Methods for Intelligent Network Forensics

Jan Pluskal
Supervisor: prof. Ing. Miroslav Švéda, CSc.
Supervisor-specialist: doc. Ing. Ondřej Ryšavý, Ph.D.

Brno University of Technology, Faculty of Information Technology
Božetěchova 1/2. 612 66 Brno - Královo Pole
ipluskal@fit.vutbr.cz

March 2, 2017

Year	Class	Type	Stud	CH
2016	*ISA*	Project	41	65.6
	PDI	Lab	40	6
		Project	17	43
		BP	3	54
		DP	1	29
		Other	0	...
		Summary	0	**207.26**
2015	*ISA*	Lab	80	80
		Project	44	70.4
	PDI	Lab	52	18
		Project	29	29
		BP	4	74
		DP	1	29
		Other	0	...
		Summary	0	**364.9**

Table: Teaching activities overview.

Year	Class	Type	Stud	CH
2014	*ISA*	Lab	78	80
		Project	53	84.4
	IPK	Lab	160	76
		Project	131	65.5
		BP	2	74
		Other	0	...
		Summary	0	**377.08**
Total summary				**949.24**

Table: Teaching activities overview.

Accomplishments

- Invited speech at ISS World Europe, Cyber Security and Privacy conferences
- NES@FIT – Active Directory, data storage, ShareLaTeX administration
- WUGDays 2016, MS Fest 2017 conferences co-organization
- Cooperation with industry – research contract (400K) Safetica s.r.o
- CESNET z.s. – TNC16, IETF Berlin 2016
- Strathmore University of Kenya
  - Lectures in MST courses
  - Master thesis supervision

Cooperation on Grants

- **Integrated platform for analysis of digital data from security incidents**, VI20172020062, *Ministry of Interior of the Czech Republic*, 2017-2020
- **Design of a system for testing security in IPv6 networks and processing incidents containing private addresses**, *CESNET National Research and Education Network*, 2016-2016
- **Research and application of advanced methods in ICT**, FIT-S-14-2299, *Brno University of Technology*, 2014-2016
- **Modern Tools for Detection and Mitigation of Cyber Criminality on the New Generation Internet**, VG20102015022, *Ministry of Interior of the Czech Republic*, 2010-2015

Pluskal Jan and Ryšavý Ondřej. Detection, and Analysis of SIP Fraud Attack on 100Gb Ethernet with NEMEA System. (Invited speech). Pristina, Kosovo, 2017.

Publications 2016 I

- Pluskal Jan and Ryšavý Ondřej. Network Forensic Tool Netfox Detective. (Invited speech). Pristina, Kosovo, 2016.
- PLUSKAL Jan, RYŠAVÝ Ondřej, et al. "On the Identification of Applications from Captured Network Traffic". In: 8th International Conference on Digital Forensics Cyber Crime. New York, 2016.
- Pluskal Jan, VESELÝ Vladimír, et al. TLS/SSL Decryption Workshop. (Invited speech). Prague, Czech Republic, 2016.
- Marušic Marek, Pluskal Jan, et al. Automatization of MitM Attack for SSL/TLS Decryption, software. (Computer Software). 2016.
- Vondráček Martin, Pluskal Jan, et al. Automation of MitM Attack on WiFi Networks. (Computer Software). 2016.
- Hvězda Matěj, Pluskal Jan, et al. Network Forensics Distrubuted Platform. (Computer Software). 2016.

Publications 2016 II

Letavay Viliam, Pluskal Jan, et al. Reconstruction of Captured Communication on iOS Platform. (Computer Software). 2016.

Janeček Vít, Pluskal Jan, et al. Web Traffic Data Export to MAFF. (Computer Software). 2016.

Publications 2015 I

- Pluskal Jan, Kmeť Martin, et al. Netfox Detective - a network forensics tool for analyzing network traffic. (Computer Software). 2015.
- Pluskal Jan and Ryšavý Ondřej. Concepts of Intercepted Communication Processing with Netfox Detective. (Invited speech). Prague, Czech Republic, 2015.
- Petr Matoušek, Jan Pluskal, et al. "Advanced Techniques for Reconstruction of Incomplete Network Data". In: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2015.157 (2015), pp. 69–84. ISSN: 1867-8211.
- Jan Pluskal, Petr Matoušek, et al. "Netfox Detective: A tool for advanced network forensics analysis". In: Proceedings of Security and Protection of Information (SPI) 2015. Brno, CZ: Brno University of Defence, 2015, pp. 147–163. ISBN: 978-80-7231-997-8.

Jan Pluskal. "NetFox.Framework - The network forensic extandable analysis tool". In: Proceedings of the 20th Conference STUDENT EEICT 2014 Volume 2. Brno, CZ: Brno University of Technology, 2014, pp. 280–282. ISBN: 978-80-214-4923-7.

Jan Pluskal, Ondřej Ryšavý, et al. "NetFox - The network forensic extandable analysis tool". In: 6th AFCEA Student Conference Future of Information and Communication Technology. Bucharest, RO: University Politehnica of Bucharest, 2014, pp. 68–71. ISBN: 978-606-551-047-0.

Pluskal Jan, Veselý Vladimír, et al. Netfox.Framework - Network traffic decoder and content analyzer. (Computer Software). 2013.

Jan Pluskal. "Analýza a rekonstrukce komunikace typu instant messaging (YMSG a ICQ)". Czech. In: Proceedings of the 18th Conference Student EEICT 2012 Volume 1. Brno, CZ: Faculty of Information Technology BUT, 2012, pp. 176–178. ISBN: 978-80-214-4460-7.

Publication Summary

Type	Count
Articles	1
Conference paper	4
Invited speech	4
Software	7
Poster	1

Table: Summary of overall publication activities.

Dissertation Contents

- **Introduction** (20%)
- **Chapter 1 – From Incomplete Network Communication Towards Application Messages** (90%)
  - Challenges in TCP Reassembling
  - Building L7 PDUs from the Captured Communication
- **Chapter 2 – The Captured Communication Processing in a Distributed Environment** (20%)
  - Bottleneck Identification with Single Machine Processing
  - Data Dependencies and Parallelization
  - Multinode Processing
- **Chapter 3 – Application Protocol Identification** (40%)
  - Summary of State of the Art Methods
  - Proposal - EPI - Enhanced Probabilistic Identification
  - Proposal - EMLI - Enhanced Machine Learning Identification
- **Conclusion** (30%)

Thank You for Your Attention !