Network Traffic Analysis for Cyber Security

Pavel Čeleda

Submitted for habilitation at
The Faculty of Informatics, Masaryk University

Brno, 2013

Except where otherwise indicated, this thesis is my own original work.

Pavel Čeleda
Brno, October 2013

Acknowledgments

It would not have been possible to write this habilitation thesis without the help and support of the kind people around me, to only some of whom it is possible to give particular mention here.

Above all, I would like to thank my wife Zuzana for her personal support and great patience at all times. I would also like to thank my colleagues and co-authors Vojtěch Krmíček, Martin Rehák, and Radek Krejčí. Quiet thanks go in memoriam to my highly valued colleague, friend, and research partner Jiří Novotný.

Last, but by no means least, I thank Václav Račanský and Jan Vykopal for their support of my research and the effort they put into the operation of CSIRT-MU.

Contents

Conference, IAT 2007, Silicon Valley, USA: IEEE Computer Society, 2007, pp. 477-480. ISBN 978-0-7695-3027-7. DOI 10.1109/IAT.2007.66. **37**

K REHÁK, M., M. PĚCHOUČEK, K. BARTOŠ, M. GRILL, P. ČELEDA, and V. KRMÍČEK
CAMNEP: An intrusion detection system for high-speed networks
Progress in Informatics. 2008, no. 5, pp. 65-74. ISSN 1349-8614. DOI 10.2201/NiiPi.2008.5.7. **38**

L REHÁK, M., M. PĚCHOUČEK, M. GRILL, K. BARTOŠ, V. KRMÍČEK, and P. ČELEDA
Collaborative approach to network behaviour analysis based on hardware-accelerated FlowMon probes
International Journal of Electronic Security and Digital Forensics. 2009, vol. 2, no. 1, pp. 35-48. ISSN 1751-911X. DOI 10.1504/IJESDF.2009.023874. **39**

M REHÁK, M., M. PĚCHOUČEK, M. GRILL, J. STIBOREK, K. BARTOŠ, and P. ČELEDA
Adaptive Multiagent System for Network Traffic Monitoring
IEEE Intelligent Systems. 2009, vol. 24, no. 3, pp. 16-25. ISSN 1541-1672. DOI 10.1109/-MIS.2009.42. **40**

N ČELEDA, P., R. KREJČÍ, J. VYKOPAL, and M. DRAŠAR
Embedded Malware - An Analysis of the Chuck Norris Botnet
In: RIECK, K. (Ed.). *European Conference on Computer Network Defense*. EC2ND 2010, Berlin, Germany: IEEE Computer Society, 2010, pp. 3-10. ISBN 978-1-4244-9377-7. DOI 10.1109/EC2ND.2010.15. **41**

O ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK
Revealing and Analysing Modem Malware
In: *Communication and Information Systems Security Symposium*. IEEE International Conference on Communications, ICC 2012, Ottawa, Canada: IEEE Communications Society, 2012, pp. 971-975. ISBN 978-1-4577-2053-6. DOI 10.1109/ICC.2012.6364598. **42**

P KREJČÍ, R., P. ČELEDA, and J. DOBROVOLNÝ
Traffic Measurement and Analysis of Building Automation and Control Networks
In: SADRE, R. et al. (Eds.). *Dependable Networks and Services*. 6th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2012, Luxembourg, Luxembourg: Springer Berlin Heidelberg, 2012, LNCS Volume 7279, pp. 62-73. ISBN 978-3-642-30632-7. DOI 10.1007/978-3-642-30633-4_9. **43**

Q ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK
Flow-Based Security Issue Detection in Building Automation and Control Networks
In: SZABÓ, R. and A. VIDÁCS (Eds.). *Information and Communication Technologies*. 18th EUNICE/ IFIP WG 6.2, 6.6 International Conference, EUNICE 2012, Budapest, Hungary: Springer Berlin Heidelberg, 2012, LNCS Volume 7479, pp. 64-75. ISBN 978-3-642-32807-7. DOI 10.1007/978-3-642-32808-4_7. **44**

Abstract

Cyber security is of the utmost importance in today's networked world. Since the Internet has no borders, cyber-attacks may come from anywhere and at any time. These attacks targeting government and critical infrastructure can swiftly become an issue of national security. Our research aims to provide new insights into traffic analysis to address the specific needs of cyber security.

This habilitation thesis presents research on *(i)* hardware-accelerated traffic processing in high-speed networks, *(ii)* flow-based traffic measurement and analysis in large-scale networks, *(iii)* network behavior analysis and anomaly detection, and *(iv)* traffic analysis of embedded network devices. In our work, we propose new acceleration methods for traffic acquisition without packet loss. Time critical parts of measurement algorithms are processed in hardware (working at line-rate), while complex algorithms are processed in the host computer (working on pre-processed data). We use this approach to generate flow data in heavy loaded networks. Flows provide a near real-time overview of all active network connections on large-scale networks. The manual oversight of such high flow volumes is nearly impossible and only events of an extraordinary scale are typically reported. We research methods of network behavior analysis to identify relevant malicious traffic and unknown threats that are significant on the network level. We propose new methods to monitor network traffic even in automation and control networks which interconnect embedded network devices in intelligent buildings. We conduct and evaluate our work on the Czech National Research and Education Network (CESNET) and on the campus network of Masaryk University.

Our research is achieving results of scientific, governmental and commercial interest. We achieve academic impact by advancing traffic monitoring in high-speed networks. We develop network and security monitoring technology for the Computer Security Incident Response Team of Masaryk University (CSIRT-MU). CSIRT-MU collaborates closely with other national and international security teams. Our research results have been successfully transferred to three university spin-off companies.

This habilitation thesis is organised as a collection of three journal papers, eleven conference papers, one book chapter, and two prototypes (published in proceedings with peer reviewed technical reports). The papers are selected to show the author's contribution to, and research efforts in the field of network traffic analysis for cyber security. The contribution per paper ranges between 10 % and 70 %. The average contribution is around 36 %.

Abstrakt (Abstract in Czech)

V současném síťovém světě hraje kybernetická bezpečnost důležitou roli. Kybernetické útoky mohou přijít kdykoliv a odkudkoliv, protože Internet nemá hranice. Útoky zaměřené na vládní a kritickou infrastrukturu se tak mohou rychle stát problémem národní bezpečnosti. Svůj výzkum proto zaměřuji na porozumění síťového provozu a jeho analýzu pro specifické potřeby kybernetické bezpečnosti.

Předložená habilitační práce prezentuje výzkum v oblastech *(i)* hardwarové akcelerace zpracování provozu ve vysokorychlostních sítích, *(ii)* měření a analýzy provozu pomocí toků v rozlehlých sítích, *(iii)* analýzy síťového chování a detekce anomálií a *(iv)* analýzy provozu zařízení připojených do sítě. Řešené problémy zahrnují nové akcelerační metody pro bezztrátové získávání dat ze sítě. Časově kritické operace měřicích algoritmů jsou prováděny v akcelerační kartě (zpracování na rychlosti linky) a složité algoritmy jsou prováděny v hostitelském počítači (zpracování předzpracovaných dat). Zvolený přístup umožňuje vytvářet toky rozšířené o doplňující informace např. o aplikační data. Zároveň je možné provádět v reálném čase sledování všech aktivních toků v rozsáhlých sítích. U takto velkých objemů toků je manuální sledování nemožné a typicky jsou reportovány pouze události velkého významu. Proto se věnuji výzkumu metod analýzy chování sítě k odhalení škodlivého provozu a neznámých hrozeb, které je možné pozorovat na úrovni sítě. Navrhl jsem nové metody pro sledování síťového provozu v automatizačních a řídicích sítích, které propojují zařízení v inteligentních budovách. Předkládaná práce je prováděna a ověřována v síti CESNET (síť národního výzkumu) a na síti Masarykovy univerzity.

O dosažené výsledky výzkumu projevila zájem, jak odborná veřejnost, tak i státní a soukromý sektor. Akademický impakt se snažím dosáhnout zlepšením metod na monitorování provozu ve vysokorychlostních sítích. Vytvářím nové síťové a bezpečnostní technologie pro bezpečnostní tým Masarykovy univerzity (CSIRT-MU). CSIRT-MU spolupracuje s řadou národních i mezinárodních bezpečnostních týmů. Výsledky mého výzkumu byly úspěšně převedeny formou technologického transferu do třech univerzitních spin-off společností.

Habilitační práce je organizována jako sbírka tří článků v časopise, jedenácti konferenčních článků, jedné kapitoly v knize a dvou prototypů (publikovaných ve sbírce recenzovaných technických zpráv). Jednotlivé články byly vybrány, aby ukázaly můj přínos a výzkumné snažení zaměřené na oblast analýzy síťového provozu pro kybernetickou bezpečnost. Můj autorský podíl se pohybuje mezi 10 % a 70 % u jednotlivých publikací. Průměrný podíl na všech publikacích je přibližně 36 %.

Part I

Commentary

Chapter 1

Introduction

Globally, the number of cyber-attacks is growing day by day [61]. Since the Internet has no borders, these attacks threatening computer systems, networks, and critical infrastructure may come from anywhere and at any time [55]. The security landscape is changing. Advanced persistent threats (malware, botnets and attack tools) are built to hide their presence and remain in the compromised networks for years providing access to them at any time. The cyber-attackers are adopting techniques to increase the costs of detecting these attacks [69, 58]. Many stakeholders (i.e., cyber criminals, governments, academia) are active in cyberspace and follow different goals to protect or to threaten highly-valuable cyber assets. This increases the importance of cyber security in today's high-tech society.

1.1 Motivation

Ensuring security awareness in high-speed networks is a resource intensive task. We need highly experienced network security teams, which must have a deep insight into network behavior, as well as a knowledge of the network and connected hosts. Their usual work procedures [38] consist of observing traffic statistics charts, looking for unusual spikes in volumes of transferred bytes or packets, and consequently examining particular suspect incidents using tools such as packet analysers, flow analysers, intrusion detection systems, and firewall and system log viewers. Such in-depth traffic analysis of particular packets and flows is time consuming and requires excellent knowledge of network behavior. Research on advanced traffic analysis is necessary to provide methods that will require less human intervention and, at the same time, to improve the detection of attacks, threats, and system misuse.

Challenges in traffic analysis are the limitations of measurement and detection methods, the high volume of traffic and events, and the necessity to protect privacy. Every network environment is unique, and the simple correlation of security events may work in small, strict, and well-maintained networks. Such environments are rare. Normally, any network connected to the Internet is exposed to a daily barrage of network scans, spamming hosts, zero-day attacks, and malicious network users hidden in the huge traffic volumes crossing the Internet. The huge volume of traffic may overwhelm measurement tools, drive them to drop data and degrade their overall analysis capabilities. For example, an improperly working anomaly detection system can create so many messages that the security team will

stop analyzing them. Last, but no least, the sensitive nature of data carried over the network requires that traffic analysis takes privacy concerns carefully into account.

1.2 Focus of the Thesis

In this thesis, we focus on traffic analysis in high-speed and large-scale networks. Our research attempts to answer following questions.

(i) *How can traffic be captured and processed in today's high-speed networks?* With network technologies expanding at an ever-increasing rate, we face progressively greater amounts of traffic being carried over networks. New approaches like hardware-software co-design are necessary to monitor the latest 10, 40, and 100 Gigabit Ethernet networks with packet rates of up to 148.8 Mpkt/s (maximum rate).

(ii) *How can network data be measured and collected in large-scale networks?* Currently, there is a shift from host to cloud-based applications and services. These applications rely on high-speed and large-scale networks. New methods are required to provide extended flow data (i.e., application visibility, performance information). This approach may have an impact on the performance of current flow meters and introduce privacy-sensitive information into flow data.

(iii) *How can abnormal behavior and malicious network traffic be detected?* Any device connected to a network creates communication traces. The corresponding flow data may reveal malicious or abnormal network behavior. Anomaly detection techniques use statistical methods, rule based methods, profiling methods, and model-based approaches to detect unknown threats and to reduce false positives (legitimate traffic classified as malicious).

