

Securing Critical Infrastructures from Targeted Attacks

Edited by

Marc Dacier¹, Frank Kargl², and Alfonso Valdes³

1 Symantec Research Labs – Sophia Antipolis, FR, Marc_Dacier@symantec.com

2 Universität Ulm, DE, frank.kargl@uni-ulm.de

3 University of Illinois – Urbana, US, avaldes@illinois.edu

Abstract

This report documents the program and the outcomes of Dagstuhl Seminar 12502 “Securing Critical Infrastructures from Targeted Attacks”. Through a series of presentations, discussions, and working group meetings, the seminar achieved to shape a clearer picture of what actually constitutes a targeted attack on a critical infrastructure and defined the terms PEST (persistent, sophisticated and targeted) attacks and Critical Cyber Infrastructure in this context. This clearer view will hopefully help the research community and industry to address such threats in a more consistent and holistic way.

Seminar 09.–12. December, 2012 – www.dagstuhl.de/12502

1998 ACM Subject Classification K.6.5 Security and Protection

Keywords and phrases Critical Infrastructures, Targeted Attacks, Security


Digital Object Identifier 10.4230/DagRep.2.12.49

1 Executive Summary

Frank Kargl

Mark Dacier

Alfonso Valdes

License  Creative Commons BY-NC-ND 3.0 Unported license
© Frank Kargl, Mark Dacier, and Alfonso Valdes

The last years have highlighted the fact that our ICT security precautions in many critical infrastructure (CI) systems are clearly insufficient, especially if considering targeted attacks carried out by resourceful and motivated individuals or organizations. Critical infrastructures, like energy or water provisioning, transportation, telecommunication, or health support are relying to an ever-larger extent on ICT, often being monitored or controlled in a semi or fully automated way. Disruption of these control processes could turn out to be disastrous, especially as many of these systems are cyber-physical systems that interact with the real world through sensors and actuators and can thus have a direct influence on the physical world not mediated by the common sense of a human being.

Rendering ICT systems in such critical infrastructure unusable or malfunctioning can cause huge economical damages or even endanger human lives. Some examples: it is reported by the Institute for Science and International Security (ISIS) in December 2010¹ that the Stuxnet malware actually damaged around 1000 Uranium enrichment centrifuges in the

¹ <http://www.isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>



Except where otherwise noted, content of this report is licensed under a Creative Commons BY-NC-ND 3.0 Unported license

Securing Critical Infrastructures from Targeted Attacks, *Dagstuhl Reports*, Vol. 2, Issue 12, pp. 49–63

Editors: Marc Dacier, Frank Kargl, and Alfonso Valdes



DAGSTUHL
REPORTS

Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Iranian enrichment facility in Natanz (which was possibly its goal). If the same would happen in a European Uranium enrichment facility, the economical damage would be significant and danger to population due to failure of systems could not be ruled out completely. In 2000, an insider attack on a sewage treatment facility in Queensland, Australia caused millions of liters of raw sewage to spill out into local parks and rivers². The CIP Vigilance Blog collects a long list of such issues³.

There are many similar examples where Industrial Control Systems (ICS) have been affected due to insufficient security precautions. Moreover, the apparent success in infiltrating Critical Infrastructure environments is calling attention on the ineffectiveness of standard security mechanisms in detecting similar attacks. Stuxnet is believed to have been operating undetected for almost one year leveraging multiple vulnerabilities that were previously unknown, and has been discovered only as a consequence to an operational anomaly that triggered the attention of the field operators. This fact clearly shows that not only our security mechanisms in ICS are insufficient, but that even our methods to find vulnerabilities and detect ongoing or successful attacks in Critical Infrastructure environments are not up to their task. It is very likely that Stuxnet could be the “first of a kind”, as demonstrated by the recent apparition of the so-called Duqu threat, apparently based on the same code (see the Symantec thorough analysis for more on this topic⁴).

