

Philipp Winter

Department of Computer Science
Karlstad University
Tel.: +46 70 009 71 57
Web: <http://www.cs.kau.se/philwint/>
Mail: philipp.winter@kau.se
GnuPG: 0x2D081E16

EDUCATION

- Karlstad University** **Sep. 2011 – present**
Ph.D. in Computer Science
Research topic: Analysis and evasion of censorship systems
Karlstad, Sweden
- Upper Austria University of Applied Sciences** **Oct. 2008 – Sep. 2010**
M.Sc. in Secure Information Systems
Pass with high distinction
Hagenberg, Austria
- Upper Austria University of Applied Sciences** **Oct. 2005 – Jul. 2008**
B.Sc. in Computer and Media Security
Pass with high distinction
Hagenberg, Austria

RESEARCH INTERESTS

I am working on the analysis and circumvention of censorship systems. In particular, I am interested in the censorship resistance of the Tor anonymity network. Aside from my current work, my research interests include most topics in computer networks and applied security.

SELECTED PUBLICATIONS

- WINTER, P., LINDSKOG, S. How China Is Blocking Tor. *Technical Report* (Karlstad University, 2012).
- WINTER, P., LAMPESBERGER, H., ZEILINGER, M., AND HERMANN, E. On Detecting Abrupt Changes in Network Entropy Time Series. In *Communications and Multimedia Security* (Ghent, 2011), Springer, pp. 194–205.
- LAMPESBERGER, H., WINTER, P., ZEILINGER, M., AND HERMANN, E. An On-line Learning Statistical Model to Detect Malicious Web Requests. In *Security and Privacy in Communication Networks* (London, 2011), Springer.
- WINTER, P., HERMANN, E., AND ZEILINGER, M. Inductive Intrusion Detection in Flow-Based Network Data using One-Class Support Vector Machines. In *New Technologies, Mobility and Security* (Paris, 2011), IEEE.

RESEARCH & INDUSTRY EXPERIENCE

- Upper Austria University of Applied Sciences, R&D** **Sep. 2010 – Jul. 2011**
Full-time research assistant
Development of an algorithm which detects abrupt changes in network entropy time series. The algorithm was tested with real and large-scale network flow data collected at an ISP.
Hagenberg, Austria
- Upper Austria University of Applied Sciences, R&D** **Oct. 2009 – Jul. 2010**
Research assistant
Design and development of an inductive network intrusion detection system for
Hagenberg, Austria

large-scale computer networks. The system makes use of one-class support vector machines to classify NetFlow records as benign or malicious.

Upper Austria University of Applied Sciences, R&D

Research assistant

Evaluation of suitable algorithms for anomaly detection in large-scale computer networks.

Sep. 2009
Hagenberg, Austria

underground_8

Summer intern

Development of iptables scripts which provide blocking capabilities for several instant messaging protocols such as AIM, ICQ and Microsoft Messenger.

Jul. 2008 – Sep. 2008
Linz, Austria

Siemens CERT

Industrial intern

Participated in the development of a virtualized system for the automated (static and dynamic) analysis of malicious executables (in PE-format) and documents.

Feb. 2008 – May 2008
Munich, Germany

underground_8

Summer intern

Design and development of a Linux networking daemon which runs in user space and parses the ICQ instant messaging protocol (e.g. to block file transfers).

Jun. 2007 – Jul. 2007
Linz, Austria

TEACHING EXPERIENCE

Topics in Computer Security

Teaching assistant

Apr. 2012 – May 2012
Karlstad, Sweden

Computer Security II

Teaching assistant

Nov. 2011 – Jan. 2012
Karlstad, Sweden

Introduction to Programming I

Teaching assistant

Oct. 2010 – Mar. 2011
Hagenberg, Austria

Object-oriented Programming II

Tutorial coordinator

Mar. 2009 – Jul. 2009
Hagenberg, Austria

SERVICES

Participation in the *Hagenberg Security Group*

Nov. 2008 – Jul. 2011

Participation and organization in the *h4ck!nb3rg* CTF team

Sep. 2008 – Jul. 2011

Secretary of the club *Hagenberger Kreis*

Nov. 2006 – Nov. 2007

Deputy chairman of the club *Hagenberger Kreis*

Nov. 2005 – Nov. 2006

Deputy secretary of the club *Hagenberger Kreis*

Nov. 2005 – Nov. 2006