(iv) *How can traffic from embedded network devices be analysed?* New malware variants are increasingly designed to exploit high-value targets. At the same time they are looking for new kinds of vulnerable devices. Cyber-attackers can compromise ADSL modems, Wi-Fi routers, set-top-boxes, and even high-end enterprise devices like backbone routers and firewalls. No anti-virus or anti-malware solution is available to protect such devices. New methods are required to detect attacks and infected devices in standard and critical infrastructure networks.

This thesis is organised as a collection of selected papers which show the author's contribution and research effort in answering the relevant research questions. The papers are organised in four groups related to research topics. Chapter 2 provides a brief overview of the state of the art in the field of traffic analysis. Chapter 3 describes the author's contribution to the work and its impact. Chapter 4 summarises the results presented in this thesis, draws conclusions and outlines future work.

Chapter 2

State of the Art

In this chapter, we discuss the state of the art in *(i)* high-speed traffic processing (packet capture), *(ii)* network traffic measurement (flow generation and collection), and *(iii)* network intrusion detection (anomaly detection). The research presented in this thesis is strongly coupled to networking technologies. The use of cutting-edge technologies opens up new research opportunities and is essential in the world today with its rapidly evolving networking. We show how networks and related research topics have evolved during our research from 2006 up to today. In addition, we list future research directions in network traffic analysis for cyber security.

2.1 High-Speed Traffic Processing

Local area networks and metropolitan area networks are specified in IEEE 802 standards. They have evolved over a considerable time span (the last 30 years) and encompass wired and wireless physical links and speeds from 1 Mb/s to 100 Gb/s. Increasing speeds have an impact on important traffic measurement features such as packets per second (p/s), which have evolved from 1,488 pkt/s to 148.8 Mpkt/s. Figure 2.1 shows IEEE 802.3 Higher Speed Study Group (HSSG) bandwidth demand projections. The HSSG bandwidth forecast for core networking is 400 Gb/s in 2013 and 1 Tb/s in 2015.

According to [47, 52], "The total amount of data created or replicated on the planet in 2010 was over 1 zettabyte (1 zettabyte is 10^{21} bytes) – that's 143 GB for each of the 7 billion people on the planet. This volume of information requires high-speed links between server farms, cloud storage, and end users to make sure that it can be processed in a timely and reliable fashion." It will not be possible to analyse such huge traffic volumes in the coming 100 GbE network installations with the current generation of network measurement tools.

In 1994, the DAG project [79] at the University of Waikato started to combine hardware design (Field Programmable Gate Arrays – FPGA technology) with a PC server to process high-speed traffic. The project developed network measurement cards which were able to capture packet headers with very high precision time stamps. The acceleration cards targeted the problem of capturing data at line-rate into host memory. In contrast to commodity network cards, they used a simple ring buffer model for data transfers [28]. Other FPGA cards include prototypes proposed by the academic projects Liberouter [16] and NetFPGA [59], and commercial solutions provided by the companies Endace, Napatech,

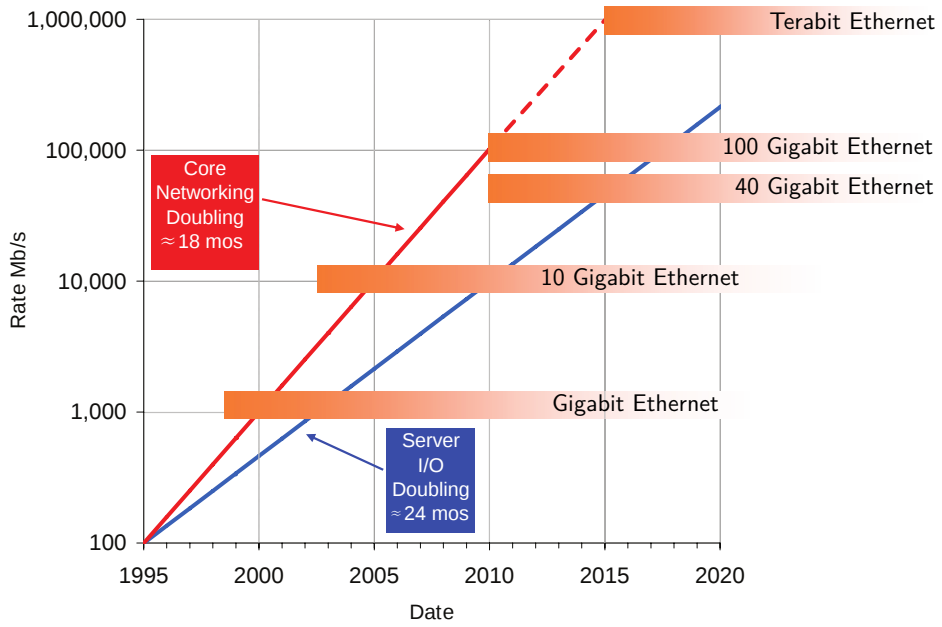


FIGURE 2.1: IEEE 802.3 Higher Speed Study Group bandwidth demand projections [53].

Fiberblaze, and INVEA-TECH. To extend basic packet capture capabilities, several methods have been proposed to process network traffic in hardware [17, 62].

Packet capture is a principal application for acceleration cards. The overall packet capture performance depends on system costs with respect to handing over packets from the network card to the capture application (via a packet capture library). Packet capture usually suffers from performance penalties since the networking stack of an operating system is designed for general-purpose networking. Packets have to traverse several layers, which increase latency and limit the overall performance, as they add per-packet processing overheads. Several methods have been proposed to speed up packet capture in software [11, 33].

FPGA cards provide high-performance, but their prices are higher than commodity cards. This has motivated many researches [10, 39, 65] to employ commodity hardware. They make use of the acceleration capabilities [40] of recent network cards (e.g., Intel 82599, Myri-10G Lanai Z8ES) in order to provide line-rate (or close to it) traffic processing. Some of these cards still lack advanced FPGA-based capabilities like precise time-stamping (with GPS synchronisation), traffic filtering, and flexible hardware-based traffic distribution by means of multiple receive queues. However, commodity network cards are starting to replace FPGA-based accelerators in 1 and 10 GbE networks, which represent most of today's high-speed installations. FPGA cards are still used in applications which perform in-depth analysis, patter matching, and low-latency operations, and in 40/100 Gb/s networks.

2.2 Network Traffic Measurement

Detailed traffic information is necessary to provide permanent situational awareness of a network. Such information can be packet traces, flow statistics, or volume statistics. Typically a trade-off must be made between computational feasibility and the provided level of information to efficiently handle high-speed traffic in large-scale networks.

- *Full packet traces* traditionally used by traffic analysers [22, 73] provide the most detailed information. However, the scalability and processing feasibility of permanent traffic observation and storage in high-speed networks is an issue due to privacy concerns and high operational costs.
- *Flow statistics* provide information from Internet Protocol (IP) headers [21]. They do not include any payload information; however, we still know from the IP point of view *who* communicates with *whom*, *when*, and *for how long*; *what protocol* and *service* was used; and also *how much data* was transferred. This approach significantly reduces the amount of data which it is necessary to process and store. Flow statistics provide information even about encrypted traffic, since packet headers are not encrypted.
- *Volume statistics* are provided by most network appliances for network management (i.e., Simple Network Management Protocol (SNMP) [42] interface statistics). They provide a less detailed network view in comparison to flow statistics and full packet traces, and do not allow advanced traffic analysis.

Flow measurement [13] has become a widely-used method for traffic analysis and network security monitoring. It is based on grouping packets into sets that have common properties. The simplest type of flow is a 5-tuple, with all its packets having the same source and destination IP addresses, port numbers and protocol. Flows are unidirectional and all their packets travel in the same direction. Figure 2.2 shows a flow-based network measurement setup. Generated flow data is stored in flow collectors and used for traffic analysis and network forensics by a security team.

Cisco introduced NetFlow in 1996, and made the NetFlow data format freely available [20]. In 2004, the IETF decided to standardise a flow export protocol, and chartered the IP Flow Information Export (IPFIX) working group. Architecture for IPFIX is described in [67]. Specification of the IPFIX protocol is available in [21]. Originally NetFlow was implemented in Cisco routers, and stand-alone probes [26, 32, 45] were proposed to enable flow monitoring in any network place. The stand-alone approach provides a possibility to generate flow data from highly utilised networks. For example, nProbe on top of Direct NIC Access (DNA) [34] and multi RX-queue can process about 11 Mpkt/s as described in [27], FlowMon generates flow data from two 10 Gb/s lines at full rate (2x 14,88 Mpkt/s) [81].

Flow meters provide high performance for layer 2-through-4 flow measurements, since they do not inspect packet payload. However, application visibility (payload inspection) is increasingly necessary for network operators to identify all forms of present day traffic. AppFlow [18] is an example of how to describe the actual applications in use within the flow. Similar functionality is provided by Cisco NBAR with Flexible NetFlow [19], Palo Alto next-generation firewalls, and other application-aware flow exporters. They use IPFIX enterprise Information Elements (IE) to store application layer (L7) information [44]. The performance

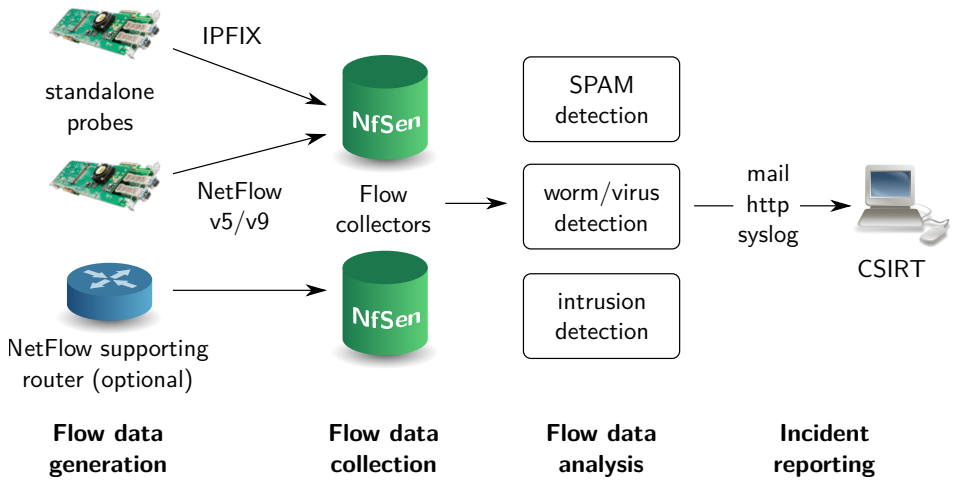


FIGURE 2.2: Flow-based network security monitoring system.

decrease introduced by deep-packet inspection (application parsers) is still not well-known and may limit the deployment of flow meters in highly utilised networks [75].

Performance drops are not the only artifacts associated with flow meters. Some flow meters introduce periodic patterns, measurement gaps, TCP flows without flag information, and invalid byte counters in the exported flow data. The set of known artifacts is presented in [25, 43]. Since network traffic is constantly adapting, reacting and changing, these artifacts may be hard to detect and may have a critical impact on applications [56] that are using flow data. Measurement accuracy and reliability is key to many network traffic analysis methods, including network behavior analysis and anomaly detection.

The actual flow analysis is performed at the collector site. Flow collectors receive, store, and pre-process flow data from one or more flow meters. Various flow collection implementations exist [15, 35, 41, 74]. They provide capabilities for flow visualisation, filtration, aggregation, and statistics evaluation, using source and destination IP addresses, ports, and protocol [6]. Challenges for collectors are the real-time processing of high flow volumes and support for new IE (i.e, variable length strings – HTTP URI, Host, User-Agent).

The centralised collector approach no longer scales for flow data collection. Available solutions [4, 41, 51] are able to process up to 250.000 flows/s. Such high-flow volumes are already present in large-scale collection setups with tens and hundreds of flow sources. The amount of flow data is growing and renders obsolete the real-time capabilities of current traffic analysis tools. New approaches like cloud collection [31] and distributed [54] processing are essential for the real-time flow aggregation and processing of this “big flow data”.

2.3 Network Intrusion Detection

Network Intrusion Detection Systems (NIDS) identify malicious activities targeted at computer and network systems [9]. In 2005, “Promises that IDSs are capable of reliably identifying malicious activity in large networks were premature and never turned into reality.” [48].

This motivated other research on advanced detection and alert correlation methods [1, 71, 76] to enable NIDS deployment in large networks [72]. Network intrusion detection approaches can be split into three categories [68].

