Report from Dagstuhl Seminar 12061

Network Attack Detection and Defense Early Warning Systems – Challenges and Perspectives

Edited by

Georg Carle[1], Hervé Debar[2], Falko Dressler[3], and Hartmut König[4]

1 **TU München, DE,** carle@in.tum.de
2 **Télécom SudParis, Evry, FR,** herve.debar@telecom-sudparis.eu
3 **Universität Innsbruck, AT,** falko.dressler@uibk.ac.at on behalf of Jelena Mirkovic
4 **BTU Cottbus, DE,** koenig@informatik.tu-cottbus.de

Abstract

The increasing dependence of human society on information technology (IT) systems requires appropriate measures to cope with their misuse. The growing potential of threats, which make these systems more and more vulnerable, is caused by the complexity of the technologies themselves. The potential of threats in networked systems will further grow as well as the number of individuals who are able to abuse these systems. It becomes increasingly apparent that IT security cannot be achieved by prevention alone. Preventive measures and reactive aspects need to complement one another. A major challenge of modern IT security technologies is to cope with an exploding variability of attacks which stems from a significant commercial motivation behind them. Increasingly proactive measures are required to ward off these threats.

Increased efforts in research and society are required to protect critical civil infrastructures, such as the health care system, the traffic system, power supply, trade, military networks, and others in developed countries. This is a consequence of the increasing shift of industrial IT systems to the IP protocol leading to sensible IT infrastructures which are more vulnerable as the proprietary systems used in the past. The abundance of services of modern infrastructures critically depends on information and communication technologies. Though, being key enablers of critical infrastructures, these technologies are, at the same time, reckoned among the most vulnerable elements of the whole system. The cooperative information exchange between institutions is mandatory in order to detect distributed and coordinated attacks. Based on a large-scale acquisition of pertinent information, *Early Warning Systems* are a currently pursued approach to draw up situation pictures that allows the detection of trends and upcoming threats, allowing furthermore taking appropriate measures.

The Dagstuhl seminar brought together researchers from academia and industry. The objective of the seminar was to further discuss challenges and methods in the area of attack detection and defense. The seminar was supposed to focus on design aspects of early warning systems and related monitoring infrastructures, e.g., intrusion detection overlays, to protect computer systems, networks, and critical infrastructures. The seminar was jointly organized by Georg Carle, Hervé Debar, Hartmut König, and Jelena Mirkovic. It was attended by 34 participants from nine countries.

Seminar 05.–10. February, 2012 – www.dagstuhl.de/12061
1998 ACM Subject Classification K.6.5 Security and Protection, K.4.2 Social Issues
Keywords and phrases early warning systems, critical infrastructure protection, botnets, intrusion detection, malware assessment, vulnerability analysis, network monitoring, flow analysis, denial-of-service detection and response, event correlation, attack response and countermeasures
Digital Object Identifier 10.4230/DagRep.2.2.1
Edited in cooperation with Franka Schuster (BTU Cottbus, DE)

Network Attack Detection and Defense Early Warning Systems, *Dagstuhl Reports*, Vol. 2, Issue 2, pp. 1–20
Editors: Georg Carle, Hervé Debar, Falko Dressler, and Hartmut König
Dagstuhl Reports
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Executive Summary

Georg Carle
Hervé Debar
Falko Dressler
Hartmut König

The objective of the seminar was to discuss new challenges, technologies, and architectures in the area of network attack detection and defense. The focus of this seminar laid in particular on *early warning systems*, *malware detection*, and the *protection of critical infrastructures*, but also other recently emerging topics were supposed to be discussed. On this account, the seminar consisted of plenary sessions with technical talks and various breakout sessions. Beside the topics mentioned above two other topics on recently emerging issues were added, namely *cyber crime versus cyber war* and the *protection of cyber-physical systems*.

The seminar started off with an introductory session in which all participants shortly introduced themselves and discussed the focus and the structure of the seminar. Thereafter the first topic *Challenges on Early Warning Systems and Malware Detection* was raised. Michael Meier gave a state of the art talk on the development of early warning systems in the last years and open issues. Felix C. Freiling and Falko Dressler reported on the results of their projects in this field with the German Federal Office for Information Security (BSI). Jan Kohlrausch gave an overview of the experience with the deployment of early warning systems in practice with the DFN-CERT. In the afternoon the first breakout sessions were held. The topics discussed were the *Future of Early Warning Systems*, *Cloud Security*, and *Teaching IT Security*.

Tuesday was devoted to the topic *Protection of Critical Infrastructures*. Introductory talks of the various aspects and challenges for protecting critical infrastructures were given by Stephen Wolthusen and Corrado Leita, followed by technical talks by Franka Schuster and Andreas Paul about a project for protecting supervisory control and data acquisition (SCADA) networks, by Simin Nadjm-Tehrani on the security of smart meters, and by Georg Carle, Lothar Braun and Holger Kinkelin on large-scale vulnerability assessment. In the afternoon Jens Tölle spoke about the protection of IP infrastructures with model-based cyber defense situational awareness. After coffee break we continued with two further breakout sessions on *Information Security for Novel Devices* and *Fighting against Botnets*.

