

Curriculum Vitae

Dr. Robin Sommer

International Computer Science Institute	Lawrence Berkeley National Laboratory
Center for Internet Research	Computational Research Division
1947 Center St. Suite 600	1 Cyclotron Rd., 50B-2239
Berkeley, CA 94704 USA	Berkeley, CA 94720 USA
Phone (510) 666-2886	Phone (510) 486-7504
Fax (510) 666-2956	Fax (510) 486-6363

Email: robin@icsi.berkeley.edu
Web: <http://www.icir.org/robin>

Research Interests

Network Security, Traffic Monitoring, Intrusion Detection, Network Architectures

Education

TECHNICAL UNIVERSITY MÜNCHEN, GERMANY

Doctorate (Dr. rer. nat.) in Computer Science Sep 2005
Dissertation

Viable Network Intrusion Detection in High-Performance Environments

Advisor Prof. Anja Feldmann

Thesis Committee

Prof. Alfons Kemper, Prof. Anja Feldmann,

Prof. Manfred Broy, Prof. Vern Paxson

UNIVERSITY OF PADERBORN, GERMANY

Diploma in Computer Science ($\hat{=}$ M.Sc.) Aug 2001

Intermediate Diploma in Computer Science Sep 1998

Professional Experience

Research

Research Staff Scientist Oct 2006—today

International Computer Science Institute, Berkeley, CA

Affiliated Researcher Oct 2006—today

Lawrence Berkeley National Laboratory, Berkeley, CA

Visiting Researcher Nov/Dec 2007

Distributed Systems Group, RWTH Aachen, Germany

I3P Fellow Oct 2006—Sep 2007
 Lawrence Berkeley National Laboratory, Berkeley, CA
 Fellowship of the Institute for Information Infrastructure Protection

Post-doctoral fellowship Oct 2005—Sep 2006
 International Computer Science Institute, Berkeley, CA
 Fellowship of the German Academic Exchange Service (DAAD)

Research Assistant Aug 2002—Sep 2005
 Network Research Group, Technical University München, Germany

Research Assistant Sep 2001—Jul 2002
 Network Research Group, Saarland University, Saarbrücken, Germany

Internship Sep 2003—Nov 2003
 International Computer Science Institute, Berkeley, CA

Internship May 2002—Aug 2002
 International Computer Science Institute, Berkeley, CA

Teaching

Summer School Instructor
Summer School on Internet Security, La Villa, Italy
 Organized by the German National Academic Foundation Aug/Sep 2008

Guest Lecture
Hands-on Network Intrusion Detection, RWTH Aachen, Germany Dec 2007

Tutorial Instructor and Organizer
Bro Hands-On Workshop, San Diego Supercomputer Center Jul 2007
Bro Hands-On Workshop, Lawrence Berkeley National Laboratory Feb 2009

Teaching Assistant
 Lectures on Fundamentals of Computer Science 1–4 2002–2004
 Seminar Courses on Internet Security (4 courses) 2001–2004
 Seminar Course on Internet Routing 2004

Supervisor for diploma/master theses and term projects 2001—today

Professional Activities

Steering Committee Memeber
 Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA)

Program Committee Chair
 Detection of Intrusions & Malware, and Vulnerab. Assessment 2007

Program Committee Member
 Detection of Intrusions & Malw., and Vuln. Ass. 2005, 2006, 2008, & 2009
 Recent Advances in Intrusion Detection 2007, 2008, & 2009 (RAID)
 IEEE Workshop on Mission-Critical Networking 2008 (MCN)
 Critical Information Infrastructure Security 2007 (CRITIS)

Organizational Committee Member

ACM SIGCOMM 2003

External Reviewer

Including ACM CCR, ACM SIGCOMM, ACM TISSEC, ACM TOIT, IEEE S&P.

Memberships

Association for Computing Machinery (ACM)

Gesellschaft für Informatik (GI) (*German ACM equivalent*)

Other appointments

UNIX System Administrator

University of Paderborn, Germany

Apr 1998—Apr 2001

Languages

German, English (fluent)

References

On request.

Publications

Books

Robin Sommer

Viable Network Intrusion Detection: Trade-Offs in High-Performance Environments

VDM Verlag, ISBN 978-3-639-05529-0, 2008

Bernhard M. Hämmerli, Robin Sommer (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA)

Springer, Lecture Notes in Computer Science, ISBN 978-3-540-73613-4, 2007

Articles

Robin Sommer, Vern Paxson, Nicholas Weaver

An Architecture for Exploiting Multi-Core Processors to Parallelize Network Intrusion Prevention

Concurrency and Computation: Multi-core Supported Network & System Security, Wiley, 2009

Nicholas Weaver, Robin Sommer, Vern Paxson

Detecting Forged TCP Reset Packets

Proc. Network & Distributed System Security Symposium, 2009

Holger Dreger, Anja Feldmann, Vern Paxson, Robin Sommer

Predicting the Resource Consumption of Network Intrusion Detection Systems

Proc. Symposium on Recent Advances in Intrusion Detection, 2008

Gregor Maier, Robin Sommer, Holger Dreger, Anja Feldmann, Vern Paxson, Fabian Schneider