- *The signature-based* approach inspects the evaluated content (e.g., network traffic, files in the file system, log records, etc.) by looking for a predefined set of signatures [57] defined in the rule base of the IDS. The effectiveness of this approach depends entirely on the completeness and rule quality of the base.
- *Anomaly-based* detection [29, 30] actually reverses the approach of signature detection. Instead of maintaining a base of individual attack types, the detection mechanism builds a model of normal system behavior, and reports discrepancies between the modelled and observed traffic.
- *Stateful protocol analysis* compares the sequences of protocol commands [78] with the implicit or explicit models of normal (or attack) behavior, and reports the sessions that might correspond to an attack. Such analysis can be performed in several locations (host, firewall, network IDS) and on various levels (transport, application).

The effectiveness of the detection process is affected by the quality of the input data. The criteria used for quantitative evaluation of IDS systems are as follows.

- The *false negative rate* is the fraction of attacks classified as legitimate traffic. The fraction can be evaluated in terms of number of sessions, connections, flows, packets or bytes, depending on the type of IDS system.
- The *false positive rate* is the fraction of legitimate traffic designated as attacks by the system. We use the same quantifications as for the false negatives: sessions, connections, flows, packets or bytes.
- The *performance* of the system is typically measured in a bandwidth (b/s) of the link it can fully process. The problem of this designation is that the performance of systems working on flow/connection levels depends also on the average number of bytes in a packet, and the number of packets in a connection. Therefore, these assumptions will be clarified, or at least mentioned in the benchmark.

Signature matching intrusion detection systems have been the most common type of NIDS deployed in past. Well known systems in this category are Bro [12, 63], Snort [66, 70], and Suricata [60]. Today, they are more commonly known as Network Security Monitoring (NSM) [8] frameworks. Another approach uses next-generation firewalls. They combine user identity information and deep packet inspection to enhance application visibility and intrusion prevention.

Network Behavior Analysis (NBA) NIDS systems are typically based on the classification of sessions or network flows into classes and deciding whether a particular class contains malicious or legitimate flows. Compared to previous NIDS types, these systems use different types of inputs and treat them with significantly different methods [46, 49, 50, 80]. They are typically used to provide a broad overview of anomalous (and potentially malicious) activities in the network rather than to detect all on-going attacks against individual hosts.

The methods used for network behavior analysis (see Figure 2.3) are very different in their nature from the more "low level" pattern matching approaches deployed in signature matching and stateful protocol analysis. These differences arise because of the different nature of the data, as the information we have about a single flow does not typically provide enough information to make a judgment about its maliciousness. Therefore, the methods have to evaluate flows in the context of other flows in the flow set [64]. In the flow sets acquired over two subsequent periods, the same flow can be considered as completely normal in one, and completely anomalous in the other, as the frequency of flows falling into similar classes can increase or decrease.

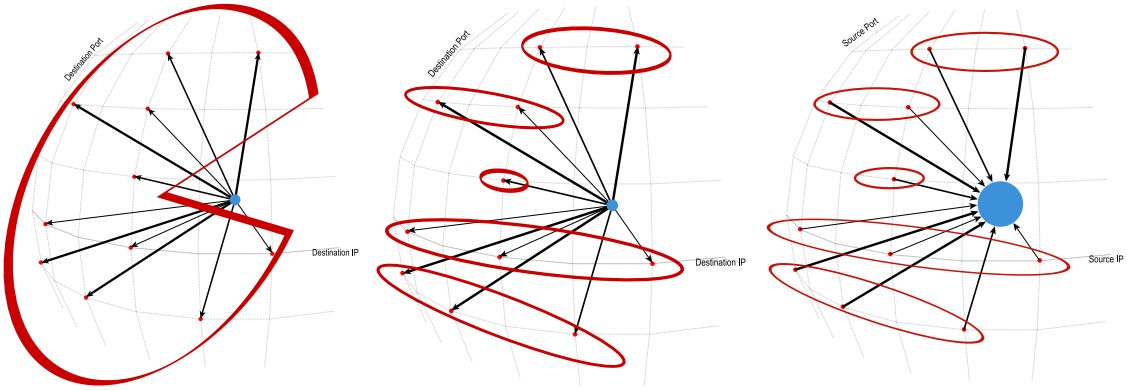


FIGURE 2.3: MINDS : Anomaly Detection Methods [36]. Flow counts from/to important IP/port combinations.

Network intrusion detection has evolved [77] into a broader field that includes malware detection and the analysis of malicious behavior. The connection and communication among devices over the Internet is increasing. This phenomenon is known as the Internet of Things (IoT), and according to ABI Research [2], more than 30 billion devices are expected to be connected by 2020. Today, smart phones, tablets, and laptops are typical connected devices. They are dissolving the network perimeter, as employees can bring their own devices to work and connect them to the network. This is known as the Bring Your Own Device (BYOD) phenomenon [3]. New attacks and new ways of compromising these devices are being introduced, which confirms the importance of network intrusion detection research in the "any-to-any" world.

Chapter 3

Impact of the Work

In this chapter, the author's contribution to the performed research effort is presented. A summary of, and commentary to selected papers is provided, which presents an overview of the author's contribution towards achieving the research goals of this thesis.

The author's contribution is in four areas: *(i)* hardware acceleration to develop technologies to enable reliable traffic measurement in high-speed networks, *(ii)* the analysis of network traffic from large-scale networks and the proposal of new flow-based capabilities to provide traffic visibility in these networks, *(iii)* network behavior analysis and anomaly detection methods to detect malicious traffic and unknown threats, and *(iv)* the problem of malware targeting embedded network devices and the proposal of methods of network security monitoring for automation and control networks.

The results obtained so far were achieved by using Experimental Computer Science and Engineering (ECSE) [23] principles. This means that most of the papers are based on research questions which consider hardware-software prototype(s), measurement dataset(s), and experimental evaluation in various computer networks. The papers cover key areas of current network traffic analysis for cyber security.

3.1 Hardware-Accelerated Traffic Analysis

Traffic measurement can be performed either by generic network devices such as routers or switches, specialised hardware appliances (firewalls, IDS/IPS systems), or by commodity hardware based probes with appropriate software tools. Network monitoring extension in generic network devices is limited by computing power mainly intended for the device's main purpose (e.g., packet forwarding). During an attack, when all information about network traffic is important and can be critical, there is no computing power available for network monitoring. In contrast, specialised hardware appliances have sufficient computing power to work under an attack, but their high price and lack of flexibility discourage their deployment. Probes based on commodity hardware have an advantage in their flexibility and low cost. This approach may not have enough performance for recent high-speed (40 and 100 Gb/s) networks.

Hardware acceleration becomes an essential component of the monitoring tools to cope with high-speed network traffic, especially in environments where we need to guarantee monitoring functionality even in worst-case scenarios like denial-of-service attacks. How-

ever, any hardware or software acceleration mechanism often needs to use optimised versions of the operating system and monitoring tools.

We research and develop hardware accelerators [16] for high-speed (line-rate) traffic processing. To provide flexible and reliable measurement tools we combine open-source software, commodity servers, and FPGA accelerators. The special network adapters implement the time critical part of the application in FPGA, whose performance is much higher than of a traditional CPU. Unique FPGA features (massive parallelism and on-the-fly reconfiguration) are used for traffic pre-processing. Other capabilities of these adapters are precise time stamping (with GPS synchronisation), traffic filtering, and multi-core traffic distribution (multiple receive queues). We present our FPGA-based hardware acceleration framework in [Appendix A].

User-friendliness and ease of use of advanced features play an important role in the broad acceptance of hardware acceleration. To avoid any non-standard tools and proprietary extensions, we proposed modifications to our hardware acceleration framework [Appendix D] to be compatible with most of the current network monitoring applications. We added support to the Packet Capture (PCAP) library so as to receive and send packets with the COMBOv2 card family. To help users with hardware acceleration deployment, a set of use-cases describe how to use the measurement platform. In addition, we report on the line-rate performance of COMBOv2 hardware and firmware, and the application performance of respective traffic processing applications.

In 2006, IP flows become a key technology (NetFlow and IPFIX) for our traffic analyses applications. We proposed the FlowMon probe family [Appendix C] as a reliable source of complete flow statistics with a wide set of additional extensions for flow data processing and analysis. Among others, we provide the possibility to generate flow data from two 10 Gb/s lines at full rate. We contributed to the GÉANT2 security toolset, which consists of the flow analysis tools NfSen and NFDUMP and the FlowMon probe. The security toolset allows the identification and analysis of network security threats. This idea further evolved in the next-generation FlowMon probe, which is now part of the INVEA-TECH flow monitoring solution with hundreds of installations in the Czech Republic and worldwide.

In [Appendix B], we propose Network Interface Filtering Card (NIFIC) probes to be deployed at access gateways or at critical points of the network. They send security related information to the Security Operations Center (SOC). The probes can be remotely configured to focus in more detail on selected traffic and/or filter out malicious forms. This integration of monitoring and executive features enables the operating staff – the Computer Security Incident Response Team (CSIRT) – to efficiently resolve network incidents.

The presented research effort in hardware acceleration is the joint work of CESNET, Brno University of Technology (BUT), and Masaryk University (MU). A university (BUT and MU) spin-off company INVEA-TECH was founded in 2007. The impulse to start the company and commercialise R&D results was a recommendation of project reviewers from the EU project SCAMPI (IST-2001-32404). INVEA-TECH improves technology transfer from CESNET (the Liberouter project), and develops and markets comprehensive network solutions for networks from 10 Mb/s to 100 Gb/s.

[Appendix A] NOVOTNÝ, J., P. ČELEDA, and M. ŽÁDNÍK. Hardware-Accelerated Framework for Security in High-Speed Networks. In: *Information Assurance for Emerging and Future Military Systems*. RTO Meeting Proceedings MP-IST-076, Ljubljana, Slovenia:

NATO Research and Technology Organization, 2008. RTO-MP-IST-076 AC/323(IST-076)TP/238.

Contribution: I was responsible for most of the writing, but the framework we describe was designed by multiple people within the Liberouter project. I was responsible for software development, design of the FlowMon probe toolset, and flow collection and analysis. (50 %)

[Appendix B] NOVOTNÝ, J., P. ČELEDA, T. DEDEK, and R. KREJČÍ. Hardware Acceleration for Cyber Security. In: *Information Assurance and Cyber Defence*. RTO Meeting Proceedings MP-IST-091, Tallinn, Estonia: NATO Research and Technology Organization, 2010, pp. 86-101. ISBN 978-92-837-0115-6.

Contribution: I was the principal editor of the paper. I proposed and evaluated security use-cases with the NIFIC probe for network security monitoring and network protection. (40 %)

[Appendix C] ČELEDA, P., M. KOVÁČIK, T. KONÍŘ, V. KRMÍČEK, P. ŠPRINGL, and M. ŽÁDNÍK. FlowMon Probe. In: LHOTKA, L. and P. SATRAPA (Eds.). *Network Studies: Selected Technical Reports*. Prague: CESNET, 2007, pp. 67-81. ISBN 978-80-239-9285-4.

Contribution: I was the architect and leader of FlowMon probe software development and oversaw its deployment and evaluation with third-party collectors. I co-authored the text. I accomplished the technology transfer related to FlowMon transfer from academia to industry. (20 %)

[Appendix D] ČELEDA, P., R. KREJČÍ, J. BARIENČÍK, M. ELICH, and V. KRMÍČEK. HAMOC - Hardware-Accelerated Monitoring Center. In: LHOTKA, L. and P. SATRAPA (Eds.). *Networking Studies V : Selected Technical Reports*. Prague: CESNET, 2011, pp. 107-133. ISBN 978-80-904689-1-7.

Contribution: I was the principal author of the ideas behind the HAMOC. I was leader of the HAMOC research, development, and evaluation team. I co-authored and served as editor of the text. I proposed several evaluation use-cases. (30 %)

3.2 Flow-based Traffic Analysis on a Large Scale

We use flow data (NetFlow and IPFIX) for their scalability and ability to provide a sufficient amount of traffic information. Flow-based monitoring allows us to permanently observe both small end-user networks and large backbone networks. We perform our measurements on CESNET's research monitoring infrastructure and on the campus network of Masaryk University. In [Appendix E], we describe the architecture of our traffic analysis system consisting of flow exporters as well as flow collectors. We show flow analysis outputs from live campus and backbone networks.