Wednesday morning was devoted to two special topics which have emerged recently: *Security of Cyber-Physical Systems* and *Cyber Crime versus Cyber War*. Nils Aschenbruck gave an introductory talk to the first topic reflecting the evolution from sensor networks to cyber-physical systems. Falko Dressler addressed in his talk the security challenges for future nano communication. The discussion on this topic was continued in the breakout session on Thursday. The second topic was opened by Felix C. Freiling posing various questions about the differences between malware for the masses and exclusive malware, and how to detect them as basis for a longer discussion in the auditorium. Gabi Dreo Rodosek then elucidated at length the issue in her talk about cyber defense. In the afternoon we made a nice trip to the historic city of Trier. The pretty cold weather there gave many opportunities to continue the discussions in warm coffee shops.

On Thursday morning we commenced with two talks by Pavel Laskov and Konrad Rieck on *Malware Detection* which dealt especially with machine learning aspects. Sven Dietrich added a talk on his SkyNET project about the use of drones to launch attacks on wireless networks. Thereafter we continued the topic on the protection of critical infrastructures with the focus on new challenges in deep packet inspection. Radu State began with a talk on the semantic exploration of DNS domains. René Rietz continued with a talk on the increasing threat by attacks over the web. After lunch Robin Sommer introduced the new version of the intrusion detection system (IDS) Bro. Alexander von Gernler reported about the current practice of application level firewalling and virus scanning from the perspective of a firewall manufacturer. Finally, Michael Vogel presented an approach for a dynamically adapting multi-agent intrusion detection system which copes with the growing gap between the evolution of network bandwidth and the single-thread performance of today's CPU architectures. After the coffee break, two further breakout sessions on cyber-physical systems and smart energy grids took place.

Friday morning hosted two talks by Bettina Schnor and Simin Nadjm-Tehrani on IPv6 security and anomaly detection in mobile networks. After that we concluded the seminar with a discussion about the seminar outcome and possible future seminars.

Conclusion

The seminar was well-received by all participants. It gave a good opportunity to inform about current challenges in the area of network attack detection and defense and discuss possible countermeasures. Especially the breakout sessions found a great acceptance. The participants further liked much the possibility to have detailed discussions with colleagues outside the official program. They regret that not all invited foreign scientist accepted the invitation. They will advertise more strongly for this seminar. All participants agreed that proposal for another seminar should be submitted. There are two concrete contributions of this seminar:

1. Current research results of eight participating groups were published in special issue of the journal PIK 1/2012 which is especially devoted to this Dagstuhl seminar.
2. The discussion during the breakout session on cyber-physical systems showed that there is still an unclear picture on the security challenges to these systems. This raised the idea to apply for a Dagstuhl perspective workshop to discuss in detail the security challenges for protecting cyber-physical systems and to define them in a manifesto as working base for further research activities. The proposal has been submitted meanwhile.

2 Table of Contents

Executive Summary

Overview of Talks

Working Groups

3 Overview of Talks

3.1 Early Warning Systems

Michael Meier (Universität Dortmund, DE)

The talk presents a definition of early warning systems and sketches a number of research projects on early warning systems, namely InMAS (Internet Malware Analysis System), IAS (Internet Analysis System), and AMSEL, as well as the operational early warning system CarmentiS and the Deutsche Telekom early warning system. Further, the different meanings of the term "early" – incomplete and fast are discussed, and the question how fast early warning systems should be able to operate is addressed. The talk concludes with some open questions in the context of early warning systems.

3.2 Early Warning Systems – a German Project Initiative

Falko Dressler (Universität Innsbruck, AT)

This talk briefly reflects the requirements and challenges on early warning systems from a technical perspective focusing on the lower layers, i.e., the network sensors and high speed monitoring systems. The crucial issue is to collect network data at highest speeds and to process it in a distributed manner – even given unlimited processing power, it would not be possible to send data for later analysis to any central point in the network.

In the scope of the monkit project, methods for multi-core support and flow analysis with aggregated payload information have been developed. Tools, such as DPA (dialog based payload aggregation), have been implemented in the Vermont monitoring framework and show extremely satisfying results. Still, many issues remain open such as privacy aware data collection and algorithmic solutions to 10 Gbit/s monitoring supporting the use of multiple IDS in presence of correlated flows.

3.3 Early Warning Systems: Experiences from InMAS

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

InMAS is a large-scale sensor system for malware built within a project at Universität Mannheim several years ago [1]. The talk is a report on experiences with this project, especially some results of a large-scale data analysis of autonomously spreading malware [2].

