Curriculum Vitae

Christopher Kruegel

1 Personal Information

Name:	Christopher Ian Kruegel
Address (Work):	Department of Computer Science University of California, Santa Barbara Harold Frank Hall, 1117 Santa Barbara, CA 93106, USA
Telephone (Work):	+1 (805) 893-6198
Fax (Work):	+1 (805) 893-8553
Email:	chris@cs.ucsb.edu
Web:	http://www.cs.ucsb.edu/~chris/
Date-of-Birth:	17. January 1976
Nationality:	Austria

2 Education

09/2006

Habilitation from Technical University Vienna, Austria.

07/2000 - 06/2002

Dr.techn. (Ph.D.) in Computer Science (with highest distinction) from Technical University Vienna, Austria.
Advisor: Prof. Dr. Mehdi Jazayeri

09/1995 - 06/2000

Dipl.-Ing. (M.Sc.) in Computer Science (with highest distinction) from Technical University Vienna, Austria.
Advisor: Prof. Dr. Gerhard H. Schildt

3 Professional Appointments

Since 1/2008

Assistant Professor and **Eugene Aas Chair** in Computer Science at the Department of Computer Science, University of California at Santa Barbara, CA, USA.

01/2004 - 12/2007

Assistant Professor in Computer Science at the Automation Systems Group, Technical University Vienna, Austria.

10/2002 - 12/2003

Post-doctoral Researcher at the Reliable Software Group, University of California at Santa Barbara, CA, USA.

07/2000 - 09/2002

Research Assistant at the Distributed Systems Group, Technical University Vienna, Austria.

4 List of Publications

Books

[1] Christopher Kruegel, Fredrik Valeur and Giovanni Vigna. Intrusion Detection and Correlation: Challenges and Solutions. In *Advances in Information Security, Vol. 14, ISBN 0-387-23398-9, Springer Verlag*. November 2004.

[2] Gerhard-Helge Schildt, Daniela Kahn, Christopher Kruegel, and Christian Moerz. Einfuehrung in die Technische Informatik (Introduction to Technical Computer Science), German Language. Springers Lehrbuecher der Informatik (Textbooks on Computer Science), Springer Verlag, ISBN 3-211-24346-1. April 2005.

Journal Publications

[3] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Static Analysis for Detecting Taint-Style Vulnerabilities in Web Applications. In *Journal of Computer Security, IOS Press*; Accepted for publication, to appear 2008.

[4] Patrick Klinkoff, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. Extending .NET Security to Unmanaged Code. In *International Journal of Information Security, Volume 6, Number 6, Springer Computer Science Journal*, 2007.

[5] Ulrich Bayer, Andreas Moser, Christopher Kruegel, and Engin Kirda. Dynamic Analysis of Malicious Code. In *Journal in Computer Virology, Volume 2, Number 1, Springer Computer Science Journal*, 2006.

[6] Darren Mutz, Fredrik Valuer, Christopher Kruegel, and Giovanni Vigna. Anomalous System Call Detection. In *ACM Transactions on Information and System Security, Vol. 9, No. 1, ACM Press*, 2006.

[7] Engin Kirda and Christopher Kruegel. Protecting Users Against Phishing Attacks with AntiPhish. In *The Computer Journal, Volume 49, Number 5, Oxford University Press*, 2006.

[8] Christopher Kruegel, William Robertson, and Giovanni Vigna. A Multi-model Approach to the Detection of Web-based Attacks. In *Computer Networks Journal, Vol. 48, No. 5, Elsevier*, 2005.

[9] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Richard Kemmerer. A Comprehensive Approach to Intrusion Detection Alert Correlation. In *IEEE Transactions on Dependable and Secure Computing. Vol. 1, No. 3, IEEE Computer Society Press*, 2004.

[10] Christopher Kruegel, William Robertson, and Giovanni Vigna. Using Alert Verification to Identify Successful Intrusion Attempts. In *Praxis der Informationsverarbeitung und Kommunikation (PIK), Sauer Verlag*, 2004.

Conference Publications

[11] Guenther Starnberger, Christopher Kruegel, and Engin Kirda. Overbot - A botnet protocol based on Kademlia. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), IEEE Computer Society Press*, Turkey, September 2008.

[12] Eric Medvet, Engin Kirda, and Christopher Kruegel. Visual Similarity-Based Phishing Detection. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), IEEE Computer Society Press*, Turkey, September 2008.