Today, many campus and backbone networks are undergoing IPv6 transition. The exhaustion of IPv4 address space increases pressure on network operators and content providers to support IPv6. IPv6 transition (tunnelling) mechanisms such as Teredo and 6to4 allow IPv4 hosts to connect to IPv6 hosts. They are used to facilitate the adoption of IPv6. However, they increase network complexity and render ineffective many methods to monitor and control IP traffic. For example, firewalls which do not support IPv6 transition mechanisms will

leave IPv6 tunnelled traffic unattended. In [Appendix F], we provide a flow-based IPv6 measurement prototype (FlowMon exporter plugin), which enables IPv6 visibility in large-scale networks. We analyse and show IPv6 transition mechanism traffic characteristics including a tunnelled one. We show how the traffic of IPv6 transition mechanisms has evolved in the CESNET network from 2010 to 2013.

Another important traffic property is the geographical origin of communicating hosts. The importance of IP address geolocation has increased significantly in recent years, due to its applications in business advertising and security analysis, among others. Current approaches perform geolocation mostly on-demand and in a small scale fashion. As soon as geolocation needs to be performed in real-time and in high-speed and large-scale networks, these approaches are no longer scalable. To solve this problem, we propose in [Appendix G] two approaches to large-scale geolocation. Firstly, we present an exporter-based approach, which adds geolocation data to flow records in a way that is transparent to any flow collector. Secondly, we present a collector-based approach, which adds native geolocation to flow data from any exporter. We demonstrate the applicability of large-scale geolocation for traffic profiling and anomaly detection on the 10 GbE Internet connection of Masaryk University.

Today, flow-based traffic analysis uses mostly data from layer 2-through-4 flow meters (i.e, backbone routers, probes). These flow meters lack application layer (L7) visibility, which renders "classical" NetFlow and IPFIX ineffective for in-depth HTTP (web traffic) analysis. However, more and more applications (e.g., Facebook, Google Apps, Microsoft Office Live, and WebEx) rely on the HTTP protocol. HTTP traffic (TCP port 80) can usually pass through most firewalls and therefore presents a standard way of transporting/tunnelling data. The versatility, ubiquity and amount of HTTP traffic makes it easy for an attacker to hide malicious activities. In [Appendix H], we research the impacts of application layer analysis of the HTTP protocol on flow measurement. We designed and evaluated several HTTP protocol parsers representing current state of the art approaches used in today's flow meters. We report on the throughput decrease (the performance implications of using an application parser), which is of the utmost importance for high-speed deployments.

[Appendix E] ČELEDA, Pavel and Vojtěch KRMÍČEK. Flow Data Collection in Large Scale Networks. In: *Advances in IT Early Warning*. Ed. by ZEILINGER, M., P. SCHOO and E. HERMANN. Stuttgart: Fraunhofer Verlag, 2013, pp. 30-40. ISBN 978-3-8396-0474-8.

Contribution: I was the principal editor of the paper. I was responsible for most of the writing on flow introduction, flow monitoring, flow export, and flow deployments in large-scale networks. (70 %)

[Appendix F] ELICH, M., P. VELAN, T. JIRSÍK, and P. ČELEDA. An Investigation Into Teredo and 6to4 Transition Mechanisms: Traffic Analysis. To appear In: *WNM 2013, The 7th IEEE Workshop on Network Measurements*. 38th IEEE Conference on Local Computer Networks, LCN 2013, Sydney, Australia: IEEE Computer Society, 2013, pp. 1046-1052. ISBN 978-1-4799-0540-9.

Contribution: I co-authored the paper. I contributed to the measurement prototype, flow data collection, and Teredo/6to4 traffic analysis presented in the paper. (20 %)

[Appendix G] ČELEDA, P., P. VELAN, M. RÁBEK, R. HOFSTEDE, and A. PRAS. Large-Scale Geolocation for NetFlow. In: De TURCK, F. et al. (Eds.). *Experience Session*.

IFIP/IEEE International Symposium on Integrated Network Management, IM 2013, Ghent, Belgium: IEEE Communications Society, 2013, pp. 1015-1020. ISBN 978-1-4673-5229-1.

Contribution: I was the principal author of the NetFlow geolocation ideas. I contributed to the geolocation prototypes and served as editor of the text. I proposed several evaluation use-cases to demonstrate geolocation benefits. (40 %)

[Appendix H] VELAN, P., T. JIRSÍK, and P. ČELEDA. Design and Evaluation of HTTP Protocol Parsers for IPFIX Measurement. In: BAUSCHERT, T. (Ed.). *Advances in Communication Networking*. 19th EUNICE/IFIP WG 6.6 International Workshop, Chemnitz, Germany: Springer Berlin Heidelberg, 2013, LNCS Volume 8115, pp. 136-147. ISBN 978-3-642-40551-8. DOI 10.1007/978-3-642-40552-5_13.

Contribution: I co-authored the paper. I contributed to the design of HTTP protocol parsers, and to the evaluation and comparison of parsing methods. (20 %)

3.3 Network Behavior Analysis and Anomaly Detection

Flow data is traditionally, but not exclusively, used for routing optimisation, application troubleshooting, traffic monitoring, accounting and billing. Besides these applications, new uses are attracting attention including network behavior analysis, the detection of security incidents, and denial-of-service attacks already embedded in some flow collectors.

In [Appendix I], we present the design of a high-performance agent-based intrusion detection system designed for deployment on high-speed network links. To match the speed requirements, the line-rate data acquisition layer is based on hardware-accelerated FlowMon probes, which provide an overview of current network traffic. The flow data is then processed by detection agents that use heterogeneous anomaly detection methods. These methods are correlated by means of trust and reputation models, and conclusions regarding the maliciousness of individual network flows are presented to the operator. The analysis agent automatically gathers supplementary information about the potentially malicious traffic from remote data sources such as DNS, whois or router configurations. The presented system is designed to help network operators to efficiently identify malicious flows by automating most of the surveillance process. We have named the system CAMNEP (Cooperative Adaptive Mechanism for Network Protection).

In [Appendix J], we present a traffic acquisition subsystem suitable for agent-based intrusion detection systems. Hardware-accelerated probes send flow statistics to a collector server, which performs traffic statistics aggregation and pre-processing for the threat detection layer. Individual anomaly detection methods used for network threat detection have relatively high error rates. We show in [Appendix K], [Appendix L], and [Appendix M] that the use of a trust model for the integration of several anomaly detection methods and the efficient representation of history data reduces the high rate of false positives (legitimate traffic classified as malicious), which limits the effectiveness of current intrusion detection systems. We deployed the CAMNEP system as part of an experimental campus-wide intrusion detection system.

The presented research effort in network behavior analysis was the joint work of the Czech Technical University in Prague and Masaryk University funded by the U.S. Army. A Czech Technical University spin-off company Cognitive Security was founded by Michal

Pěchouček and Martin Rehák in 2009. Cisco acquired Cognitive Security in January, 2013. Cognitive Security focused on applying artificial intelligence techniques from the CAMNEP project to detect advanced cyber threats. The AdvaICT company (a spin-off of Masaryk University) exploited the Operator and Analyst Interface Layer of the CAMNEP project. On the basis of this knowledge, they developed a system for the detection of anomalies and undesirable network behavior. INVEA-TECH acquired AdvaICT in December, 2012.

[Appendix I] REHÁK, M., M. PĚCHOUČEK, P. ČELEDA, V. KRMÍČEK, J. MONINEC, T. DYMÁČEK, and D. MEDVIGY. High-Performance Agent System for Intrusion Detection in Backbone Networks. In: KLUSCH, M. et al. (Eds.). *Cooperative Information Agents XI*. 11th International Workshop, CIA 2007, Delft, The Netherlands: Springer Berlin Heidelberg, 2007, LNAI Volume 4676, pp. 134-148. ISBN 978-3-540-75118-2. DOI 10.1007/978-3-540-75119-9_10.

Contribution: I co-authored the paper. I contributed to the overall architecture, to traffic acquisition and data pre-processing, to the selection of detection methods, and to system evaluation and performance tests. (30 %)

[Appendix J] ČELEDA, P., V. KRMÍČEK, M. REHÁK, and D. MEDVIGY. High-Speed Network Traffic Acquisition for Agent Systems. In: LIN, T.Y. et al. (Eds.). *Intelligent Agent Technology*. IEEE/WIC/ACM International Conference, IAT 2007, Silicon Valley, USA: IEEE Computer Society, 2007, pp. 477-480. ISBN 978-0-7695-3027-7. DOI 10.1109/IAT.2007.66.

Contribution: I was the principal author and editor of the paper. I proposed an approach to traffic acquisition and data pre-processing for agent systems in high-speed networks. (60 %)

[Appendix K] REHÁK, M., M. PĚCHOUČEK, K. BARTOŠ, M. GRILL, P. ČELEDA, and V. KRMÍČEK. CAMNEP: An intrusion detection system for high-speed networks. *Progress in Informatics*. 2008, no. 5, pp. 65-74. ISSN 1349-8614. DOI 10.2201/NiiPi.2008.5.7.

Contribution: I co-authored the paper. I contributed to the overall architecture, to traffic acquisition and data pre-processing, and to system deployment and evaluation. (20 %)

[Appendix L] REHÁK, M., M. PĚCHOUČEK, M. GRILL, K. BARTOŠ, V. KRMÍČEK, and P. ČELEDA. Collaborative approach to network behaviour analysis based on hardware-accelerated FlowMon probes. *International Journal of Electronic Security and Digital Forensics*. 2009, vol. 2, no. 1, pp. 35-48. ISSN 1751-911X. DOI 10.1504/IJESDF.2009.023874.

Contribution: I co-authored the paper. I contributed to the overall architecture, to traffic acquisition and data pre-processing, and to system deployment and evaluation. (20 %)

[Appendix M] REHÁK, M., M. PĚCHOUČEK, M. GRILL, J. STIBOREK, K. BARTOŠ, and P. ČELEDA. Adaptive Multiagent System for Network Traffic Monitoring. *IEEE Intelligent Systems*. 2009, vol. 24, no. 3, pp. 16-25. ISSN 1541-1672. DOI 10.1109/MIS.2009.42.

Contribution: I co-authored the paper. I contributed to the selection of detection methods and to the design of the system prototype, its evaluation and experimental deployment as a campus-wide intrusion detection system. (10 %)

3.4 Embedded Network Devices Traffic Analysis

To protect the Masaryk University network we deployed our network monitoring systems described in the previous text. This network-based approach allows us to see all activities directed towards and away from our network. We use flow data as an input for the security analyses and anomaly detection systems we work on. Typically, we observe various network scan attempts, password brute force attacks, and remote exploits coming from outside. Such activities are often regarded as a normal part of today's Internet traffic.

At the beginning of December 2009, our attention was drawn to an increasing number of Telnet scans (TCP port 23). The use of the Telnet protocol should be discontinued for its security related shortcomings and replaced by the Secure Shell (SSH) protocol. Any Telnet activity, especially on the public Internet, is suspicious.

By checking the sources of the attacks, we identified subnets of ADSL modems and home routers located worldwide. At the beginning, we expected some new variant of the PSYB0T [7] botnet to be at work. We were able to gain access to an IPTV set-top-box and obtained the first bot sample. A firewall was not installed in the device and the bot was unable to block remote access.

Further investigation (bot binaries reverse engineering) revealed the IP addresses of command and control (C&C) centres, including botnet distribution sites. To acquire more information we prepared a vulnerable device (MIPS-based wireless router) in our network and voluntarily joined the botnet. We recorded all incoming and outgoing connections until the botnet paused its activity on February 23rd, 2010. We named the botnet after Chuck Norris because an early version included the string `[R]anger Killato : in nome di Chuck Norris!` An analysis of the Chuck Norris Botnet is described in [Appendix N]. We notified all affected networks before publicly announcing the existence of the Chuck Norris Botnet. The botnet attracted a great deal of media attention and there were worldwide Internet headlines about our discovery in February, 2010.