References

1 Markus Engelberth, Felix C. Freiling, Jan Göbel, Christian Gorecki, Thorsten Holz, Ralf Hund, Philipp Trinius, Carsten Willems. *The InMAS Approach.* 1st European Workshop on Internet Early Warning and Network Intelligence (EWNI), Hamburg, Germany, 2010

2 Jan Göbel, Philipp Trinius. *Towards Optimal Sensor Placement Strategies for Early Warning Systems.* Proceedings 5th Conference Sicherheit, Schutz und Zuverlässigkeit (SICHERHEIT), Berlin, Germany, 2010

3.4 Early Warning and Malware Detection at the DFN-CERT

Jan Kohlrausch (DFN-CERT Services GmbH, DE)

Aim of this talk is to give an insight into the work and experiences of the DFN-CERT that are related to early warning systems (EWS) and malware detection. First, EWS, such as the CarmentiS system, which was funded by the German BSI, allow one to assess the overall threat level of the German research network (DFN) as well as the Internet. This information is vital to react to global threats, such as large-scale DDoS attacks and new Internet worms. Apart from this, CarmentiS provides data of compromised computer systems which are used for the automatic warning service of the DFN-CERT. This service collects data about compromised systems from different sources and distributes them automatically to the affected sites within the DFN. Other data sources are the honeypots Dionaea and Argos. In addition, Dionaea is designed to capture malware to be analyzed in a sandbox environment. However, the malware constantly improves and may be able to evade the analysis in the future. Furthermore, current IDS and honeypots have to be adapted to cope with IPv6 which grows in importance.

3.5 Critical Infrastructure Protection

Stephen Wolthusen (RHUL – London, GB)

Starting from a definition of critical infrastructures and their relation to network attack detection and defense the talk presents various models applied for critical infrastructures. It describes existing dependencies and interdependencies in critical infrastructures using qualitative and quantitative models. In the second part of the talk the attacker model for critical infrastructures is discussed by referring to new challenges, especially in the field of SCADA systems and smart grids. Finally, the objectives of the EU ARTEMIES project are outlined.

3.6 Challenges in Critical Infrastructure Security

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

This presentation provides a high-level overview of the security challenges associated with the protection of critical infrastructure environments. Thanks to the convergence between standard IT systems and industrial control systems (ICS), a set of new challenges and opportunities can be identified when trying to secure these environments. How far can standard IT security techniques go in protecting critical infrastructure environments? Are there special constraints and operational characteristics that are unique to ICS and that render the current state of the art impossible to adapt? The talk tries to walk the audience through the implications associated with these questions.

3.7 Protecting Critical Infrastructures

Franka Schuster and Andreas Paul (BTU Cottbus, DE)

Joint work of Schuster, Franka; Paul, Andreas; Vogel, Michael; Rietz, René

The deployment of common information and communication technology in SCADA systems and the recent use of Industrial Ethernet (IE) down to the field level induce new security risks to critical infrastructures. In the talk the drawbacks of current security measures in critical infrastructures are discussed to address the lack of a highly tailored intrusion detection system. First a brief introduction of the concepts and vulnerabilities of Profinet as an example of an emerging IE protocol is given. On this basis, a novel approach for a distributed intrusion detection system is presented which is specialized in the analysis of network traffic of SCADA protocols, such as Profinet.

3.8 Large-scale Vulnerability Assessment Using Active and Passive Techniques

Georg Carle, Lothar Braun, and Holger Kinkelin (TU München, DE)

Joint work of Carle, Georg; Braun, Lothar; Kinkelin, Holger

Current intrusion detection systems detect attacks, while they are conducted or search for signs of successful previous attacks. If one considers previous outbreaks of worms or other exploitations of vulnerabilities in computer systems, one can often find that attackers exploit vulnerabilities which have been known for some time. Many exploited vulnerabilities have been fixed by their vendors before the first exploit for this vulnerability has been observed. Administrators of vulnerable systems therefore usually have time to fix vulnerabilities before they are exploited.

Our work aims at finding weaknesses in systems and security infrastructures to provide administrators and users with a security assessment of their deployed infrastructure. Our presentation discusses how Internet-wide large-scale network measurements can be used to assess the current deployment of computer systems and security protocols. Strengths and weaknesses of active and passive measurement techniques are discussed, including limitations that render network measurements ineffective.

Obtaining data in scenarios where network measurements are unfeasible is addressed as well. Hence, the presentation also discusses how to obtain measurement data from host-based sensors, such as host-based intrusion detection systems, in a secure and trustworthy way.

3.9 Protecting IP Infrastructures with Model-based Cyber Defense Situational Awareness

Jens Tölle (Fraunhofer FKIE – Wachtberg, DE)

The presentation focuses on the improvement of situational awareness in IP networks. Security information and event management (SIEM) systems deliver a huge amount of status data. The presented approach aims at limiting the amount of information which is presented to a human operator/security officer/manager/user in order to help him/her to gain overview without being overloaded by information. In addition, based on a model and a current state gained through measurements, the system gives the possibility to calculate consequences of reactions without applying them to the operational network.