Similar argumentation can be applied to other forms of control systems like Intelligent Transport Systems, modern health systems, Smart electric grids, and many more. The advanced metering infrastructures (AMI) now being deployed in some form on the electric grids of many countries offers potential benefits in terms of reduction of peak load, which in turn enables green house gas reduction and various economic benefits. However, it introduces potentially hundreds of millions of computationally limited networked endpoints outside of a defensible physical or electronic perimeter. Moreover, smart grids may be subject to attacks that do not require an adversary to compromise a device, whether a smart meter on a residence or a phasor measurement unit (PMU) that contributes to wide area measurement or state estimation. Real-time price signals communicated to smart meters may induce volatility, and if spoofed may lead to destabilizing load fluctuation (see [1]). Spoofing of GPS signals can cause PMUs to lose synchronization, resulting in threats to real-time control and corrupt grid state estimation.

There are many challenges involved in this, especially the heterogeneity of the systems that often involve legacy and proprietary system where not even all specification might be available to security engineers. High dependability and availability requirements of such systems often do not allow fast update cycles in case of security vulnerabilities are disclosed. The trend to use more COTS hardware and software in such systems creates problems and opportunities at the same time. A problem is that all malware that is available in such systems suddenly also becomes available to attackers on Critical Infrastructure ICT and that a lot of known vulnerabilities become exploitable. On the pro side, many established security mechanisms like firewalls, Intrusion Detection Systems, or OS security mechanisms like malware scanners can be applied. However, you often need to specifically adjust them for the new domain (e.g., by having SCADA specific signatures for an IDS). At the same time, the different (dependability) requirements and different applications in Critical Infrastructure

² http://www.theregister.co.uk/2001/10/31/hacker_jailed_for_revenge_sewage/

³ <http://ciip.wordpress.com/2009/06/21/a-list-of-reported-scada-incidents/>

⁴ http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

Systems often require new or updated approaches, e.g., regarding security updating or security testing methodologies.

The research community has taken up this challenge, as can be seen by the emergence of specific research projects (e.g., EU projects like ReSIST, IRIIS, VIKING, SERSCIS, INSPIRE, CRUTIAL, CRISALIS), and regular contributions on the topic at conferences and workshop (RAID, DIMVA, CCS, LEET, IEEE SSP, NDSS, Usenix Security, etc.). The US Department of Homeland Security and Department of Energy fund numerous projects under programs such as the National SCADA Test Bed (NSTB) and Cyber Security for Energy Delivery Systems (CSEDS). However, we identified that the research community would benefit from being better connected, having identified a clear list of major research challenges, and knowing to what extent they have been addressed so far. Stemming from this motivation, we proposed this Dagstuhl research seminar with the goal to bring together leading researchers both from academia and industry to discuss and evaluate the state of the art and to highlight where sufficient solutions exist today, where better alternatives need to be found, and also to give directions where to look for such alternatives.

One of the most important aspects was to identify whether security challenges and solutions apply to all different areas of CI, be it water, electricity, gas, transport, health-support, public safety infrastructures, or tele-communication. Our initial expectation was that there would be clusters of domains with very similar profiles on the one hand, but also large differences between clusters. This, however, was not clear previously, as many security researchers focused on specific areas or specific aspects of security.

Beyond, during the seminar we also focused on the question how targeted attacks on CI differ from ubiquitous unspecific attacks by malware or occasional hackers. As the later do not focus specifically on CI, they will typically not create large-scale damages — if damages occur, this is typically the consequence of computer systems being down. In contrast, the Stuxnet example illustrates how targeted malware can be injected into target systems in a very stealthy way and can cause subtle damage that can go unnoticed for a long time. Consequently, security countermeasures, reactions, and forensic methods have to differ as well. However, the research community has just started to address the area of targeted attacks.

The seminar started from a set of questions related to this:

- What are the specific security challenges and requirements that are ubiquitous throughout different Critical Infrastructure domains? Where do those domains differ in terms of security?
- What is the status with respect to protection from, detection, and analysis of targeted attacks on Critical Infrastructures? What solutions can be transferred from general ICT? Where have new solutions already been found? Where is further research needed?
- Do these solutions apply to Critical Infrastructures in general, or do we need to work on domain-specific solutions?
- How can the negative effects of successful attacks be contained?
- How can CI be made resilient to attack, and able to maintain critical (possibly degraded) function in the presence of attack?
- How can we bridge the gap between low-level research on the granularity of individual ICT devices or single networks, e.g., to conduct forensic analysis or deploy IDS, on the one hand and on the other the research that assesses the system-wide effects of targeted attacks, e.g., on effect propagation?
- How can technical solutions and organizational policies be aligned and enhanced in a consistent way?