Malware targeting broadband devices such as ADSL modems, routers and wireless access points has become more frequent recently. Insecure embedded devices were used by the Carna Botnet [14] to measure the extent of the Internet. Cui et al. [24] found over 540,000 publicly accessible broadband devices, including routers, wireless access points, modems and VoIP appliances, configured with factory default root passwords. In [Appendix O], we propose a set of techniques to perform detailed analysis of these insecure devices (infected modems). We provide a formal description of the modem malware life cycle, and we propose a flow-based method to detect the spread of such malware.

We detected another massive Telnet scan against university computers on December 4th, 2011. The source of the attacks was the new Aidra botnet. The Aidra botnet is an open source IRC-based mass router scanner/exploiter publicly available for download from the Internet [37]. The novelty of this botnet is in its support for multiple hardware platforms of vulnerable devices. Equivalent versions for six different hardware architectures (ARM, MIPS, MIPSEL, PPC, SH4, x86) have been observed up to now. The first remote device we were able to analyse was a building automation and control station (BACnet controller [5]). Other infected devices ranged from firewalls, routers, modems, and VoIP appliances to consumer electronics, including satellite receivers and IPTV boxes, etc. This confirmed the utmost importance of network security monitoring for any network and any device.

Masaryk University Campus is so far the largest Building Automation and Control network (BACnet) installation in the Czech Republic. More than 24 teaching and research pavil-

ions are monitored and controlled by the Building Management System (BMS). A dedicated LAN, BACnet over Ethernet, and BACnet over IP network interconnects several power systems, fire systems, security systems, data information systems, and lighting. Any system failure or attack against BMS could be critical for the entire campus. In [Appendix P], we propose a novel system for the flow-based network traffic monitoring of building automation and control networks. We show our measurement results and report on our experience of using such a system for monitoring the university campus.

The interconnection of building automation and control system networks with public networks has exposed them to a wide range of security problems. In [Appendix Q], we research flow data usability to detect security issues in these networks. We describe several use cases in which flow monitoring provides information on network activities in building automation and control systems. We demonstrate the detection of Telnet brute force attacks, list remote connections to building network, and show possible targeted attacks on the building automation system network.

[Appendix N] ČELEDA, P., R. KREJČÍ, J. VYKOPAL, and M. DRAŠAR. Embedded Malware - An Analysis of the Chuck Norris Botnet. In: RIECK, K. (Ed.). *European Conference on Computer Network Defense*. EC2ND 2010, Berlin, Germany: IEEE Computer Society, 2010, pp. 3-10. ISBN 978-1-4244-9377-7. DOI 10.1109/EC2ND.2010.15.

Contribution: I discovered the Chuck Norris botnet and performed the analysis of the botnet. I proposed an extension to the botnet to demonstrate the man-in-the-middle attack on HTTPS with a rogue home router. I was the principal author and editor of the paper. (45 %)

[Appendix O] ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK. Revealing and Analysing Modem Malware. In: *Communication and Information Systems Security Symposium*. IEEE International Conference on Communications, ICC 2012, Ottawa, Canada: IEEE Communications Society, 2012, pp. 971-975. ISBN 978-1-4577-2053-6. DOI 10.1109/ICC.2012.6364598.

Contribution: I was the principal author and editor of the paper. I proposed several methods to analyse infected devices. I proposed a method of detecting modem malware network activities. (40 %)

[Appendix P] KREJČÍ, R., P. ČELEDA, and J. DOBROVOLNÝ. Traffic Measurement and Analysis of Building Automation and Control Networks. In: SADRE, R. et al. (Eds.). *Dependable Networks and Services*. 6th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2012, Luxembourg, Luxembourg: Springer Berlin Heidelberg, 2012, LNCS Volume 7279, pp. 62-73. ISBN 978-3-642-30632-7. DOI 10.1007/978-3-642-30633-4_9.

Contribution: I co-authored the paper. I proposed the BACnetFlow monitoring prototype and managed its pilot deployment on the Masaryk University Campus network. I reported on BACnet traffic features. (45 %)

[Appendix Q] ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK. Flow-Based Security Issue Detection in Building Automation and Control Networks. In: SZABÓ, R. and A. VIDÁCS (Eds.). *Information and Communication Technologies*. 18th EUNICE/ IFIP WG 6.2, 6.6 International Conference, EUNICE 2012, Budapest, Hungary: Springer Berlin Heidelberg, 2012, LNCS Volume 7479, pp. 64-75. ISBN 978-3-642-32807-7. DOI 10.1007/978-3-642-32808-4_7.

Contribution: I was the principal author and editor of the paper. I proposed three use-cases to demonstrate the advantages of flow monitoring for detecting security threats in the BACnet network. (50 %)

Chapter 4

Conclusion

The growth in the number of devices connected to the network has led to an explosive growth in bandwidth and the amount of data exchanged over the network. In 2006, hardware accelerators based on FPGA were required to process 10 GbE traffic. We have used our FPGA experience to exploit commodity network adapters to provide acceleration capabilities for today's 10 GbE networks. In our current research, we are designing a new 100 GbE card and researching new techniques to process traffic in 100 GbE networks. The huge volume of traffic in these networks may overwhelm measurement tools, drive them to drop data, and degrade their overall analysis capabilities. The key to high-performance packet processing is efficient memory management, low-level hardware interaction, and application optimization. An aggregated and/or filtered traffic view is necessary to provide inputs for subsequent network management and traffic analysis tools.

Network operators use aggregation-based monitoring techniques (IP flows) to enable permanent network situational awareness. Original flow data created from packet headers does not include any payload information. Today's applications use dynamic port allocation relying on the HTTP protocol, and the high amount of such traffic makes it easy for an attacker to hide malicious activities. Flow meters are beginning to adopt deep packet inspection techniques to extract payload information. They close the gap between packet-based and flow-based monitoring. Flow analysis provides a scalable approach to the monitoring of large networks. However, it is necessary to analyse the flow data, not only to store them for data retention, incident handling and forensics.

Network security monitoring is essential in network environments with liberal usage rules (e.g., academic networks, ISP networks). We advocate an approach which detects and mitigates attacks and abnormal behavior instead of limiting users' activities by a deny-by-default policy. The Chuck Norris botnet and Aidra botnet proved that we can detect attacks before our hosts are infected. Virtually any network-connected device can be a source of an attack. Many organizations underestimate security. For example, we notified all network operators affected by the Chuck Norris botnet, but we received no responses and the operators failed to fix the vulnerable devices in their networks. Network security monitoring helps us to better understand actual network configuration and all network activities.

We proposed the Cybernetic Proving Ground (CPG) project to increase security awareness and to demonstrate current security threats. In the context of the CPG project, we are creating a unique environment for the research and development of new methods to protect critical infrastructure against cyber attacks. A developed virtualized environment will

be used to simulate complex cybernetic attacks against critical infrastructure and analyse their behavior and impact on that infrastructure. The CPG will serve for the research and development of new security tools and methods. In addition, it will be used for educating members of security teams.

The presented research has thrown up many questions in need of further investigation. To address them, we founded CSIRT-MU in 2009. Beyond operational activities, we focus on security research in order to remain at the forefront of cyber security and to be able to provide a secure network environment at Masaryk University. In addition, we are contributing to the preparation of a new cyber security study program at the Faculty of Informatics, where we plan to participate in teaching courses related to our research.

Bibliography

[1] ABDUVALIYEV, A., A.-S. PATHAN, J. ZHOU, R. ROMAN, and W.-C. WONG. On the Vital Areas of Intrusion Detection Systems in Wireless Sensor Networks. In: *Communications Surveys Tutorials, IEEE* 15.3 (2013), pp. 1223–1237. ISSN: 1553-877X. DOI: 10.1109/SURV.2012.121912.00006.

[2] ABI RESEARCH. More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020. 2013. URL: https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne (visited on 10/19/2013).

[3] ACKERMAN, E. The bring-your-own-device dilemma [Resources_At Work]. In: *Spectrum, IEEE* 50.8 (2013), pp. –. ISSN: 0018-9235. DOI: 10.1109/MSPEC.2013.6565553.

[4] ARBOR. Pravail Network Security Intelligence. 2013. URL: http://www.arbornetworks.com/products/pravail/nsi (visited on 10/15/2013).

[5] ASHRAE SSPC 135. BACnet – A Data Communication Protocol for Building Automation and Control Networks. 2013. URL: http://www.bacnet.org (visited on 10/19/2013).

[6] BAJPAI, V., J. SCHAUER, and J. SCHÖNWÄLDER. NFQL: A tool for querying network flow records. In: *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. 2013, pp. 643–649. ISBN: 978-1-4673-5229-1.

[7] BAUME, T. PSYB0T Information Page. 2009. URL: http://baume.id.au/psyb0t (visited on 09/15/2013).

[8] BEJTLICH, R. The Tao Of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley Professional, 2004. ISBN: 0-3212-4677-2.

[9] BHUYAN, M., D. BHATTACHARYYA, and J. KALITA. Network Anomaly Detection: Methods, Systems and Tools. In: *Communications Surveys Tutorials, IEEE* PP.99 (2013), pp. 1–34. ISSN: 1553-877X. DOI: 10.1109/SURV.2013.052213.00046.

[10] BONELLI, N., A. PIETRO, S. GIORDANO, and G. PROCISSI. On Multi–gigabit Packet Capturing with Multi–core Commodity Hardware. In: *Passive and Active Measurement*. Vol. 7192. LNCS. Springer Berlin Heidelberg, 2012, pp. 64–73. ISBN: 978-3-642-28536-3.

[11] BRAUN, L., A. DIDEBULIDZE, N. KAMMENHUBER, and G. CARLE. Comparing and improving current packet capturing solutions based on commodity hardware. In: *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. IMC '10. Melbourne, Australia: ACM, 2010, pp. 206–217. ISBN: 978-1-4503-0483-2.

[12] BRO PROJECT. The Bro network security monitor. 2013. URL: http://www.bro.org (visited on 09/16/2013).

[13] BROWNLEE, N. Flow-Based Measurement: IPFIX Development and Deployment. In: *IEICE Transactions on Communications* E94.B.8 (2011), pp. 2190–2198. DOI: http://dx.doi.org/10.1587/transcom.E94.B.2190.

[14] CARNA BOTNET. Internet Census 2012 – Port scanning /0 using insecure embedded devices. 2012. URL: http://internetcensus2012.bitbucket.org (visited on 10/19/2013).

[15] CERT NETSA. SiLK - System for Internet-Level Knowledge. 2013. URL: http://tools.netsa.cert.org/silk/ (visited on 09/26/2013).

[16] CESNET. Liberouter project. 2013. URL: http://www.liberouter.org/ (visited on 10/19/2013).

[17] CHEN, H., Y. CHEN, and D. SUMMERVILLE. A Survey on the Application of FPGAs for Network Infrastructure Security. In: *Communications Surveys Tutorials, IEEE* 13.4 (2011), pp. 541–561. ISSN: 1553-877X. DOI: 10.1109/SURV.2011.072210.00075.

[18] CITRIX. AppFlow Specification. 2012. URL: http://www.appflow.org/ (visited on 09/10/2013).

[19] CLAISE, B., P. AITKEN, and N. BEN-DVORA. Cisco Systems Export of Application Information in IP Flow Information Export (IPFIX). RFC 6759 (Informational). Internet Engineering Task Force, 2012. URL: http://www.ietf.org/rfc/rfc6759.txt.

[20] CLAISE, B. Cisco Systems NetFlow Services Export Version 9. RFC 3954 (Informational). Internet Engineering Task Force, 2004. URL: http://www.ietf.org/rfc/rfc3954.txt.

[21] CLAISE, B., B. TRAMMELL, and P. AITKEN. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information. RFC 7011 (Standards Track). Internet Engineering Task Force, 2013. URL: http://www.ietf.org/rfc/rfc7011.txt.

[22] COMBS, G. Wireshark network protocol analyzer. 2013. URL: http://www.wireshark.org/ (visited on 10/15/2013).

[23] COMMITTEE ON ACADEMIC CAREERS FOR EXPERIMENTAL COMPUTER SCIENTISTS, NATIONAL RESEARCH COUNCIL. Academic Careers for Experimental Computer Scientists and Engineers. The National Academies Press, 1994. ISBN: 978-0-309-04931-3. URL: http://www.nap.edu/openbook.php?record_id=2236.

