Institute of IT-Security
and Security Law

ISL University of Passau D-94030 Passau

Dana Komarkova
R&D office
FI MU
Botanicka 68a
602 00 Brno
Czech Republic

Prof. Dr. rer. nat. Joachim Posegga
Chair of IT Security

University of Passau
Innstr. 43
D-94032 Passau

Tel. + 49 851 509-30 21
Fax + 49 851 509-32 12

isl-info@uni-passau.de
www.isl.uni-passau.de

Passau, April 1, 2014

Habilitation thesis reader's report

Faculty	Faculty of Informatics, Masaryk University
Field of Habilitation	Informatics
Applicant	Ing. Pavel Čeleda, Ph.D.
Affiliation	Masaryk University, Institute of Computer Science
Habilitation Thesis	„Network Traffic Analysis for Cyber Security"

This report considers the cumulative habilitation thesis entitled "Network Traffic Analysis for Cyber Security" submitted by Pavel Čeleda in October 2013. The thesis is comprised of 17 publications (appendices A-Q) in the area of Networking and Network Security.

We will begin with briefly reviewing and classifying the submitted publication.

Focus of the thesis

The research area of the thesis can be characterized as practical network security; the work carried out is largely motivated from the perspective of a researcher confronted with the challenge of maintaining security of large, high speed data networks. The research goals do not span over the whole area of Security, instead they are concentrated on Integrity and partially availability of network infrastructures and components.

The research takes into account particular approaches where maintaining security properties of such networks is carried out in parallel to the evolving and growing of these networks driven by their usage. The papers comprising the habilitation thesis nicely demonstrate this approach to the problem space, as they gradually extend their scope towards maintaining such security properties:

The first group of publications in appendices A-D is concerned with gathering data for analyzing traffic in high-speed networks, thus it provides a basis for the analytical evaluation and monitoring of security; the work is largely based on IP flows, a technique to represent data flow in large-scale networks. The work follows a strong engineering-based approach; it offers interesting insights since it combines

hardware-near aspects with software-based approaches. The research was carried out jointly with other colleagues; Dr. Čeleda's contribution is largely on the software side. The publications describe practical approaches to solving the given problems under real-word constraints rather than addressing fundamental research questions that would contribute to insights into the theoretical underpinning of the area; the approaches taken do follow a straight engineering paradigm instead.

The subsequently presented research results in the publications comprising appendices E-H go beyond collecting data flow information: They also take structural information into account for maintaining security in network infrastructures. In particular, approaches to integrate geolocation and to consider protocols at higher OSI-layers like HTTP are followed. The presented results provide significant contributions to enhance IP-based traffic flow information with knowledge about network topologies and application usage in these networks. Both aspects are very relevant when considering operational security in high-speed networks.

The publications of appendices I-M extend towards anomaly and intrusion detection in networks; the research is again tightly coupled to managing a high-speed network infrastructure: The given needs and constraints lead to innovative solutions for detecting attacks to networks, which is a prerequisite for defending them.

Lastly, the contributions in appendices N-Q demonstrate that the candidate moved into core areas in IT-Security, namely network intrusion detection and detection of integrity violations in network components like routers or modems. This work is conceptually closely related to the other presented approaches but extends the scope of the candidate's research to detecting and mitigating attacks based on network monitoring and evaluating IP flows to aggregate network meta-data. Again, the work presented contributes to the advancement of the research field.

Contributions of the thesis

Informatics is a field where two scientific paradigms merge: Firstly, mathematical and analytical approaches that are primarily manifested in theoretical Computer Science. Second, engineering-based approaches, those are predominant in hardware-related areas and networking. Security is a discipline that lies orthogonal to these poles and spans over most of the "vertical" subareas in Informatics/Computer Science.

The habilitation thesis submitted by Pavel Čeleda takes an engineering-centric approach to the problem(s) considered: The research presented is motivated by observations made in practical network management, and the approaches carried out are derived from needs thereof; thus real-life problems are addressed, which is always a very positive aspect for IT-Security research. Pavel Čeleda's contributions span from core topics of network monitoring towards intrusion detection based on network flow meta-data and structural information like geolocation.

The contribution to IT-Security, or cyber-security (the notion the author has chosen), is to provide tools and techniques that help maintaining operational security, in particular integrity, of high-speed network infrastructure. These networks are not test beds, but operational infrastructure being used extensively on a daily basis. Under these constraints, security is not a goal *per se*, but a property that needs to be maintained for providing a service for users of these network infrastructures. When carrying out research in such an area, many other aspects need to be taken into account, ranging from usability, options for deployment, to impacts to availability.

This being said, my assessment of the thesis is as follows: Pavel Čeleda clearly demonstrated in his work that he is able to analyse the requirements and constraints in large-scale, high-speed networks, to identify existing threats and challenges, and to map these observations into scientifically new and technologically innovative approaches that tackle these problems. The approaches taken follow engineering approaches and clearly go beyond the state-of-the-art in the field. Thus, the thesis shows the ability of the candidate to carry out independent research. The contribution is always oriented towards solving the concrete problems and mastering the involved challenges, only to a lesser extend does the work address fundamental problems. It is focused, applied research in the tradition of engineering disciplines or practical Computer Science.

The quality of the presented publications is good, though not outstanding; this is all reflected in the publication media (conferences) that were chosen. Most of the work is joint work with other colleagues; the contributions of the candidate are clearly indicated and consistent.

My questions to answer for the habilitation thesis defense are:

1. Security is often seen as field addressing aspects of Confidentiality, Integrity, and Availability; please clarify where your contributions are here and how they relate to all three aspects.
2. Try to extrapolate the future advancement in Networking in the next ten years and outline the major threats that you see arising.
3. How would you further advance the research you carried out so far to address the issues of Q 2?

Conclusion

Pavel Čeleda's habilitation thesis of "Network Traffic Analysis for Cyber Security" dated October 2013 meets the standard requirements for a habilitation thesis in the field of Informatics.

Joachim Posegga