- How can we bridge the gap of knowledge between security experts rarely aware of the specific characteristics of CI systems and CI experts not necessarily up to date with the latest security research outcomes.
- How can we shed some light on CI insecurity without running the risks of opening a Pandora box? What are the consequences of such risks? Are there legal implications to consider?
- How do the approaches of academia and industry in addressing targeted attacks on CI differ?

Many of these questions were addressed during our two and a half day Dagstuhl seminar from December 9 to 12, 2012. We had the envisioned nice mix of participants with an industry participation of over 30 % and experts from various domains of critical infrastructures.

The agenda featured two main plenary talks, nine short presentations, and regular working group breakout sessions. The plenary talks were given by Alvaro Cárdenas Mora from Fujitsu Laboratories of America / UT Dallas who spoke on “Short-term and Long-term research Challenges for Securing Cyber-Physical Systems” and Levente Buttyán from the BME CrySyS Lab who gave us a first hand insight into analysing targeted attack malware in his presentation on “The cousins of Stuxnet: Duqu, Flame, and Gauss”.

The short presentations focussed on a broad variety of topics, some giving broader updates on research agendas and activities like the European CRISALIS project, some others addressing specific areas like train control systems or smart grids. One short talk by Felix Freiling asked the challenging question whether detecting targeted attacks has to be considered impossible by their very nature, a discussion that working group 2 later continued in depth. Other topics addressed in the short presentations included intrusion detection mechanisms for industrial control systems, a report on the CERT run by Siemens, and on societal consequences of cyber attacks on electrical supply systems.

These talks provided perfect input for our working groups. We initially envisioned four working groups with the titles (1) Business Aspects of Security for CI in Different Domains, (2) Attacker Models and Risk Analysis for Targeted Attacks on CI, (3) CI Security in different CI Domains, and (4) Technical Security Approaches for Intrusion Detection and Network Monitoring. However, during initial discussions and working group assignments, groups (1) and (3) found their topics to be closely related and decided to merge.

The merged working groups (1) and (3) first identified the challenge that definitions of what a *Critical Infrastructure* actually is are quite diverse and fuzzy which led to a narrowed down definition of *Critical Cyber Infrastructure* which provided a working definition to then reason about the nature of security incidents and solutions in such systems. One conclusion from their work was that there is a gap between generic IT security and the large number of different CI domains that may be bridged by providing clearer reference scenarios that security researchers can focus on. That way, one could then identify whether generic security solutions can be applied to such scenarios or even cross- scenario or whether specific solutions need to be found.

Working group (2) mostly investigated attacker models for targeted attacks. Again, the term targeted attack was not clear and the first result of the working group was a attack classification scheme to be able to narrow down on this term and distinguish various types of attacks. The group even went beyond the targeted attack term and suggested PEST (persistent, sophisticated and targeted) as a categorization of the most critical types of attacks. In a second meeting, the working group discussed attacker motivations and identified a clear lack of intelligence regarding such motivations. Therefore, a lot today is more guesswork than based on clear facts and more investigations into the nature or PEST attacks seems to be required.

Finally, working group (4) focussed on the technical topic of intrusion detection and network monitoring in ICS, coming up with a list of attack scenarios, technical challenges and ideas for enhancement of countermeasures.

In a final plenary wrap-up discussion, all participants agreed that the seminar's topic was definitely a very challenging one. As both the definition of Critical Infrastructure and Targeted Attack are not even clearly agreed upon and as CIs are so diverse, we were not even able to cover all possible instantiations of CIs by dedicated experts. Especially the work in the working groups provided important first steps towards clearer definition and a common understanding of these issues and as such the seminar has to be considered a success that should be followed up by future activities.

The question whether joint security approaches and solutions for targeted attacks on critical infrastructures can be found can therefore not finally be answered. However, the research community and industry would definitely benefit from a closer cooperation of researchers and practitioners that work on *PEST attacks on Critical Cyber Infrastructures*.