[24] CUI, A. and S. STOLFO. A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. In: *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC'10)*. New York, NY, USA, 2010, pp. 97–106.

[25] CUNHA, I., F. SILVEIRA, R. OLIVEIRA, R. TEIXEIRA, and C. DIOT. Uncovering Artifacts of Flow Measurement Tools. In: *Passive and Active Network Measurement*. Vol. 5448. LNCS. Springer Berlin Heidelberg, 2009, pp. 187–196. ISBN: 978-3-642-00974-7.

[26] ČELEDA, P., M. KOVÁČIK, T. KONÍŘ, V. KRMÍČEK, P. ŠPRINGL, and M. ŽÁDNÍK. FlowMon Probe. In: *Network Studies: Selected Technical Reports*. Prague: CESNET, 2007. ISBN: 978-80-239-9285-4.

[27] DANELUTTO, M., L. DERI, and D. D. SENSI. Network Monitoring on Multicores with Algorithmic Skeletons. In: *PARCO*. 2011, pp. 519–526.

[28] DEGIOANNI, L. and G. VARENNI. Introducing scalability in network measurement: toward 10 Gbps with commodity hardware. In: *IMC '04: Proceedings of the 4th ACM SIGCOMM conference on Internet measurement*. Taormina, Sicily, Italy: ACM, 2004, pp. 233–238. ISBN: 1-58113-821-0.

[29] DENNING, D. E. An Intrusion-Detection Model. In: *IEEE Symposium on Security and Privacy*. 1986, pp. 118–133.

[30] DENNING, D. E. An intrusion-detection model. In: *IEEE Trans. Softw. Eng.* 13.2 (1987), pp. 222–232. ISSN: 0098-5589.

[31] DERI, L. and F. FUSCO. Realtime MicroCloud-based flow aggregation for fixed and mobile networks. In: *Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International*. 2013, pp. 96–101.

[32] DERI, L. nProbe: An Open Source NetFlow Probe for Gigabit Networks. In: *Proceedings of the TERENA Networking Conference, TNC'03*. 2003.

[33] DERI, L. Improving Passive Packet Capture:Beyond Device Polling. 2004. URL: `http://luca.ntop.org/Ring.pdf` (visited on 09/10/2013).

[34] DERI, L. DNA - Direct NIC Access. 2012. URL: `http://www.ntop.org/products/pf_ring/dna/` (visited on 09/25/2013).

[35] DERI, L., V. LORENZETTI, and S. MORTIMER. Collection and Exploration of Large Data Monitoring Sets Using Bitmap Databases. In: *Traffic Monitoring and Analysis*. Vol. 6003. LNCS. Springer Berlin Heidelberg, 2010, pp. 73–86. ISBN: 978-3-642-12364-1.

[36] ERTOZ, L., E. EILERTSON, A. LAZAREVIC, P.-N. TAN, V. KUMAR, J. SRIVASTAVA, and P. DOKAS. MINDS - Minnesota Intrusion Detection System. In: *Next Generation Data Mining*. MIT Press, 2004.

[37] FAZZI, F. Lightaidra – IRC-based mass router scanner/exploiter. 2012. URL: `http://packetstormsecurity.org/files/109244` (visited on 09/15/2013).

[38] FRY, C. and M. NYSTROM. Security monitoring - proven methods for incident detection on enterprise networks. O'Reilly, 2009, pp. I–XV, 1–227. ISBN: 978-0-596-51816-5.

[39] FUSCO, F. and L. DERI. High speed network traffic analysis with commodity multi-core systems. In: *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. IMC '10. Melbourne, Australia: ACM, 2010, pp. 218–224. ISBN: 978-1-4503-0483-2.

[40] GARCÍA-DORADO, J., F. MATA, J. RAMOS, P. Santiago del RÍO, V. MORENO, and J. ARACIL. High-Performance Network Traffic Processing Systems Using Commodity Hardware. In: *Data Traffic Monitoring and Analysis*. Vol. 7754. LNCS. Springer Berlin Heidelberg, 2013, pp. 3–27. ISBN: 978-3-642-36783-0.

[41] HAAG, P. Watch your Flows with NfSen and NFDUMP. 2005. URL: `http://meetings.ripe.net/ripe-50/presentations/ripe50-plenary-tue-nfsen-nfdump.pdf` (visited on 09/15/2013).

[42] HARRINGTON, D., R. PRESUHN, and B. WIJNEN. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. RFC 3411 (Standards Track). Network Working Group, 2002. URL: `http://www.ietf.org/rfc/rfc3411.txt`.

[43] HOFSTEDE, R., I. DRAGO, A. SPEROTTO, R. SADRE, and A. PRAS. Measurement Artifacts in NetFlow Data. In: *Passive and Active Measurement*. Vol. 7799. LNCS. Springer Berlin Heidelberg, 2013, pp. 1–10. ISBN: 978-3-642-36515-7.

[44] IANA. IP Flow Information Export (IPFIX) Entities. 2013. URL: http://www.iana.org/assignments/ipfix/ipfix.xhtml (visited on 10/15/2013).

[45] INACIO, C. M. and B. TRAMMELL. YAF: Yet Another Flowmeter. In: *Proceedings of the 24th international conference on Large installation system administration*. LISA'10. San Jose, CA: USENIX Association, 2010, pp. 1–16.

[46] KIND, A., M. STOECKLIN, and X. DIMITROPOULOS. Histogram-based traffic anomaly detection. In: *Network and Service Management, IEEE Transactions on* 6.2 (2009), pp. 110–121. ISSN: 1932-4537. DOI: 10.1109/TNSM.2009.090604.

[47] KIPP, S. Storage Growth and Ethernet. 2011. URL: http://www.ieee802.org/3/ad_hoc/bwa/public/sep11/kipp_01a_0911.pdf (visited on 09/24/2013).

[48] KRUEGEL, C., F. VALEUR, and G. VIGNA. Intrusion Detection and Correlation: Challenges and Solutions. Vol. 14. Advances in Information Security. Springer, 2005. ISBN: 978-0-387-23398-7. DOI: http://dx.doi.org/10.1007/b101493.

[49] LAKHINA, A., M. CROVELLA, and C. DIOT. Diagnosis Network-Wide Traffic Anomalies. In: *ACM SIGCOMM '04*. New York, NY, USA: ACM Press, 2004, pp. 219–230. ISBN: 1-58113-862-8.

[50] LAKHINA, A., M. CROVELLA, and C. DIOT. Mining Anomalies using Traffic Feature Distributions. In: *ACM SIGCOMM, Philadelphia, PA, August 2005*. New York, NY, USA: ACM Press, 2005, pp. 217–228. ISBN: 1-59593-009-4.

[51] LANCOPE. StealthWatch FlowCollector. 2013. URL: http://www.lancope.com/products/stealthwatch-system/flowcollector/ (visited on 10/15/2013).

[52] LAW, D., D. DOVE, J. D'AMBROSIA, M. HAJDUCZENIA, M. LAUBACH, and S. CARLSON. Evolution of ethernet standards in the IEEE 802.3 working group. In: *Communications Magazine, IEEE* 51.8 (2013), pp. –. ISSN: 0163-6804. DOI: 10.1109/MCOM.2013.6576344.

[53] LAW, D. ET AL. IEEE 802.3 Industry Connections Ethernet Bandwidth Assessment. 2012. URL: http://www.ieee802.org/3/ad_hoc/bwa/BWA_Report.pdf (visited on 09/24/2013).

[54] LEE, Y. and Y. LEE. Toward scalable internet traffic measurement and analysis with Hadoop. In: *SIGCOMM Comput. Commun. Rev.* 43.1 (Jan. 2012), pp. 5–13. ISSN: 0146-4833. DOI: 10.1145/2427036.2427038.

[55] LESK, M. The New Front Line: Estonia under Cyberassault. In: *Security Privacy, IEEE* 5.4 (2007), pp. 76–79. ISSN: 1540-7993. DOI: 10.1109/MSP.2007.98.

[56] LI, B., J. SPRINGER, G. BEBIS, and M. H. GUNES. A survey of network flow applications. In: *Journal of Network and Computer Applications* 36.2 (2013), pp. 567 –581. ISSN: 1084-8045. DOI: http://dx.doi.org/10.1016/j.jnca.2012.12.020.

[57] LU, H., K. ZHENG, B. LIU, X. ZHANG, and Y. LIU. A Memory-Efficient Parallel String Matching Architecture for High-Speed Intrusion Detection. In: *Selected Areas in Communications, IEEE Journal on* 24.10 (2006), pp. 1793–1804. ISSN: 0733-8716. DOI: 10.1109/JSAC.2006.877221.

[58] MANDIANT. APT1: Exposing One of China's Cyber Espionage Units. 2013. URL: http://intelreport.mandiant.com/ (visited on 09/26/2013).

[59] NETFPGA. NetFPGA 1G and 10G platform. 2013. URL: http://www.netfpga.org/ (visited on 10/19/2013).

[60] OPEN INFORMATION SECURITY FOUNDATION. Suricata – Open Source IDS / IPS / NSM engine. 2013. URL: http://suricata-ids.org (visited on 09/16/2013).

[61] PASSERI, P. 2013 Cyber Attacks Timeline Master Index. 2013. URL: http://hackmageddon.com/2013-cyber-attacks-timeline-master-index/ (visited on 09/26/2013).

[62] PAXSON, V., K. ASANOVIĆ, S. DHARMAPURIKAR, J. LOCKWOOD, R. PANG, R. SOMMER, and N. WEAVER. Rethinking hardware support for network analysis and intrusion prevention. In: *Proceedings of the 1st USENIX Workshop on Hot Topics in Security*. HOTSEC'06. Vancouver, B.C., Canada: USENIX Association, 2006, pp. 11–11.

[63] PAXSON, V. Bro: a system for detecting network intruders in real-time. In: *Proceedings of the 7th conference on USENIX Security Symposium - Volume 7*. SSYM'98. San Antonio, Texas: USENIX Association, 1998, pp. 3–3.

[64] REHÁK, M., M. PĚCHOUČEK, M. GRILL, J. STIBOREK, K. BARTOŠ, and P. ČELEDA. Adaptive Multiagent System for Network Traffic Monitoring. In: *IEEE Intelligent Systems* 24 (2009). ISSN: 1541-1672.

[65] RIZZO, L., L. DERI, and A. CARDIGLIANO. 10 Gbit/s Line Rate Packet Processing Using Commodity Hardware: Survey and new Proposals. 2011. URL: http://luca.ntop.org/10g.pdf (visited on 09/10/2013).

[66] ROESCH, M. Snort - Lightweight Intrusion Detection for Networks. In: *Proceedings of the 13th USENIX conference on System administration*. LISA '99. Seattle, Washington: USENIX Association, 1999, pp. 229–238.

[67] SADASIVAN, G., N. BROWNLEE, B. CLAISE, and J. QUITTEK. Architecture for IP Flow Information Export. RFC 5470 (Informational). Internet Engineering Task Force, 2009. URL: http://www.ietf.org/rfc/rfc5470.txt.

[68] SCARFONE, K. and P. MELL. Guide to Intrusion Detection and Prevention Systems (IDPS). Tech. rep. Recommendations of the National Institute of Standards and Technology, 2007. URL: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[69] SOOD, A. and R. ENBODY. Targeted Cyberattacks: A Superset of Advanced Persistent Threats. In: *Security Privacy, IEEE* 11.1 (2013), pp. 54–61. ISSN: 1540-7993. DOI: 10.1109/MSP.2012.90.

[70] SOURCEFIRE, INC. SNORT – Intrusion Prevention System. 2013. URL: http://www.snort.org (visited on 09/16/2013).

[71] SPEROTTO, A., G. SCHAFFRATH, R. SADRE, C. MORARIU, A. PRAS, and B. STILLER. An Overview of IP Flow-Based Intrusion Detection. In: *Communications Surveys Tutorials, IEEE* 12.3 (2010), pp. 343–356. ISSN: 1553-877X. DOI: http://dx.doi.org/10.1109/SURV.2010.032210.00054.

[72] STEINBERGER, J., L. SCHEHLMANN, S. ABT, and H. BAIER. Anomaly Detection and Mitigation at Internet Scale: A Survey. In: *Emerging Management Mechanisms for the Future Internet*. Vol. 7943. LNCS. Springer Berlin Heidelberg, 2013, pp. 49–60. ISBN: 978-3-642-38997-9.