3.10 SecFutur: Security Engineering Process for Networked Embedded Devices

Simin Nadjm-Tehrani (Linköping University, SE)

Ask an engineer in the embedded systems sector about the challenges in product development and chances are that the keywords *size*, *performance*, and *cost* will be included in the answer. Indeed the driving forces in the embedded market have been miniaturisation, faster time to market, and higher performance in the past decade. This equation is subject to a rapid change in the years to come. With more embedded devices perpetually connected via a network we see the emergence of security properties among the basic requirements in product development. This is a radical departure from the earlier state of the "things", where the devices were naturally protected from security threats by operating in closed and controlled environments. Today's systems are increasingly adopting open standards; and when it comes to networked devices we see the emergence of IP networks in diverse domains, such as the energy sector, banking, and telecommunications.

This dramatic change together with the increased hostility in the operational environment of networked applications makes security requirements a basic tenet that needs to be realized by additional building blocks (e.g., access control, authentication, intrusion monitoring, and forensics). It is also increasingly evident that these requirements cannot be met through an add-on feature developed at late development stages. Efficient development of secure embedded systems requires an engineering process that brings together existing solutions in hardware and software and can be demonstrated to achieve design goals, such as resource efficiency as well as meeting legal and international requirements.

This talk briefly describes the objectives of a three-year European FP7 project addressing security in future networked environments (SecFutur). The project aims to flexibly integrate security solutions into a framework for development of networked embedded systems. During the talk the embedding of an anomaly detector into a smart metering device as work in progress is presented.

3.11 From WSN to CPS Security – How Crucial are the Remaining Challenges

Nils Aschenbruck (Universität Bonn, DE)

Joint work of Aschenbruck, Nils; Bauer, Jan; Bieling, Jakob; Bothe, Alexander; Gerhards-Padilla, Elmar; Schwamborn, Matthias
Main reference N. Aschenbruck, J. Bauer, J. Bieling, A. Bothe, M. Schwamborn, P. Martini, D. Pfisterer, K. Hakim, S. Fischer, C. Buschmann, F. Gehring, C. Wieschebrink, "Wireless Sensor Networks-Labor," Projektbericht, Abschlussdokumentation, 2011.
URL http://net.cs.uni-bonn.de/fileadmin/ag/martini/projekte/wsnlab/wsnlab_abschlussbericht.pdf

Security in wireless sensor networks (WSN) has been an active research area for several years. In the last years different solutions were evaluated in real-world deployments. This helped to highlight the remaining challenges. Cyber-physical systems (CPS) assume a tight combination and coordination of computational and physical resources. WSN (as well as robotics) are typically seen as essential parts of CPS. Thus, the remaining security challenges in the area of WSN do affect CPS. After some motivation and definitions, the talk surveys selected projects and results in the area of WSN and discusses the impact on CPS.

3.12 Going Nano – A New Playground and Novel Challenges for Security

Falko Dressler (Universität Innsbruck, AT)

Nano communication is one of the fastest growing emerging research fields. Experts agree that only the interaction among nano machines allows to address the very complex requirements in the field. Drug delivery and environmental control are only two of the many interesting application domains. Relevant communication concepts have been investigated, such as RF radio communication in the terra hertz band or molecular communication based on transmitter molecules. However, one question has not been considered so far and that is nano communication security.

The objective of the talk is to provide some first insights into the security challenges and to highlight some of the open research challenges in this field. A key observation is that especially for molecular communication existing security and cryptographic solutions might not be applicable.

3.13 Attack Detection 2.0: Detecting High-Quality Attacks

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

The appearance of the Stuxnet worm has given rise to a new level in the design of attacks and opened a broad discussion on cyber crime versus cyber war. The talk provides a basis for the discussion on the differences between dedicated and mass attacks in this context. What are the distinguishing features of high-quality targeted attacks in comparison to low-quality (e.g., randomly scanning) malware infections? How can we detect targeted attacks? What research path should we take regarding this? The talk intends to simply pose these questions illustrating them with examples from different categories.

3.14 Cyber Defense: A View from the Research Perspective

Gabi Dreo Rodosek (Universität der Bundeswehr – München, DE)

Cyber defense, the defense in the virtual world, refers to countermeasures against IT threats. The communication possibilities are various, from e-mails, the use of P2P applications, such as Skype to Voice over IP, or social networks like Facebook. In addition, the mobility, heterogeneity, the huge number of ubiquitous devices, and the encryption of the data are further challenges to face.

Terms like *cyber war*, *cyber defense*, *cyber threats*, *cyber crime*, and *cyber security* refer to threats and conflicts in the cyber space, either with military or criminal background, by means of IT. Very often, however, it is almost impossible to recognize the intentions behind the attack (either military or criminal), since attackers are mostly using botnets (i.e., networks of computers that are infected by malware and under the control of cyber criminals). In fact, there is always a battle between the latest attack methods, on the one hand, and the protective mechanisms, on the other side.