[13] Sean McAllister, Christopher Kruegel, and Engin Kirda. Leveraging User Interactions for In-Depth Testing of Web Applications. In *11th International Symposium on Recent Advances in Intrusion Detection (RAID)*, USA, September 2008.

[14] Brett Stone-Gross, David Sigal, Rob Cohn, John Morse, Kevin Almeroth, and Christopher Kruegel. VeriKey: A Dynamic Certificate Verification System for Public Key Exchanges. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, France, July 2008.

[15] Davide Balzarotti, Marco Cova, Vika Felmetsger, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications. In *IEEE Symposium on Security and Privacy, IEEE Computer Society Press*, USA, May 2008.

[16] Gilbert Wondracek, Paulo Milani, Christopher Kruegel, and Engin Kirda. Automatic Network Protocol Analysis. In *Network and Distributed System Security Symposium (NDSS), Internet Society*, USA, February 2008.

[17] Andreas Moser, Christopher Kruegel, and Engin Kirda. Limits of Static Analysis for Malware Detection. In *23rd Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, December 2007.

[18] Davide Balzarotti, William Robertson, Christopher Kruegel, and Giovanni Vigna. Improving Signature Testing Through Dynamic Data Flow Analysis. In *23rd Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, December 2007.

[19] Martin Szydlowski, Christopher Kruegel, and Engin Kirda. Secure Input for Web Applications. In *23rd Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, December 2007.

[20] Heng Yin, Dawn Song, Manuel Egele, Christopher Kruegel, and Engin Kirda. Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis. In *14th ACM Conference on Computer and Communications Security (CCS), ACM Press*, USA, October 2007.

[21] Thomas Raffetseder, Christopher Kruegel, and Engin Kirda. Detecting System Emulators. In *10th Information Security Conference (ISC), Lecture Notes in Computer Science, Springer Verlag*, Chile, October 2007.

[22] Mihai Christodorescu, Somesh Jha, and Christopher Kruegel. Mining Specifications of Malicious Behavior. In *6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE), ACM Press*, Croatia, September 2007.

[23] Angelo Rosiello, Engin Kirda, Christopher Kruegel, and Fabrizio Ferrandi, A Layout-Similarity-Based Approach for Detecting Phishing Pages. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), IEEE Computer Society Press*, France, September 2007.

[24] Christian Ludl, Sean McAllister, Engin Kirda, and Christopher Kruegel. On the Effectiveness of Techniques to Detect Phishing Sites. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, Switzerland, July 2007.

[25] Manuel Egele, Christopher Kruegel, Engin Kirda, Heng Yin, and Dawn Song. Dynamic Spyware Analysis. In *Usenix Annual Technical Conference*, USA, June 2007.

[26] Andreas Moser, Christopher Kruegel, and Engin Kirda. Exploring Multiple Execution Paths for Malware Analysis. In *IEEE Symposium on Security and Privacy, IEEE Computer Society Press*, USA, May 2007.

[27] Philipp Vogt, Florian Nentwich, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna. Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. In *Network and Distributed System Security Symposium (NDSS), Internet Society*, USA, February 2007.

[28] Patrick Klinkoff, Christopher Kruegel, and Engin Kirda. Extending .NET Security to Unmanaged Code. In *Information Security Conference (ISC), Lecture Notes in Computer Science, Springer Verlag*, Greece, September 2006.

[29] Nenad Jovanovic, Engin Kirda, and Christopher Kruegel. Preventing Cross Site Request Forgery Attacks. In *IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm)*, USA, August 2006.

[30] Engin Kirda, Christopher Kruegel, Greg Banks, Giovanni Vigna, and Richard Kemmerer. Behavior-based Spyware Detection. In *15th Usenix Security Symposium*, Canada, August 2006.

[31] Manuel Egele, Martin Szydlowski, Engin Kirda, and Christopher Kruegel. Using Static Program Analysis to Aid Intrusion Detection. In *Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), Lecture Notes in Computer Science, Springer Verlag*, Germany, July 2006.

[32] Stefan Kals, Engin Kirda, and Christopher Kruegel. SecuBat: A Web Vulnerability Scanner. In *15th International World Wide Web Conference*, United Kingdom, May 2006.

[33] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper). In *IEEE Symposium on Security and Privacy, IEEE Computer Society Press*, USA, May 2006.

[34] Ulrich Bayer, Christopher Kruegel, and Engin Kirda. TTAnalyze: A Tool for Analyzing Malware. In *15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR)*, Germany, May 2006.