[73] TCPDUMP.ORG. TCPDUMP command-line packet analyzer. 2013. URL: `http://www.tcpdump.org` (visited on 10/15/2013).

[74] VELAN, P. Practical experience with IPFIX flow collectors. In: *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*. 2013, pp. 1021–1026. ISBN: 978-1-4673-5229-1.

[75] VELAN, P., T. JIRSÍK, and P. ČELEDA. Design and Evaluation of HTTP Protocol Parsers for IPFIX Measurement. In: *Advances in Communication Networking*. Vol. 8115. LNCS. Springer Berlin Heidelberg, 2013, pp. 136–147. ISBN: 978-3-642-40551-8.

[76] VIEIRA, K., A. SCHULTER, C. WESTPHALL, and C. WESTPHALL. Intrusion Detection for Grid and Cloud Computing. In: *IT Professional* 12.4 (2010), pp. 38–43. ISSN: 1520-9202. DOI: `10.1109/MITP.2009.89`.

[77] VIGNA, G. Network intrusion detection: dead or alive? In: *Proceedings of the 26th Annual Computer Security Applications Conference*. ACSAC '10. Austin, Texas: ACM, 2010, pp. 117–126. ISBN: 978-1-4503-0133-6.

[78] VIGNA, G., W. ROBERTSON, V. KHER, and R. A. KEMMERER. A Stateful Intrusion Detection System for World-Wide Web Servers. In: *Proceedings of the 19th Annual Computer Security Applications Conference*. ACSAC '03. Washington, DC, USA: IEEE Computer Society, 2003, pp. 34–. ISBN: 0-7695-2041-3.

[79] WAND NETWORK RESEARCH GROUP. DAG Project. 2013. URL: `http://dag.cs.waikato.ac.nz` (visited on 09/24/2013).

[80] XU, K., Z.-L. ZHANG, and S. BHATTACHARYYA. Profiling internet backbone traffic: behavior models and applications. In: *SIGCOMM '05*. Philadelphia, Pennsylvania, USA: ACM Press, 2005, pp. 169–180. ISBN: 1-59593-009-4.

[81] ŽÁDNÍK, M., L. POLČÁK, O. LENGÁL, M. ELICH, and P. KRAMOLIŠ. FlowMon for Network Monitoring. 2010. URL: `http://archiv.cesnet.cz/doc/techzpravy/2010/flowmon/` (visited on 10/15/2013).

Part II

Collection of Papers

Appendix A

Hardware-Accelerated Framework for Security in High-Speed Networks

by NOVOTNÝ, J., P. ČELEDA, and M. ŽÁDNÍK

In: *Information Assurance for Emerging and Future Military Systems.* RTO Meeting Proceedings MP-IST-076, Ljubljana, Slovenia: NATO Research and Technology Organization, 2008. RTO-MP-IST-076 AC/323(IST-076)TP/238.

Appendix B

Hardware Acceleration for Cyber Security

by NOVOTNÝ, J., P. ČELEDA, T. DEDEK, and R. KREJČÍ

In: *Information Assurance and Cyber Defence*. RTO Meeting Proceedings MP-IST-091, Tallinn, Estonia: NATO Research and Technology Organization, 2010, pp. 86-101. ISBN 978-92-837-0115-6.

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-091)TP/328

www.rto.nato.int

RTO MEETING PROCEEDINGS

MP-IST-091

Information Assurance and Cyber Defence

(Assurance de l'information et cyberdéfense)

Papers presented at the Information Systems and Technology Panel (IST) Symposium held in Tallinn, Estonia, 22 - 23 November 2010.

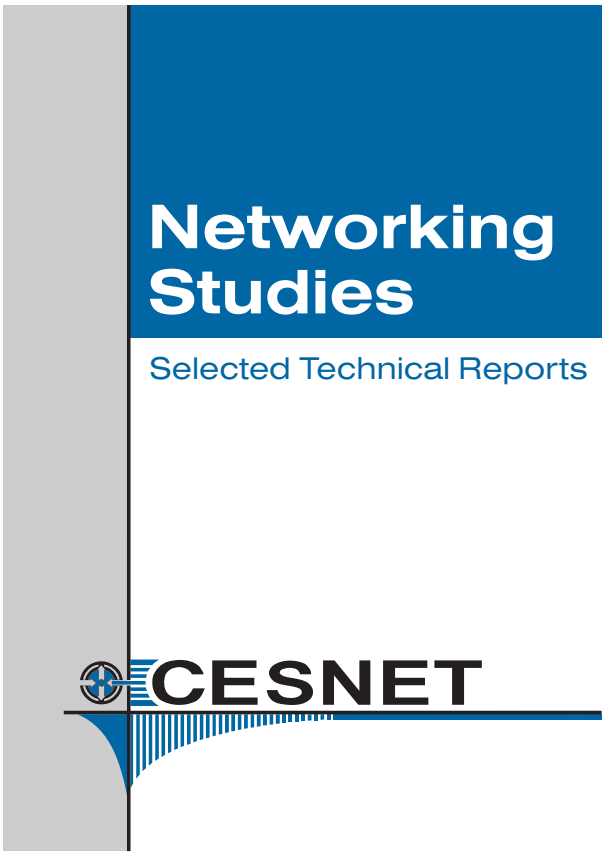
Published November 2010

Appendix C

FlowMon Probe

by ČELEDA, P., M. KOVÁČIK, T. KONÍŘ, V. KRMÍČEK, P. ŠPRINGL, and M. ŽÁDNÍK

In: LHOTKA, L. and P. SATRAPA (Eds.). *Network Studies: Selected Technical Reports*. Prague: CESNET, 2007, pp. 67-81. ISBN 978-80-239-9285-4.

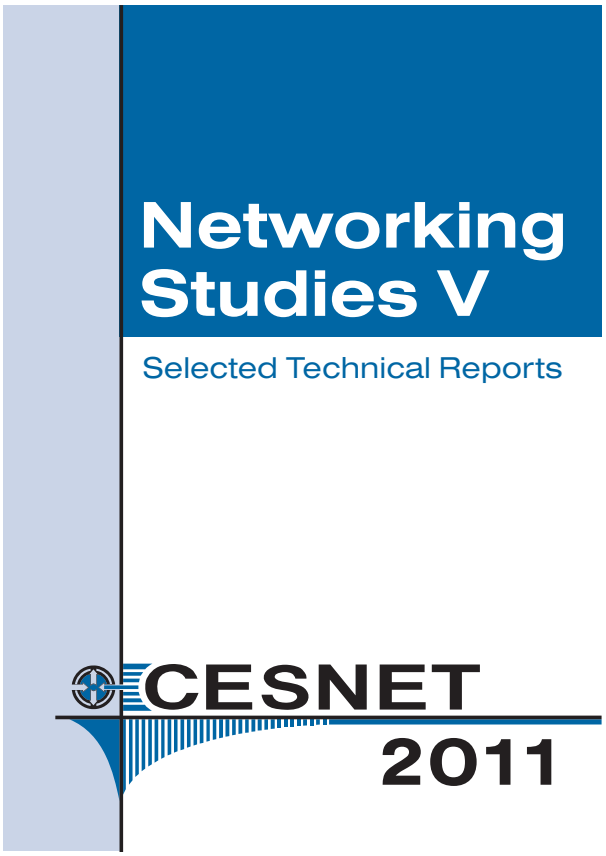


Appendix D

HAMOC - Hardware-Accelerated Monitoring Center

by ČELEDA, P., R. KREJČÍ, J. BARIENČÍK, M. ELICH, and V. KRMÍČEK

In: LHOTKA, L. and P. SATRAPA (Eds.). *Networking Studies V : Selected Technical Reports*. Prague: CESNET, 2011, pp. 107-133. ISBN 978-80-904689-1-7.

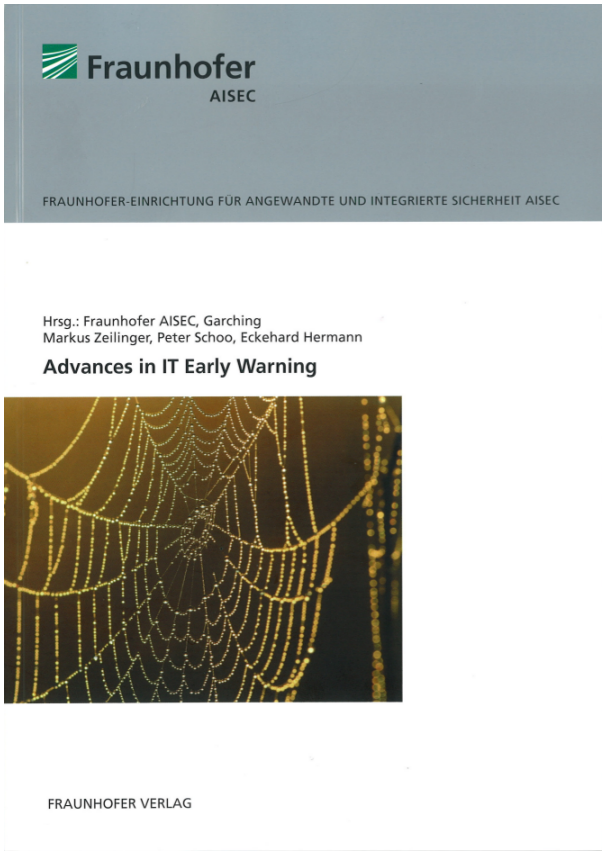


Appendix E

Flow Data Collection in Large Scale Networks

by ČELEDA, Pavel and Vojtěch KRMÍČEK

In: *Advances in IT Early Warning*. Ed. by ZEILINGER, M., P. SCHOO and E. HERMANN. Stuttgart: Fraunhofer Verlag, 2013, pp. 30-40. ISBN 978-3-8396-0474-8.



Appendix F

An Investigation Into Teredo and 6to4 Transition Mechanisms: Traffic Analysis

by ELICH, M., P. VELAN, T. JIRSÍK, and P. ČELEDA

To appear In: *WNM 2013, The 7th IEEE Workshop on Network Measurements*. 38th IEEE Conference on Local Computer Networks, LCN 2013, Sydney, Australia: IEEE Computer Society, 2013, pp. 1046-1052. ISBN 978-1-4799-0540-9.

Appendix G

Large-Scale Geolocation for NetFlow

by ČELEDA, P., P. VELAN, M. RÁBEK, R. HOFSTEDE, and A. PRAS

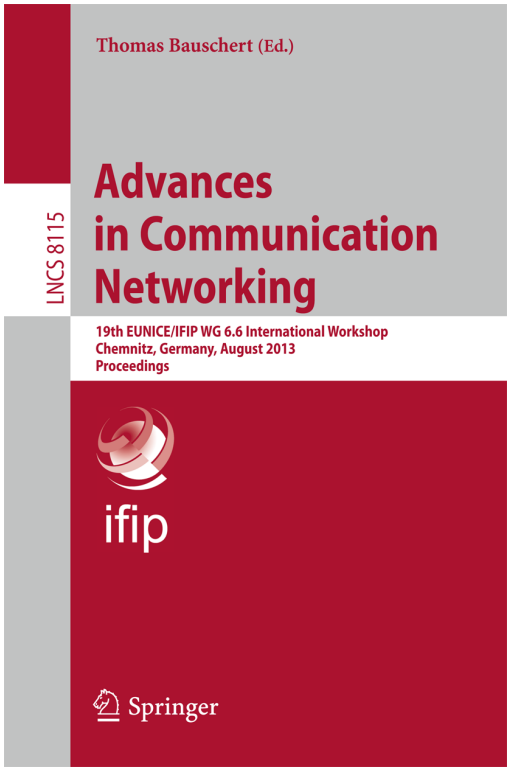
In: De TURCK, F. et al. (Eds.). *Experience Session*. IFIP/IEEE International Symposium on Integrated Network Management, IM 2013, Ghent, Belgium: IEEE Communications Society, 2013, pp. 1015-1020. ISBN 978-1-4673-5229-1.