The challenges are increased by the fact that a paradigm shift can be recognized with respect to the targets being attacked. So far, mostly state institutions have been the target of attacks. Nowadays, an increasing number of attacks against other targets, such as specific industrial or other enterprises as well as organizations, are recognized. Stuxnet is a recent example of a malware – a computer worm – that targets only SCADA systems.

The increasing usage of encrypted data, the number of targeted attacks, the mobility, the heterogeneity, as well as the need to detect insiders, are demanding challenges for cyber defense. Current approaches for detecting attacks are not sufficient. Signature-based approaches, where the collected data is compared to known patterns (signatures), the most widespread and used approach in intrusion detection/prevention systems (IDS/IPS), as well as virus scanners, are not suitable to detect targeted attacks. Anomaly-based approaches that observe the behavior of the system – instead of searching for patterns – to identify anomalies are much more promising, however, not yet really applicable.

Since IT security needs to be addressed in a holistic way, it is necessary to address aspects raising from the protection of communication infrastructures (systems, services, and data), critical infrastructures, such as energy networks, to cloud services and cloud resources. The research activities of Cyber Defense@UniBwM are focusing on these topics.

3.15 The Threat of Love Letters: Detection of Document-based Attacks

Pavel Laskov (Universität Tübingen, DE)

Most of the information that users access via their computers is stored in some non-trivial format, e.g., HTML, PDF, Excel, JPG, etc. Users access this information via appropriate rendering software which, if vulnerable, can be exploited by sending a specially crafted "document" in the respective format. Due to the high complexity of formats as well as of the rendering software, a steady flow of vulnerabilities is discovered which can be potentially exploited before the vulnerabilities are patched. Traditional signature-based methods are hardly adequate for protection against document-based attacks, since they mostly detect only old attacks with well-known signatures.

In this talk, the challenges of detecting novel attacks that are embedded in specific document formats are elucidated. The talk contains a presentation of previous relevant work on detection of attacks using embedded JavaScript and a discussion on its features and limitations. Finally, a new approach pursued in our current work for building a general framework for detection of document-based attacks is outlined.

3.16 Learning-based Defenses against Malicious JavaScript Code

Konrad Rieck (Universität Göttingen, DE)

Joint work of Rieck, Konrad; Krueger, Tammo; Dewald, Andreas
Main reference K. Rieck, T. Krueger, A. Dewald, "Cujo: Efficient Detection and Prevention of Drive-by-Download Attacks," in Proc. of 26th Annual Computer Security Applications Conference (ACSAC'10), pp. 31–39, ACM, 2010.
URL http://dx.doi.org/10.1145/1920261.1920267

JavaScript is increasingly used for exploiting vulnerabilities in web browsers and infecting users with malicious software. Conventional detection systems that rely on rules and signatures fail to protect from these attacks, as they are unable to cope with the evolving diversity and obfuscation of malicious JavaScript code. This talk explores how machine learning can be applied for analyzing and identifying JavaScript attacks more effectively. Different approaches from recent research are presented along with empirical results and perspectives for future work.

3.17 Semantic Exploration of DNS

Radu State (University of Luxembourg, LU)

The DNS structure discloses useful information about the organization and the operation of an enterprise network which can be used for designing attacks as well as monitoring domains supporting malicious activities. This talk introduces a new method for exploring the DNS domains. In contrast to our previous work of a tool to generate existing DNS names accurately for probing a domain automatically, the presented approach is extended by leveraging the semantic analysis of domain names. In particular, the semantic distribution similarities and relatedness of sub-domains are considered as well as sequential patterns. The evaluation shows that the discovery is highly improved, while the overhead remains low compared to non-semantic DNS probing tools including ours and others.

3.18 Intrusion Detection for the Web 2.0

René Rietz (BTU Cottbus, DE)

The talk is about the limitations of intrusion detection systems (IDS) in the context of the Web 2.0. Most classical IDS have been designed with simple buffer overflows in mind, but they do not work if they face structured web content with plenty of opportunities for obfuscation. We think that the protection of the clients and servers of Web 2.0 applications requires some kind of firewall approach which denies or allows specific web applications. For this we have to analyze the web languages (HTML, XML, JavaScript, ...) and to describe the structure of their contents. If we can identify these structures later, it is possible to pass or deny the underlying packets in a web firewall and to detect any changes (e.g., malicious code).

3.19 From the Unexpected Side: SkyNET

Sven Dietrich (Stevens Institute of Technology, US)

The talk considers attacks that bypass the traditional sensor/IDS locations. By using a commercially available toy drone, it is possible to compromise wireless access points and to install a botnet. The network of bots is separated from the botmaster. Linkage between botnet and botmaster is realized by one or more drones. After presenting the differences of such a scenario compared to the traditional botnet behaviour the attack framework is explained. Finally, the challenge for network security in such a scenario is outlined. Since the proximity to the target is easy to realize, a new stance for network defense has to evolve.