References

- 1 Roozbehani, M.; Dahleh, M.A.; Mitter, S.K., "Volatility of Power Grids Under Real-Time Pricing", Power Systems, IEEE Transactions on , vol.27, no.4, pp.1926,1940, Nov. 2012

2 Table of Contents

Executive Summary

<i>Frank Kargl, Mark Dacier, and Alfonso Valdes</i>	49
---	----

Overview of Talks

Assessment of Social Impact Costs and Social Impact Magnitude from Breakdowns in Critical Infrastructures <i>Gunnar Björkman</i>	55
The cousins of Stuxnet: Duqu, Flame, Gauss <i>Levente Buttyán</i>	55
Short and Long-Term Research Challenges for Protecting Critical Infrastructure Systems <i>Alvaro A. Cárdenas</i>	56
Signature-Less Network Intrusion Detection for Industrial Control Systems <i>Sandro Etalle</i>	57
Detecting Targeted Attacks Considered Impossible <i>Felix C. Freiling</i>	57
On the (In)Security of Train Control Systems <i>Stefan Katzenbeisser</i>	57
The future of Smart Grids <i>Erwin Kooi</i>	57
CRISALIS – Preventing Targeted Attacks on Critical Infrastructures <i>Corrado Leita</i>	58
A CERT for products’ perspective on security <i>Tobias Limmer</i>	58
Smart Grid Security Research <i>Alfonso Valdes</i>	59

Working Groups




Report of Joint Working Groups 1 & 3 <i>Nils Aschenbruck and Working Group 1 & 3 Participants</i>	59
Report of Working Group 2 “Attacker Models for Targeted Attacks” <i>Stefan Katzenbeisser and Working Group 2 Participants</i>	60
Report of Working Group 4 “Technical Security Approaches for Intrusion Detection and Network Monitoring” <i>Damiano Bolzoni, Marco Caselli, Emmanuele Zambon, and Working Group 4 Participants</i>	62

Participants	63
-------------------------------	----

3 Overview of Talks

3.1 Assessment of Social Impact Costs and Social Impact Magnitude from Breakdowns in Critical Infrastructures

Gunnar Björkman (ABB AG – Mannheim, DE)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Gunnar Björkman




This presentation described a method and a tool to calculate societal consequences from outages in the electrical supply. The method and tool have been developed in the EU/Framework 7 project VIKING that was successfully ended in November 2011, see <http://www.vikingproject.eu/>.

Two types of societal consequences from power blackouts were presented; one that calculates the economic losses to society as lost Gross Domestic Product (GDP), i.e. Social Impact Cost (SIC), and the other as a new type of measure for non-economic damages, Social Impact Magnitude (SIM). For the economic loss calculation, SIC, the national GDP is broken down on individual object level, e.g. public services, small and big companies, hospitals, etc., with a high time resolution. The breakdown of GDP makes it possible to calculate the economic activities for smaller parts of the country and for defined times. The economic loss for society is then calculated as the difference in economic activity for a certain geographic part and for a defined time with and without electrical supply considering the stepwise electrical restoration procedures.

The Social Impact Magnitude (SIM) is a new logarithmic measure considering the number of people impacted by the outage and the outage length. Using the 10- logarithm of the outage length in seconds and thousands of people a measure is reached that closely resembles the well-known Richter scale for earthquakes and is very easy to calculate. Applying the SIM measure on previous, well-known power blackouts gives an intuitively very reasonable value, e.g. the 2003 Northeast American blackout gets a value of 9,67, i.e. a very serious disturbance. The intention of the SIM is to be able to classify power outages in an-easy-to-understandable way and to use such classification to plan society responses, e.g. a value below 6 has only regional consequences but values above require a national response.

3.2 The cousins of Stuxnet: Duqu, Flame, Gauss

Levente Buttyán (Budapest Univ. of Technology & Economics, HU)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Levente Buttyán

Joint work of Bencsáth, B.; Pék, G.; Buttyán, L.; Félegyházi, M.

Main reference B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi, “The Cousins of Stuxnet: Duqu, Flame, and Gauss,” in *Future Internet*, Vol. 4, Issue 4, pp. 971–1003, 2012.

URL <http://dx.doi.org/10.3390/fi4040971>

Stuxnet was the first targeted malware that received worldwide attention for causing physical damage in an industrial infrastructure seemingly isolated from the online world.


