.
8. ICSs also pose big challenges for security management because of the huge scale of some installations, the lack of realistic attacker models that would allow one to find the right level of security, and the economic pressure to build cost-effective security solutions.
9. In general, diversity and redundancy are good for ICS security. If a large number of ICSs are from a single vendor and use only one brand of devices, attacks and malware can easily spread and create huge damage. It is therefore not clear yet, whether convergence of ICS to a few vendors and standards (in terms of protocols, operating systems, etc.) will provide more benefits to attackers or to defenders.
10. The fact that ICSs are often very long-lived installations and that duration of innovation cycles in ICSs is very different from ICT creates huge problems for maintaining ICS security. Well-defined, certified update processes that are guaranteed for the lifetime of ICSs would significantly support security. However, maintaining own ICS software ecosystems also has economic consequences.
11. Separation and isolation (like air gaps, virtualization, sandbox, VPNs) are likely the most effective security mechanisms for ICS. As a corollary, this means that multi-stakeholder ICS like power grids are inherently harder to secure, as they require more interfaces between parties.
12. While ICS is a very broad term and encompasses a lot of extremely heterogeneous types of systems, participants were confident that the security challenges to be addressed are often very similar and thus that there can be meaningful progress on ICS security in general without the need to divide the field into further sub-disciplines.

We want to thank all participants of the Dagstuhl seminar that contributed to reach these conclusions. A list of participants and additional information on the seminar can be found at http://www.dagstuhl.de/14292.