Enriching Network Security Analysis with Time Travel

Proc. ACM SIGCOMM, 2008

Mark Allman, Christian Kreibich, Vern Paxson, Robin Sommer, Nicholas Weaver
Principles for Developing Comprehensive Network Visibility
Proc. USENIX Workshop on Hot Topics in Security, 2008

Mark Allman, Christian Kreibich, Vern Paxson, Robin Sommer, Nicholas Weaver
The Strengths of Weaker Identities: Opportunistic Personas
Proc. USENIX Workshop on Hot Topics in Security, 2007

Nicholas Weaver, Robin Sommer
Stress Testing Cluster Bro
Proc. DETER Community Workshop on Cyber Security Experimentation and Test, 2007

Matthias Vallentin, Robin Sommer, Jason Lee, Craig Leres, Vern Paxson, Brian Tierney
The NIDS Cluster: Scalable, Stateful Network Intrusion Detection on Commodity Hardware
Proc. Symposium on Recent Advances in Intrusion Detection, 2007

Vern Paxson, Robin Sommer, Nicholas Weaver
An Architecture for Exploiting Multi-Core Processors to Parallelize Network Intrusion Prevention
Proc. IEEE Sarnoff Symposium, 2007

Ruoming Pang, Vern Paxson, Robin Sommer, Larry Peterson
binpac: A yacc for Writing Application Protocol Parsers
Proc. ACM SIGCOMM Internet Measurement Conference, 2006

Vern Paxson, Krste Asanovic, Sarang Dharmapurikar, John Lockwood, Ruoming Pang, Robin Sommer, Nicholas Weaver
Rethinking Hardware Support for Network Analysis and Intrusion Prevention
Proc. USENIX Workshop on Hot Topics in Security, 2006

Holger Dreger, Anja Feldmann, Michael Mai, Vern Paxson, Robin Sommer
Dynamic Application-Layer Protocol Analysis for Network Intrusion Detection
Proc. USENIX Security Symposium, 2006

Robin Sommer, Vern Paxson
Exploiting Independent State For Network Intrusion Detection
Proc. Annual Computer Security Applications Conference, 2005

Stefan Kornexl, Vern Paxson, Holger Dreger, Anja Feldmann, Robin Sommer
Building a Time Machine for Efficient Recording and Retrieval of High-Volume Network Traffic
Proc. ACM SIGCOMM Internet Measurement Conference, 2005

Holger Dreger, Christian Kreibich, Vern Paxson, Robin Sommer
Enhancing the Accuracy of Network-based Intrusion Detection with Host-based Context
Proc. GI Conference on Detection of Intrusions and Malware & Vulnerability Assessment , 2005

Christian Kreibich, Robin Sommer
Policy-controlled Event Management for Distributed Intrusion Detection
Proc. International Workshop on Distributed Event-Based Systems, 2005

Holger Dreger, Anja Feldmann, Vern Paxson, Robin Sommer
Operational Experiences with High-Volume Network Intrusion Detection
Proc. ACM Conference on Computer and Communications Security, 2004

Andy Rupp, Holger Dreger, Anja Feldmann, Robin Sommer
Packet Trace Manipulation Framework for Test Labs
Proc. ACM SIGCOMM Internet Measurement Conference, 2004

Robin Sommer
Bro: An Open Source Network Intrusion Detection System
Proc. DFN-Arbeitstagung über Kommunikationsnetze, 2003

Robin Sommer, Vern Paxson
Enhancing Byte-Level Network Intrusion Detection Signatures with Context
Proc. ACM Conference on Computer and Communications Security, 2003

Robin Sommer, Anja Feldmann
NetFlow: Information Loss or Win?
Proc. ACM SIGCOMM Internet Measurement Workshop, 2002

Theses

Robin Sommer
Viable Network Intrusion Detection in High-Performance Environments
TU München, 2005

Robin Sommer
Verfahren zum Clustering von Dokumenten
University of Paderborn, Germany, 2001

Invited Talks

Robin Sommer
Exploiting Multi-Core Processors For Parallelizing Network Intrusion Prevention
TRUST Seminar Series, UC Berkeley, 2009

Robin Sommer
A High-Performance NIDS Architecture for the Lawrence Berkeley National Lab
Network World IT Roadmap Conference, San Francisco, 2008

Robin Sommer
Monitoring Network Security with the Open-Source Bro NIDS
DOE Network Security Monitoring Technical Summit, Jefferson Lab, 2008

Robin Sommer
The Bro Network Intrusion Detection System
Guest Lecture, RWTH Aachen, Germany, 2007

Robin Sommer

High-Performance Network Security Monitoring at the Lawrence Berkeley National Lab
Internet2 Member Meeting, San Diego, 2007

Robin Sommer

Seeking Visibility Into Network Activity for Security Analysis
University of Adelaide, 2007

Robin Sommer

The Bro Network Intrusion Detection System
UC Computing Services Conference, UC Santa Cruz, 2007

Robin Sommer

Distributed Cooperative Security Monitoring
Consortium Meeting of the Institute for Information Infrastructure Protection, Carnegie Mellon University, 2007

Robin Sommer

Parallelizing Network Analysis
Deutsche Telekom Laboratories, Berlin, 2007