Stuxnet was a powerful targeted cyber-attack, and soon other malware samples were discovered that belong to this family. This presentation first presented our analysis of Duqu, an information-collecting malware sharing striking similarities with Stuxnet. It described our contributions in the investigation ranging from the original detection of Duqu via finding the

dropper file to the design of a Duqu detector toolkit and then continued with the analysis of the Flame advanced information-gathering malware.

Flame is unique in the sense that it used advanced cryptographic techniques to masquerade as a legitimate proxy for the Windows Update service. The talk also presented the newest member of the family, called Gauss, whose unique feature is that one of its modules is encrypted such that it can only be decrypted on its target system; hence, the research community has not yet been able to analyze this module. For this particular malware, the authors designed a Gauss detector service and we are currently collecting intelligence information to be able to break its very special encryption mechanism. Besides explaining the operation of these pieces of malware, the presentation also examined if and how they could have been detected by vigilant system administrators manually or in a semi-automated manner using available tools. Finally, the talk discussed lessons that the community can learn from these incidents.

3.3 Short and Long-Term Research Challenges for Protecting Critical Infrastructure Systems

Alvaro A. Cárdenas (The University of Texas – Dallas, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Alvaro A. Cárdenas

Our critical infrastructure systems are being modernized with information and communication technologies to face the operational requirements and efficiency challenges of the 21st century. The smart grid in particular, will introduce millions of new intelligent components to the electric grid, buildings, and homes within the next decade. While this modernization will bring many operational benefits to infrastructure systems, it will also introduce new vulnerabilities, a larger attack surface, and raise privacy concerns.

This presentation focused on the short, medium, and long-term research challenges for protecting cyber-physical systems.




As a short-term goal, it discussed some of the incentives (economic or regulation) to develop, deploy, and maintain control systems following security best practices.

In the medium-term discussion, it focused on the large-scale instrumentation being deployed in critical infrastructure, and the advantages of analyzing this data for better security intelligence. The talk exemplified some of these notions with smart grid data being used for electricity theft and anomaly detection.

The final part of the talk focused on long-term research projects and included the fact that we can combine physical dynamical models of the critical infrastructure with information security models to obtain more resilient and survivable systems against targeted attacks. This part of the talk discussed examples for survivable control of a chemical reactor and other generic control systems resilient to false-data injection and DoS attacks.

3.4 Signature-Less Network Intrusion Detection for Industrial Control Systems




Sandro Etalle (TU Eindhoven, NL)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Sandro Etalle

This talk presented a new technology to do network monitoring and intrusion detection on industrial control system networks, and touched on the limits of the classic intrusion detection technology when applied to industrial control systems.

3.5 Detecting Targeted Attacks Considered Impossible




Felix C. Freiling (Universität Erlangen-Nürnberg, DE)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Felix C. Freiling

As a followup to a presentation at the Dagstuhl Seminar 12061, this talk tried to stimulate discussion on what a targeted attack is as opposed to “mass-malware” attacks like Conficker and Storm.

3.6 On the (In)Security of Train Control Systems




Stefan Katzenbeisser (TU Darmstadt, DE)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Katzenbeisser

In the talk, the author described the state-of-the art technologies that are used to safely control trains in the network of German rail. The presentation detailed the future architecture of train control systems, discussed related security aspects and briefly reported on an ongoing project in collaboration with DB Netz that attempts to define the security architecture of next-generation signal boxes.

3.7 The future of Smart Grids


Erwin Kooi (Alliander – Duiven, NL)

License    Creative Commons BY-NC-ND 3.0 Unported license
© Erwin Kooi

The change from a production-follows-demand to a demand-follows-production model introduces challenges for grid operation. These challenges can be addressed by installing more and heavier powerlines or by using data to manage the grid, production and demand more intelligently.

3.8 CRISALIS – Preventing Targeted Attacks on Critical Infrastructures

Corrado Leita (Symantec Research Labs – Sophia Antipolis, FR)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Corrado Leita

The presentation introduced the CRISALIS FP7 project that aims at providing new means to secure critical infrastructure environments from targeted attacks, carried out by resourceful and motivated individuals.