[35] Engin Kirda, Christopher Kruegel, Giovanni Vigna, and Nenad Jovanovic. Noxes: A Client-Side Solution for Mitigating Cross Site Scripting Attacks. In *21st ACM Symposium on Applied Computing (SAC), ACM Press*, France, April 2006.

[36] Fredrik Valeur, Giovanni Vigna, Christopher Kruegel, and Engin Kirda. An Anomaly-driven Reverse Proxy for Web Applications. In *21st ACM Symposium on Applied Computing (SAC), ACM Press*, France, April 2006.

[37] William Robertson, Giovanni Vigna, Christopher Kruegel and Richard Kemmerer. Using Generalization and Characterization Techniques in the Anomaly-based Detection of Web Attacks. In *Network and Distributed System Security Symposium (NDSS)*, Internet Society, USA, February 2006.

[38] Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Polymorphic Worm Detection Using Structural Information of Executables. In *8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, USA, September 2005.

[39] Christopher Kruegel, Engin Kirda, Darren Mutz, William Robertson, and Giovanni Vigna. Automating Mimicry Attacks Using Static Binary Analysis. In *14th Usenix Security Symposium*, USA, August 2005.

[40] Engin Kirda and Christopher Kruegel. Protecting Users Against Phishing Attacks with AntiPhish. In *29th Annual International Computer Software and Applications Conference (COMPSAC), IEEE Computer Society Press*, United Kingdom, July 2005.

[41] Darren Mutz, Christopher Kruegel, William Robertson, Giovanni Vigna, and Richard Kemmerer. Reverse Engineering of Network Signatures. In *Information Technology Security Conference (AusCERT)*, Australia, May 2005.

[42] Christopher Kruegel, William Robertson, and Giovanni Vigna. Detecting Kernel-Level Rootkits Through Binary Analysis. In *20th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, December 2004.

[43] Christopher Kruegel, William Robertson, Fredrik Valeur, and Giovanni Vigna. Static Analysis of Obfuscated Binaries. In *13th Usenix Security Symposium*, USA, August 2004.

[44] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur. Bayesian Event Classification for Intrusion Detection. In *19th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, December 2003.

[45] Christopher Kruegel and Giovanni Vigna. Anomaly Detection of Web-based Attacks. In *10th ACM Conference on Computer and Communications Security (CCS), ACM Press*, USA, October 2003.

[46] Engin Kirda, Clemens Kerer, Christopher Kruegel and Roman Kurmanowytsch. Web Service Engineering with DIWE. In *29th Euromicro, IEEE Computer Society Press*, Turkey, September 2003.

[47] William Robertson, Christopher Kruegel, Darren Mutz and Fredrik Valeur. Run-time Detection of Heap-based Overflows. In *17th Large Installation Systems Administration Conference (LISA), Usenix*, USA, October 2003.

[48] Christopher Kruegel, Darren Mutz, Fredrik Valeur and Giovanni Vigna. On the Detection of Anomalous System Call Arguments. In *8th European Symposium on Research in Computer Security (ESORICS), Lecture Notes in Computer Science, Springer Verlag*, Norway, October 2003.

[49] Christopher Kruegel, Darren Mutz, William Robertson and Fredrik Valeur. Topology-based Detection of Anomalous BGP Messages. In 6th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag, USA, September 2003.

[50] Christopher Kruegel and Thomas Toth. Using Decision Trees to Improve Signature-based Intrusion Detection. In *6th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag*, USA, September 2003.

[51] Thomas Toth and Christopher Kruegel. Evaluating the Impact of Automated Intrusion Response Mechanisms. In *18th Annual Computer Security Applications Conference (ACSAC), IEEE Computer Society Press*, USA, November 2002.

[52] Thomas Toth and Christopher Kruegel. Accurate Buffer Overflow Detection via Abstract Payload Execution. In *5th Symposium on Recent Advances in Intrusion Detection (RAID), Lecture Notes in Computer Science, Springer Verlag*, Switzerland, October 2002.

[53] Pascal Fenkam, Harald Gall, Mehdi Jazayeri and Christopher Kruegel. DPS - An Architectural Style for Development of Secure Software. In *Infrastructure Security Conference (InfraSec), Lecture Notes in Computer Science, Springer Verlag*, United Kingdom, October 2002.

[54] Christopher Kruegel, Fredrik Valeur, Giovanni Vigna and Richard Kemmerer. Stateful Intrusion Detection for High-Speed Networks. In *IEEE Symposium on Security and Privacy, IEEE Computer Society Press*, USA, May 2002.