3.20 State of the Art and Limitations to Application Level Firewalling and Virus Scanning

Alexander von Gernler (GeNUA – Kirchheim bei München, DE)

This talk gives a presentation of the current practice of application level firewalling and virus scanning from the perspective of a firewall manufacturer.

Application level firewalling means the interpretation and possibly normalization or modification of traffic passing through the firewall. It is performed at OSI layers higher than 4. While being more expensive, it filters out certain connection-based attacks implicitly and allows for mitigating other attacks easily, also by scanning processed content for viruses on the fly.

Virus scanning in this case cannot be given solely to the usual suspects, the anti-virus industry, but is helped by the firewall by doing preprocessing. As with honeypots and the anti-virus software itself, the way that the firewall interprets content is highly relevant for the security of the whole system.

The talk is concluded by presenting a relatively new problem that emerged with the rise of Web 2.0 applications: Suddenly, web content to be processed by the firewall is no longer static, but carries executable content (here: JavaScript). As many web-based attacks rely on malicious JavaScript code, Web 2.0 applications represent a whole new attack vector. The talk ends with a discussion of some thoughts about this new phenomenon and open questions regarding the topic.

3.21 Bro 2.0 and Beyond

Robin Sommer (ICSI – Berkeley, US)

In this talk the most recent version of Bro, an open-source network security monitor, is presented that has been developed in our group at ICSI for more than a decade now.

Today, Bro is used operationally by many universities, labs, and science communities to protect their infrastructure. The talk starts with a short introduction to Bro focusing on the differences between Bro and other systems in the same space. Then, the main changes going into Bro 2.0 are summarized, and the roadmap for the near-term future is presented.

In the second part of the talk, two areas that Bro-related research at ICSI is currently focusing on are discussed: (1) integrating real-time intelligence into the system and (2) increasing performance to address emerging 100 Gbit/s deployments.

3.22 A Dynamically Adapting Distributed Multi-Agent IDS

Michael Vogel (BTU Cottbus, DE)

Joint work of Vogel, Michael; Schmerl, Sebastian; Schuster, Franka
Main reference M. Vogel, S. Schmerl, H. König, "Efficient Distributed Signature Analysis," in Proc. of the 5th Int'l. Conf. on Autonomous Infrastructure, Management, and Security (AIMS"11), pp. 13–25, LNCS, vol. 6734, Springer, 2011.
URL http://dx.doi.org/10.1007/978-3-642-21484-4_2

This talk is motivated by the problem current IDS have to face because of the growing gap between the evolution of network bandwidth and the single-thread performance of today's CPU architectures. Especially in the case of high analysis load caused by network traffic characterized by short network flows in average and many contained attack traces, the Snort

IDS throughput cannot keep pace with the link bandwidth, so that monitoring data has to be dropped.

In this talk a dynamically adapting and distributed intrusion detection infrastructure is proposed which can utilize different existing IDS as a black box. Resource shortages in high bandwidth situations can be handled by analysis distribution. Performance improvements that could be gained by function or data parallel approaches are discussed for an existing multi-step signature-based IDS as well as the Snort IDS (single step signatures). Finally, the architecture of an IDS agent is presented that applies the examined distribution approaches to dynamically adapt to changing analysis demands and available resources.

3.23 Security Challenges of IPv6 Networks

Bettina Schnor (Universität Potsdam, DE)

URL http://www.idsv6.de

The transition from IPv4 to the official successor protocol IPv6 is on the way. New features like for example MTU path discovery have to be supported by IPv6 firewalls with new filter rules. IPv6 comes along with new concepts like the stateless address autoconfiguration (SLAAC) which results in new ICMPv6 message types and new security risks.

There is still a deficit of tools for the analysis of the threat level in IPv6 networks. The same applies to the testing of IPv6 firewalls and intrusion detection systems. The talk presents some of the IPv6 security risks and gives an overview over the IDSv6 project: the Snort IPv6 extension, which detects attacks on the IPv6 address autoconfiguration, and the honeypot honeydv6.

3.24 Anomaly Detection in Challenged Networks

Simin Nadjm-Tehrani (Linköping University, SE)

This talk addresses information dissemination in disaster area networks with common handheld devices using no existing infrastructure. The open and distributed nature of these networks makes them challenging from the security point of view. Malicious actors may try to disrupt the communication to create more chaos for their own benefit.

The talk presents a general survivability framework for monitoring and reacting to disruptive attacks. The idea is to have a fully distributed framework to detect anomalies, diagnose them, and perform mitigation individually in each node while adapting to the changing environment.

The approach has been evaluated in the context of a simulated disaster area network running a manycast dissemination protocol that uses the Wifi interface in ad hoc mode. The results demonstrate that the approach diminishes the impact of attacks considerably. In addition, in order to evaluate the impact on the resources and specifically the energy footprint of the survivability framework itself, the framework has been implemented in a modular way in an Android smart phone.