The discovery of highly sophisticated and targeted attacks such as Stuxnet showed that these threats are a reality. Their success in infiltrating Critical Infrastructure environments is calling attention on the ineffectiveness of standard security mechanisms at detecting them.

Stuxnet, for instance, is believed to have been operating undetected for almost one year leveraging multiple vulnerabilities that were previously unknown, and has been discovered only as a consequence to an operational anomaly that triggered the attention of the field operators. This fact clearly shows that our methods to find vulnerabilities and detect ongoing or successful attacks in critical infrastructure environments are not sufficient. The talk gave an overview over the CRISALIS project which aims at filling this gap with practical, short-term solutions.

See <http://www.crisalis-project.eu/> for details.

3.9 A CERT for products' perspective on security

Tobias Limmer (Siemens – München, DE)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Tobias Limmer


Multiple trends in cyber security affect product vendors of industrial IT. On the one hand, the amount of targeted attacks that involve critical infrastructures is rising. On the other hand, attention on non-office IT environments by security researchers is rising. This effect is caused by the adaptation of standards, protocols and paradigms that are prevalent in the office IT world into the industrial world. Attack methodologies that have long been used in standard IT environments can increasingly be reused in industrial environments, easing the work of security researchers, both on the black hat and white hat side.

The heterogeneity of devices is an additional problem, as well as static environments that were implemented with focus on safety. One example regarding static environments is the problem of continuous patch deployment of security updates when acceptance tests are required after each system change. Authentication is another problem, as strong authentication methods contradict with quick information transfer that is needed for safety functions.

Product vendors need to adapt to this changed environment by implementing preventative (e.g., secure development) and reactive (e.g., vulnerability handling) measures and focus on bridging the gap between product security and ease-of-use for customers.

3.10 Smart Grid Security Research

Alfonso Valdes (University of Illinois – Urbana, US)

License  Creative Commons BY-NC-ND 3.0 Unported license
© Alfonso Valdes

Cyber assets in infrastructure systems such as smart electrical grids potentially enable advances in efficiency and resiliency, but are potentially attractive targets for cyber attack. Securing such systems presents particular challenges, since security solutions and practices from conventional enterprise systems are not always applicable. On the other hand, the constrained function and regularity of communication in infrastructure systems allows security solutions based on such approaches as specification-based intrusion detection. This talk summarized work from SRI International and the University of Illinois towards securing cyber assets in infrastructure systems, with an emphasis on smart electric grids.

4 Working Groups

4.1 Report of Joint Working Groups 1 & 3

Nils Aschenbruck and Working Group 1 & 3 Participants

License  Creative Commons BY-NC-ND 3.0 Unported license
© Nils Aschenbruck and Working Group 1 & 3 Participants

The working groups 1 on “Business Aspects of Security for Critical Infrastructure in Different Domains” and 3 on “CI Security in different Critical Infrastructure Domains” decided to merge at the beginning of the seminar. So this is their joint report.

4.1.1 Definition and Classification

For both working groups the idea was to classify the different domains of critical infrastructures first. Then, the plan was to examine business aspects (group 1) and security measures, respectively.

In the literature, there are different classifications. In the US [1], there are 18 critical infrastructures and key resources (CIKR). In the EU [2], there are 9 critical infrastructures. Further examples, e.g., [3], may be found. All the classifications were found to be quite fuzzy, mixing domains and physical infrastructure/facilities, e.g., “banking sector” and “national monuments”. Thus, the working groups decided to focus on selected critical cyber infrastructures, while also considering future development such as intelligent cities and smart power grids.

We reached a rough consensus that a critical cyber infrastructure is characterized by the following attributes: (1) the highest impact attack is a cyber attack; (2) a cyber attack potentially results injury or loss of life (although attacks can have economic consequences, such as energy theft or blackmail) (3) there is specific physical infrastructure involved; (4) there is currently rapid adoption of cyber technology due to powerful business cases for the adoption of automation. Concerning security, the specific differences lie in the targets to attack such as: (1) (distributed) control systems; (2) distributed algorithms; (3) physical entities; (3) supply chain; (4) social engineering.