Appendix H

Design and Evaluation of HTTP Protocol Parsers for IPFIX Measurement

by VELAN, P., T. JIRSÍK, and P. ČELEDA

In: BAUSCHERT, T. (Ed.). *Advances in Communication Networking*. 19th EUNICE/IFIP WG 6.6 International Workshop, Chemnitz, Germany: Springer Berlin Heidelberg, 2013, LNCS Volume 8115, pp. 136-147. ISBN 978-3-642-40551-8. DOI 10.1007/978-3-642-40552-5_13.

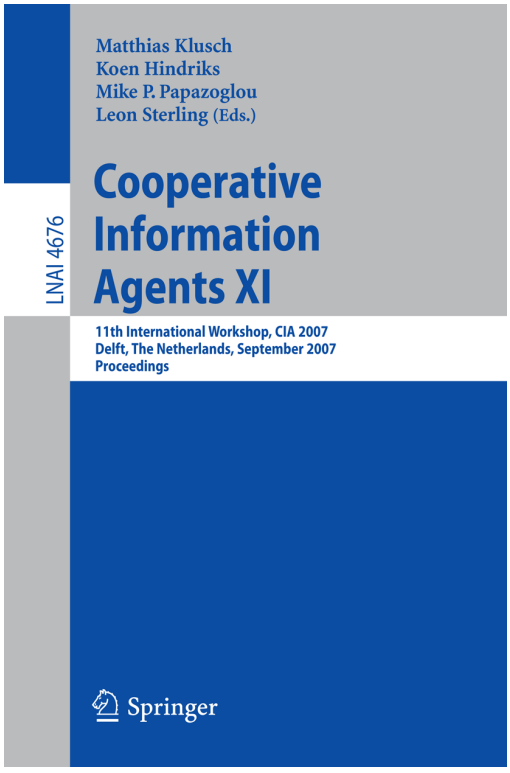


Appendix I

High-Performance Agent System for Intrusion Detection in Backbone Networks

by REHÁK, M., M. PĚCHOUČEK, P. ČELEDA, V. KRMÍČEK, J. MONINEC, T. DYMÁČEK, and D. MEDVIGY

In: KLUSCH, M. et al. (Eds.). *Cooperative Information Agents XI*. 11th International Workshop, CIA 2007, Delft, The Netherlands: Springer Berlin Heidelberg, 2007, LNAI Volume 4676, pp. 134-148. ISBN 978-3-540-75118-2. DOI 10.1007/978-3-540-75119-9_10.

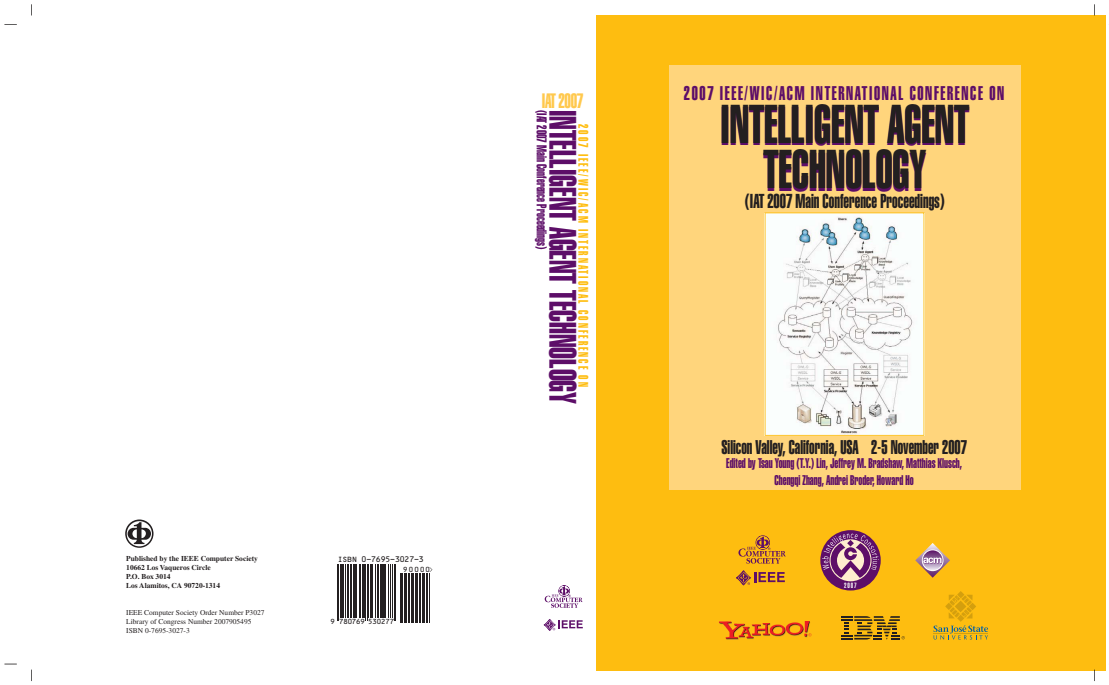


Appendix J

High-Speed Network Traffic Acquisition for Agent Systems

by ČELEDA, P., V. KRMÍČEK, M. REHÁK, and D. MEDVIGY

In: LIN, T.Y. et al. (Eds.). *Intelligent Agent Technology*. IEEE/WIC/ACM International Conference, IAT 2007, Silicon Valley, USA: IEEE Computer Society, 2007, pp. 477-480. ISBN 978-0-7695-3027-7. DOI 10.1109/IAT.2007.66.



Appendix K

CAMNEP: An intrusion detection system for high-speed networks

by REHÁK, M., M. PĚCHOUČEK, K. BARTOŠ, M. GRILL, P. ČELEDA, and V. KRMÍČEK

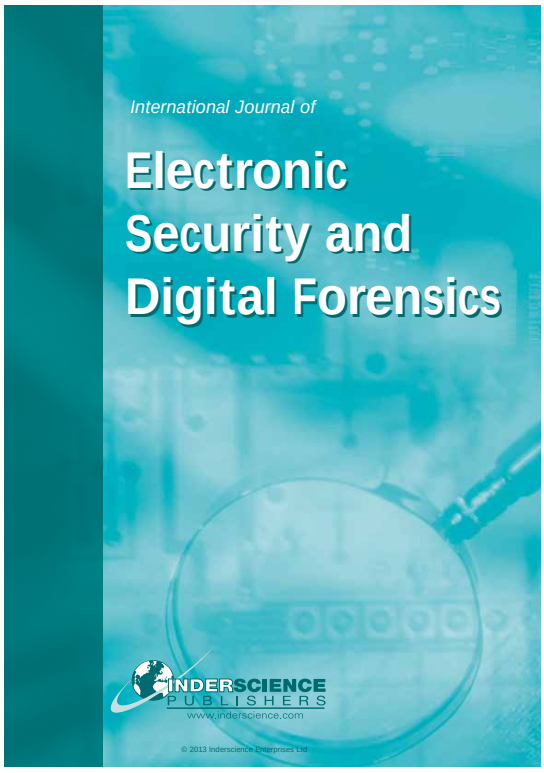
Progress in Informatics. 2008, no. 5, pp. 65-74. ISSN 1349-8614. DOI 10.2201/NiiPi.2008.5.7.

Appendix L

Collaborative approach to network behaviour analysis based on hardware-accelerated FlowMon probes

by REHÁK, M., M. PĚCHOUČEK, M. GRILL, K. BARTOŠ, V. KRMÍČEK, and P. ČELEDA

International Journal of Electronic Security and Digital Forensics. 2009, vol. 2, no. 1, pp. 35-48. ISSN 1751-911X. DOI 10.1504/IJESDF.2009.023874.



Appendix M

Adaptive Multiagent System for Network Traffic Monitoring

by REHÁK, M., M. PĚCHOUČEK, M. GRILL, J. STIBOREK, K. BARTOŠ, and P. ČELEDA

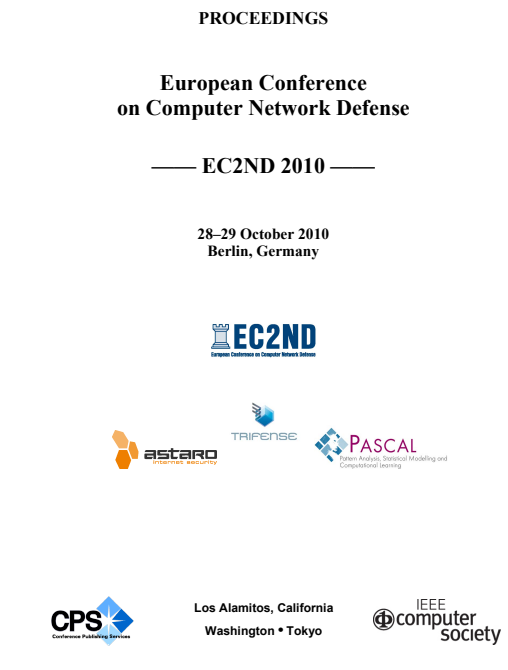
IEEE Intelligent Systems. 2009, vol. 24, no. 3, pp. 16-25. ISSN 1541-1672. DOI 10.1109/-MIS.2009.42.

Appendix N

Embedded Malware - An Analysis of the Chuck Norris Botnet

by ČELEDA, P., R. KREJČÍ, J. VYKOPAL, and M. DRAŠAR

In: RIECK, K. (Ed.). *European Conference on Computer Network Defense*. EC2ND 2010, Berlin, Germany: IEEE Computer Society, 2010, pp. 3-10. ISBN 978-1-4244-9377-7. DOI 10.1109/-EC2ND.2010.15.



Appendix O

Revealing and Analysing Modem Malware

by ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK

In: *Communication and Information Systems Security Symposium*. IEEE International Conference on Communications, ICC 2012, Ottawa, Canada: IEEE Communications Society, 2012, pp. 971-975. ISBN 978-1-4577-2053-6. DOI 10.1109/ICC.2012.6364598.

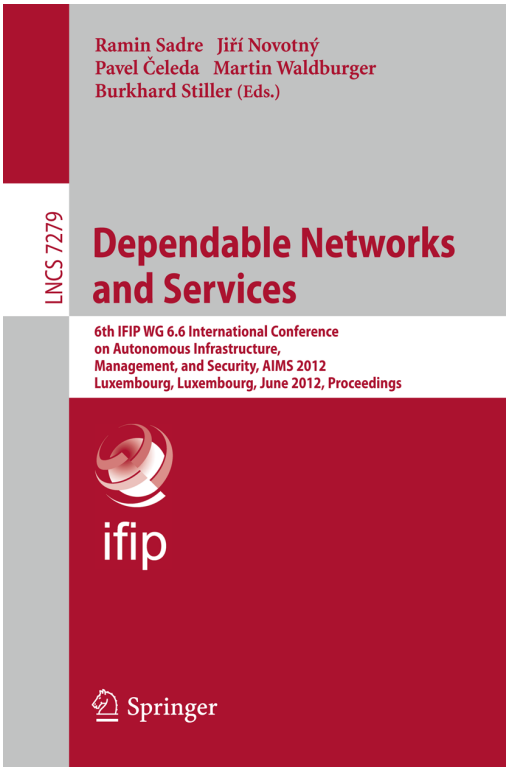
IEEE INTERNATIONAL CONFERENCE
ON COMMUNICATIONS
INDUSTRY FORUM & EXHIBITION

Appendix P

Traffic Measurement and Analysis of Building Automation and Control Networks

by KREJČÍ, R., P. ČELEDA, and J. DOBROVOLNÝ

In: SADRE, R. et al. (Eds.). *Dependable Networks and Services*. 6th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2012, Luxembourg, Luxembourg: Springer Berlin Heidelberg, 2012, LNCS Volume 7279, pp. 62-73. ISBN 978-3-642-30632-7. DOI 10.1007/978-3-642-30633-4_9.



Appendix Q

Flow-Based Security Issue Detection in Building Automation and Control Networks

by ČELEDA, P., R. KREJČÍ, and V. KRMÍČEK

In: SZABÓ, R. and A. VIDÁCS (Eds.). *Information and Communication Technologies*. 18th EUNICE/ IFIP WG 6.2, 6.6 International Conference, EUNICE 2012, Budapest, Hungary: Springer Berlin Heidelberg, 2012, LNCS Volume 7479, pp. 64-75. ISBN 978-3-642-32807-7. DOI 10.1007/978-3-642-32808-4_7.