4 Working Groups

4.1 Breakout Session: Future of Early Warning Systems

Bettina Schnor (Universität Potsdam, DE)

The participants of the breakout session came from research institutes and companies developing or operating EWS components. First, the group discussed an appropriate definition of EWS and the distinction from classical IDS. The group agreed that the following characteristics are essential: An EWS monitors *large-scale* networks and also does prediction.

There was a longer discussion whether an EWS is comparable with a weather forecast. The group came to the conclusion that this comparison is not feasible, since an EWS cannot make predictions like "There will be an attack starting in four hours." Instead, some machines will get infected and after identifying the attack, there will be a prediction about the current network situation and the expected propagation. Also the group agreed that a recommendation of actions is not in the scope of an EWS. Further, an EWS will *not* detect a targeted attack.

It was stated that the target group is limited and that the government is very much interested in EWS, since it is responsible to maintain the cyber infrastructure. The demand is not only an "early warning", but also to provide "situational awareness", i.e., the EWS should help to answer questions like: What is happening and why?

A DFN-CERT member reported about the experience in operating the early warning system CarmentiS (`http://www.carmentis.org`). According to that, the interpretation of the results requires a security expert and cannot be automated. The experience with CarmentiS also shows that seeing only a small portion of the network tends to give a representative impression of the whole network. Even for EWS approaches like CarmentiS, it is hard to enroll data suppliers. The reason for this is not technical, but political/psychological. There are some patterns of attacks known/understood. Hence, it should be possible for an EWS to give hints to understand even *new* attacks.

The group collected the expectations that an EWS should warn as early as possible, predict infection propagation ("Ausbreitungsphänomene"), warn about DDoS and massive client-side attacks, and give automatically generated hints on further investigation of *new* attacks/malware like IP ranges and ports. Furthermore, it should perform a multi-layer analysis approach by providing data analysis at different abstraction levels.

Finally, open questions were collected: Do we need new methods for data correlation? What are the challenges for EWS in IPv6/mobile/wireless networks? What data is of special interest for an EWS? What data should be provided for "situational awareness"?

4.2 Breakout Session: Cloud Security

Holger Kinkelin (TU München, DE)

The breakout session on "Cloud Security" attracted seven people. It turned out that cloud security is a very broad field of discussion. Problem fields need to be classified according to the type of the cloud service (infrastructure/platform/software as a service), to the level of privacy (private/hybrid/public cloud), and to technical and non-technical (e.g., legal or organizational) aspects. Thus, the expectations of the participants on the subjects to discuss were quite divergent.

One of the main discussion points was the question if there are any new research challenges regarding cloud security or whether existing solutions only may be adapted to the cloud. The discussion was quite controversial and without a clear result. The impression was that some research questions are common, others specific. For instance, challenges regarding cloud forensics (i.e., which evidence needs to be secured for criminal prosecution, the server or the virtual machine only) or how to control where data is allowed to be stored or processed in the cloud (i.e., tags on data items define where the data can go to, etc.) seem to be specific.

4.3 Breakout Session: Teaching IT Security

Hervé Debar (Télécom SudParis, Evry, FR)

The breakout session on “Teaching IT Security” gathered six people, all active in running IT security-related curricula. The group had a round-table discussion on the practices of each of the represented institutions, teaching network and systems security at bachelor and master level. In a nutshell, there is a convergence in the programs taught and the course material used at the institutions represented in the session.

4.4 Breakout Session: Information Security for Novel Devices

Elmar Gerhards-Padilla (Universität Bonn, DE)

The breakout session on “Information Security for Novel Devices” came to the insight that you need to take into account the characteristics of new devices when thinking about information security for these devices. The characteristics relevant in this context are: platform and software diversity, resource restrictions, criticality, and level of interaction. These characteristics have a significant impact on the applicability of conventional network attack detection and response mechanisms.

Anti-virus components are ruled out largely by resource and platform limitations, while EWS are limited mainly to broad-based attacks. Thus, IDS/IPS involving future devices seem to be the most promising field of research for information security on novel devices.

4.5 Breakout Session: Fighting against Botnets

Michael Meier (TU Dortmund, DE)

The breakout session on "Fighting against Botnets" attracted about ten people having very different expectations of the session. During the round-table discussion legal and social issues have been identified as important, but a discussion of these issues was postponed to another breakout session.

Besides some technical questions, for which the recent botnet study by ENISA was referred to, the more controversial question was whether botnets are still a problem. The main results of the overall discussion can be summarized as follows: Botnets are still a problem which will last forever and they will adapt to new (currently mobile) devices. For successfully fighting against botnets, a number of legal, social, and ethical questions have to be answered.