Compared to a standard IT attack, where the machine itself is the goal, targeted attacks on critical cyber infrastructure often have specific attributes. The attacker has a plan for a

higher goal. By doing so, he may targets specific groups, or classes of assets. This means that the propagation in contrast to a massive attack is (up to infinitely) focused; sometimes just a single machine is attacked. Usually, the attacker has background knowledge and/or part of the attack is getting more detailed knowledge. The attacker is well prepared and has large resources (knowledge, expertise, time, hardware, etc.).

For the targeted critical infrastructures often the following attributes apply: Standard security solutions, e.g., virus updates, can not be used. The systems originally started as isolated systems, but are now connected to enterprise systems due to business incentives (e.g., remote access to SCADA). Furthermore, classical independent safety loops within the industrial control system are now connected to intelligent electronic devices (IED). Thus, the former hardware independence of the safety loops is lost. Moreover, different critical infrastructures are connected; with consolidation of assets in the electric sector, for example, system operators may operate several distinct energy resources as a virtual power plant. By doing so, access control is a big challenge.

4.1.2 Challenges and Future Research Directions


A core challenge is the lack of domain knowledge. The security research is mainly IT driven, nowadays. On a high level, all challenges seem to be trivial as solutions do already exist in the IT domain. On a low level, everything seems to be Ethernet, which is well known in the IT domain as well. However, there are specific challenges for cyber critical infrastructures. But the specific domains have to be understood first. It would be great to have a set of reference scenarios. Such a set could help to understand different domains and to develop, parameterize, and evaluate security solutions for the reference scenarios. By doing so, it could be examined which solutions are applicable across domains. To figure this out is probably the core challenge regarding critical cyber infrastructures. Besides, the supply chain should be addressed as well. Verifying that hardware has no undocumented functionality is a difficult problem.

References

- 1 ICS-CERT FAQ, http://www.us-cert.gov/control_systems/csfaq.html.
- 2 Communication from the Commission to the Council and the European Parliament of 20 October 2004 – Critical Infrastructure Protection in the fight against terrorism [COM(2004) 702 final – Not published in the Official Journal], http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33259_en.htm.
- 3 Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Critical Infrastructures divided by sectors and subsectors, http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Kritis/CI_Sectors_Subsectors.pdf.

4.2 Report of Working Group 2 “Attacker Models for Targeted Attacks”

Stefan Katzenbeisser and Working Group 2 Participants

License  Creative Commons BY-NC-ND 3.0 Unported license
© Stefan Katzenbeisser and Working Group 2 Participants

The main goal of working group 2 was to define an attacker model for attacks on critical infrastructures. The participants agreed that the attacker model should include at least the following dimensions:

Targeted vs. opportunistic attacks: for targeted attacks the set of victims is known and rather small, while opportunistic attackers typically do not know the identity of the victims beforehand and do not target a specific group of victims.

Persistence vs. one-time/one-off: A persistent attacker tries to achieve his goal during a long period of time; the attack evolves over time. Even if the victim cleans her infrastructure, a persistent attacker will come back and try to infect through different paths. On the contrary, mass infections can be classified as “one-time/one-off”; once the system is cleaned and the vulnerability is fixed, the attacker will not come back to a specific victim.

Advanced skills vs. script kiddies: Advanced attacks are resourceful and are willing to devote manpower and time. However, the computational resources of an attacker are not necessarily a good measure for judging the level of sophistication, since botnets can provide virtually unlimited compute power. On the contrary, script kiddies have limited skills and resources.

Well-funded organization vs. hobbyist: Another important dimension is the funding available for carrying out the attack.

High impact vs. low impact: The impact of a targeted attack needs to be taken into account, where impact is measured by the damage potential per victim.

Lots of intelligence vs. no background information: Attacks against critical infrastructures are often carried out by attackers with a broad knowledge of the system. There are many similarities between targeted attacks and classical intelligence methods (such as placing a spy in the government of a foreign country).

Human, flexible, adaptive attack vs. fully automated attack: We can observe a big difference in sophistication between attacks that are directly controlled by humans and fully automated attacks. The use of human labor can be a bottleneck, but also allows more flexibility. Flexible attacks can also involve human factor issues, such as social engineering.

The working group concluded that attacks against critical infrastructures are typically characterized as being persistent, sophisticated and targeted (PEST).


