Carnegie Mellon
CyLab
CONFIDENCE FOR A NETWORKED WORLD

Carnegie Mellon CyLab
4720 Forbes Avenue
CIC Building
Pittsburgh, PA 15213-3890
Professor Virgil Gligor, co-Director

March 31, 2014

Professor Václav Matyáš
Faculty of Informatics
Masaryk University
Botaniká 68a
602 00 Brno, Czeck Republic

Re: Dr. Pavel Čeleda's Habilitation Thesis

Dear Professor Matyáš,

I am writing this letter in response to your request for an evaluation of Dr. Pavel Čeleda's habilitation thesis. I have read the thesis, published articles, and technical reports in which by Dr. Čeleda is the first author and primary contributor. I believe I have sufficient information to from an informed opinion regarding his thesis. I must add that I have never met, nor collaborated, nor corresponded with Dr. Čeleda and hence I do not have a conflict of interest in rendering an opinion of his accomplishments.

Contributions. Dr. Čeleda's thesis addresses four specific areas of network security, namely (1) capture and processing of communication traffic in high-speed networks, (2) network traffic measurement and analysis including packet tracing, flow and volume statistics, (3) network intrusion detection, and (4) flow-based monitoring in embedded systems, specifically in building automation and control networks. The state of the art in the first three areas is carefully analyzed (Chapter 2) and the impact of his contributions is also discussed (Chapter 3). The state of the art in flow-based monitoring in embedded systems is described along with the specific contribution and impact (Chapter 3).

In the area of communication traffic capture and processing, Čeleda's work proposes new devices and software for high-speed network monitoring and flow capture; e.g., COMBO card family used in FlowMon probe and HAMOC system. The technical ideas developed and their implementations are novel and useful. For example, the fact that the HAMOC system allows the use of widely available non-proprietary tools will enable wide dissemination of his research results. The successful transition of the technology developed to INVEA-TECH represents a good metric of success in this area.

In the area of network traffic measurement and analysis, Čeleda's work proposes a novel mechanism for large-scale flow geo-location; e.g., IP address geo-location. The approach proposed integrates geo-location (e.g., country-level information) with flow exporters and collectors and thus enables fast and continuous flow pre-processing. This enables security administrators to filter, aggregate, and analyze flow data in near real time – a nice contribution to the filed.

In the area of network intrusion detection, Čeleda's work builds upon the results obtained in the previous two areas and introduces trust and reputation models to reach more accurate conclusions regarding the maliciousness of individual network flows. Enhancing network-flow classification with supplementary information is essential in cases where malicious network flows might otherwise appear to be legitimate; e.g., protocol and traffic compliant.

Finally, in the area of flow-based monitoring in embedded systems, Čeleda's work is both new and novel. In particular, he observes that the interconnection of internal embedded system networks (e.g., building automation) and public networks, such as the Internet, exposes the embedded systems to external attacks. His work led to the discovery of the Chuck Norris botnet and to convincing illustrations of the effects of malware infestation of network and automation devices. His work on the flow-based monitoring of building automation networks to detect security threats and its results is both an example of good security engineering and a public wakeup call to industrial control operators.

Questions. The two questions I would ask Dr. Čeleda are these:

1) Intrusion detection systems (IDSes) have traditionally not taken into account the semantics of various (e.g., control) processes in industrial control systems. Based on his experience with building automation control, to what extent does he think an IDS can take advantage of process control semantics, and what are the fundamental limitations of IDSes in this sense?

2) His thesis argues that network monitoring and botnet analysis can detect potential malware-infestation attacks before hosts are infected. Is this always possible, or it possible only on a case-by-case basis? If not always possible, how can one determine when an attack can/cannot be anticipated?

Dr. Čeleda answers to these questions can be provided verbally to the members of his habilitation thesis committee. Written answers addressed to me are unnecessary.

Minor corrections. A few minor typographical errors are noted below:

1. page 4, fist line, "Last, but no least," should read "Last[] but no[t] least,"

2. page 6, last full paragraph, last sentence, "patter matching" should read "patter[n] matching"

3. page 8, first line, "Architecture for …" should read "[The] architecture for…"

4. page 8, last full paragraph, second sentence, "250.000 flows/s" should read "250[,]000 flows/s," in English numerical notation.

Other than these minor typographical errors, which can be easily corrected, the thesis is well written and understandable with minimum effort.

Recommendation. In summary, I believe that Dr. Čeleda's thesis meets the standard for habilitation in the field of informatics. I have no reservation in recommending his thesis for habilitation to the Faculty Scientific Board of Masaryk University.

Sincerely yours,

V.Gligor

Virgil Gligor

Professor of ECE and co-Director, CyLab
Carnegie-Mellon University
Pittsburgh, Pennsylvania 15213
Tel. 412-268-9833
412-268-3729 (assistant)

Virgil Gligor – Biographical Note

Virgil D. Gligor received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. He taught at the University of Maryland between 1976 and 2007, and is currently a Professor of Electrical and Computer Engineering at Carnegie Mellon University and co-Director of CyLab, the University's laboratory for information security, privacy and dependability. Over the past forty years, his research interests ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. He was a consultant to Burroughs Corporation, IBM, and SAP and is currently serving on Microsoft's Trusted Computing Academic Advisory Board (2003-present). Gligor was an Editorial Board member of Information Systems, Journal of Computer Security, ACM Transactions on Information System Security, IEEE Transactions on Computers, IEEE Transactions on Mobile Computing, and was the Editor in Chief of the IEEE Transactions on Dependable and Secure Computing. Gligor received the 2006 National Information Systems Security Award jointly given by NIST and NSA in the US, the 2011 Outstanding Innovation Award of the ACM SIG on Security Audit and Control, and the 2013 Technical Achievement Award of the IEEE Computer Society.