4.6 Breakout Session: Smart Energy Grids

Michael Vogel (BTU Cottbus, DE)

Joint work of Bueschkes, Roland; Herrmann, Peter; Nadjm-Tehrani, Simin; State, Radu; Vogel, Michael; Wolthusen, Stephen

The breakout session on "Smart Energy Grids" was formed by six participants. The discussion started by identifying the components and layers of today's energy grids and future smart energy grids. Then, security measures and possible attack vectors of smart grids have been discussed.

Finally, the participants identified preliminary security requirements and necessary research areas and gave two summarizing hypotheses on security measures for future smart energy grids: (1) preventive security in smart grids (e.g., the use of meters) is expensive and (2) reactive measures (e.g., anomaly detection) are mandatory.

4.7 Breakout Session: Critical Infrastructure Protection

Franka Schuster (BTU Cottbus, DE)

The breakout session on "Critical Infrastructure Protection" attracted more than ten people with very different previous knowledge about the topic. Thus, right at the start the question was raised, why critical infrastructures are so difficult to protect. It was stated that the introduction of IT into plant administration, control, and maintenance connects former isolated systems to the Internet world. Hence, the group agreed that security measures have to be developed which can be non-invasively applied to existing complex and highly-tailored industrial implementations with respect to real-time constraints.

The further discussion focussed on the determination of scientific research challenges on that field. The need for authentication protocols, special cryptographic protocols, and anomaly detection considering the infrastructural context was identified. Finally, specific threats and risks for critical infrastructures were made part of the session, and the limits of such threat and risk analysis were estimated.

4.8 Breakout Session: Cyber-Physical System Security

Hartmut König (BTU Cottbus, DE)

Recently, cyber-physical systems have been identified as a key research area in the years to come. These are systems which possess an intense link between the computational and physical elements. Input and output are usually realized via the physical elements. The use of the term cyber-physical system, however, is still vague. There exist many different definitions which overlap with other areas, e.g., with that of critical infrastructures. It has something of a buzzword with still varying interpretations behind it.

The development of cyber-physical systems comprises a broad range of scientific challenges [1] covering many areas which have been investigated in computer science already for years. Security is mentioned as one of the key issues [2]. The group agreed that the understanding of security challenges, however, is not matured, yet. Several ad hoc discussion papers indicated some research directions.

The further discussion pointed out that attacks on cyber-physical systems may be more complex than on IT systems; their impact may be larger. On the other hand, the security challenges of cyber-physical systems have not precisely defined up to now as well as their relation to privacy and anonymity. For that reason, the group proposed to apply for a Dagstuhl perspective workshop on the security challenges of cyber-physical systems.

References

1 M. Broy (Hrsg.): Cyber-Physical Systems: Innovation durch Software-intensive eingebettete Systeme. Springer, 2011

2 P. Pal, R. Schantz, K. Rohloff, J. Loyall: Cyber-physical Systems Security – Challenges and Research Ideas. Workshop on Future Directions in Cyber-physical Systems Security 2009

Participants

- Nils Aschenbruck
Universität Bonn, DE
- Lothar Braun
TU München, DE
- Roland Büschkes
RWE IT GmbH – Essen, DE
- Georg Carle
TU München, DE
- Hervé Debar
Télécom SudParis – Evry, FR
- Sven Dietrich
Stevens Inst. of Technology, US
- Till Dörges
PRESENSE Technologies GmbH – Hamburg, DE
- Gabi Dreo Rodosek
Universität der Bundeswehr – München, DE
- Falko Dressler
Universität Innsbruck, AT
- Ulrich Flegel
University of Applied Sciences – Stuttgart, DE
- Felix C. Freiling
Univ. Erlangen-Nürnberg, DE
- Elmar Gerhards-Padilla
Universität Bonn, DE
- Peter Herrmann
NTNU – Trondheim, NO
- Marko Jahnke
Fraunhofer FKIE – Wachtberg, DE
- Holger Kinkelin
TU München, DE
- Hartmut König
BTU Cottbus, DE
- Jan Kohlrausch
DFN-CERT Services GmbH, DE
- Pavel Laskov
Universität Tübingen, DE
- Corrado Leita
Symantec Research Labs – Sophia Antipolis, FR
- Michael Meier
TU Dortmund, DE
- Simin Nadjm-Tehrani
Linköping University, SE
- Andreas Paul
BTU Cottbus, DE
- Aiko Pras
University of Twente, NL
- Konrad Rieck
Universität Göttingen, DE
- René Rietz
BTU Cottbus, DE
- Sebastian Schmerl
AGT Germany – Berlin, DE
- Bettina Schnor
Universität Potsdam, DE
- Franka Schuster
BTU Cottbus, DE
- Robin Sommer
ICSI – Berkeley, US
- Radu State
University of Luxembourg, LU
- Jens Tölle
Fraunhofer FKIE – Wachtberg, DE
- Michael Vogel
BTU Cottbus, DE
- Alexander von Gernler
GeNUA – Kirchheim bei München, DE
- Stephen Wolthusen
RHUL – London, GB