The second meeting of the working group focussed on the goals of an attacker who is performing a targeted attack. In general, the goals can be very diverse, such as espionage, information gathering, sabotage, blackmailing, destruction, gaining financial advantage and infiltration.

Unfortunately the precise motivation of an attacker is often unclear; we have not much information about the origins of attacks. The often-cited goal of destructing a critical infrastructure is very close to a cyberwar scenario; nevertheless, there can also be situations that are closely related to cybercrime (such as attacks by insiders, terrorist groups, hacker groups and political activists such as anti-nuclear activists).

Regarding the attack strategy, one should distinguish between the intelligence gathering phase and the actual attack. We must assume that an attacker has sufficient expertise to launch multi-stage attacks that evolve over time and that starts with an intelligence gathering phase, which is followed by an execution phase. We must also distinguish between attacks against the processes and the infrastructure. This distinction is reinforced by the fact that an attacker needs to follow different attack paths when he wants to inflict physical destruction or to gain information (for example by stealing classified documents); for the former, the attacker needs to gain access to the production infrastructure. During the attack execution phase, different goals can be achieved such as denial of service, taking control or sabotage; in particular the latter one may be a goal that is not particularly relevant in classical IT-based infrastructures.

4.3 Report of Working Group 4 “Technical Security Approaches for Intrusion Detection and Network Monitoring”

Damiano Bolzoni, Marco Caselli, Emmanuele Zambon, and Working Group 4 Participants

License  Creative Commons BY-NC-ND 3.0 Unported license
© Damiano Bolzoni, Marco Caselli, Emmanuele Zambon, and Working Group 4 Participants

Last but not least, working group (4) focussed on the technical topic of intrusion detection and network monitoring in ICS, coming up with a list of attack scenarios, technical challenges and ideas for enhancement of countermeasures. The participants discussed such diverse approaches as network- and protocol-based analysis or PLC honeypots, including network-based packet-header periodicity analysis that could help operators build better firewall rules. Practical challenges include issues like rogue hardware being introduced into the system by attackers. One conclusion was that some of the more advanced detection countermeasures may not be ripe yet to be implemented by vendors or would require a very high effort to be deployed in production systems. This is definitely a field where research needs to interact even more closely with vendors to come up with solutions to work on joint definitions, reference models and attacks, testbeds, etc., to start a more focussed research with more practical outcome.

Participants

- Magnus Almgren
Chalmers UT – Göteborg, SE
- Nils Aschenbruck
Universität Osnabrück, DE
- Davide Balzarotti
Institut Eurecom – Sophia
Antipolis, FR
- Rafael Barbosa
University of Twente, NL
- Gunnar Bjoerkman
ABB AG – Mannheim, DE
- Damiano Bolzoni
University of Twente, NL
- Levente Buttyan
Budapest Univ. of Technology &
Economics, HU
- Alvaro Cárdenas Mora
The Univ. of Texas – Dallas, US
- Marco Caselli
University of Twente, NL
- Marc Dacier
Symantec Research Labs, US
- Sandro Etalle
TU Eindhoven, NL
- Felix C. Freiling
Univ. Erlangen-Nürnberg, DE
- Jakob Fritz
EURECOM – Biot, FR
- Elmar Gerhards-Padilla
Fraunhofer FKIE –
Wachtberg, DE
- Dina Hadziosmanovic
University of Twente, NL
- Frank Kargl
Uni Twente, NL & Uni Ulm, DE
- Stefan Katzenbeisser
TU Darmstadt, DE
- Erwin Kooi
Alliander – Duiven, NL
- Maryna Krotofil
TU Hamburg-Harburg, DE
- Klaus Kursawe
ENCS – The Hague, NL
- Corrado Leita
Symantec Research Labs –
Sophia Antipolis, FR
- Tobias Limmer
Siemens – München, DE
- Michael Munzert
Siemens – München, DE
- Heiko Patzlaff
Siemens – München, DE
- Andreas Paul
BTU Cottbus, DE
- Franka Schuster
BTU Cottbus, DE
- Valentin Tudor
Chalmers UT – Göteborg, SE
- Alfonso Valdes
Univ. of Illinois – Urbana, US
- Stephen Wolthusen
RHUL – London, GB
- Emmanuele Zambon
SecurityMatters B.V. –
Enschede, NL