[55] Christopher Kruegel, Thomas Toth and Engin Kirda. Service Specific Anomaly Detection for Network Intrusion Detection. In *ACM Symposium on Applied Computing (SAC), ACM Press*, Spain, March 2002.

[56] Christopher Kruegel and Thomas Toth. Distributed Pattern Detection for Intrusion Detection. In *Network and Distributed System Security Symposium (NDSS), Internet Society*, USA, February 2002.

[57] Christopher Kruegel and Thomas Toth. Flexible, Mobile Agent based Intrusion Detection for Dynamic Networks. In *European Wireless*, Italy, February 2002.

[58] Christopher Kruegel, Thomas Toth and Clemens Kerer. Decentralized Event Correlation for Intrusion Detection. In *International Conference on Information Security and Cryptology (ICISC), Lecture Notes in Computer Science, Springer Verlag*, Korea, December 2001.

[59] Christopher Kruegel and Thomas Toth. Sparta - A Mobile Agent based Intrusion Detection System. In *IFIP Conference on Network Security (I-NetSec), Kluwer Academic Publishers*, Belgium, November 2001.

[60] Christopher Kruegel and Thomas Toth. An efficient, IP based solution to the 'Logical Timestamp Wrapping' problem. In *6th International Conference on Telecommunications (ConTEL)*, Croatia, June 2001.

[61] Wolfgang Kastner and Christopher Kruegel. Improved fieldbus control via middleware technology. In *4th Conference on Automatic Control (Controlo)*, Portugal, October 2000.

[62] Wolfgang Kastner and Christopher Kruegel. Jini connectivity for EIB home and building networks - from design to implementation. In *EIB Scientific Conference*, Germany, October 1999.

[63] Wolfgang Kastner, Christopher Kruegel and Heinrich Reiter. Jini: Ein guter Geist fuer die Gebaeudesystemtechnik (german). In *Java Informations Tage (JIT)*, Germany, September 1999.

Workshop Publications

[64] Marco Cova, Christopher Kruegel, and Giovanni Vigna. There Is No Free Phish: An Analysis of "Free" and Live Phishing Kits. In *Usenix Workshop on Offensive Technologies (WOOT)*, USA, July 2008.

[65] Christoph Karlberger, Guenter Bayler, Christopher Kruegel, and Engin Kirda. Exploiting Redundancy in Natural Language to Penetrate Bayesian Spam Filters. In *Usenix Workshop on Offensive Technologies (WOOT)*, USA, August 2007.

[66] Thomas Raffetseder, Engin Kirda, and Christopher Kruegel. Building Anti-Phishing Browser Plug-Ins: An Experience Report. In *ICSE Workshop on Software Engineering for Secure Systems (SESS), IEEE Computer Society Press*, USA, May 2007.

[67] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda. Precise Alias Analysis for Static Detection of Web Application Vulnerabilities. In *ACM Workshop on Programming Languages and Analysis for Security (PLAS), ACM Press*, Canada, June 2006.

[68] Christopher Kruegel and William Robertson. Alert Verification - Determining the Success of Intrusion Attempts. In *Workshop on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA), Lecture Notes in Informatics (LNI)*, Germany, July 2004.

[69] Thomas Toth and Christopher Kruegel. Connection-history based anomaly detection. In *3rd IEEE Information Assurance Workshop, IEEE Computer Society Press*, USA, June 2002.

[70] Engin Kirda, Clemens Kerer and Christopher Kruegel. XGuide - A Practical Guide to XML-based Web Engineering. In *International Workshop on Web Engineering, Lecture Notes in Computer Science, Springer Verlag*, Italy, May 2002.

[71] Engin Kirda, Clemens Kerer, Mehdi Jazayeri and Christopher Kruegel. Supporting multi-device enabled services: Challenges and open problems. In *10th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, IEEE Computer Society Press*, USA, June 2001.

[72] Christopher Kruegel and Thomas Toth. Applying Mobile Agent Technology to Intrusion Detection. In *ICSE Workshop on Software Engineering and Mobility*, Canada, May 2001.

[73] Wolfgang Kastner and Christopher Kruegel. A new approach for Java in embedded networks. In *3rd IEEE Workshop on Factory Communication Systems, IEEE Computer Society Press*, Portugal, September 2000.

Book Chapters

[74] Christopher Kruegel. Characterizing the Behavior and Structure of Malicious Executables. In *Advances in Information Security, Vol. 27, ISBN 0-387-32720-7, Springer Verlag*, December 2006.

[75] Giovanni Vigna and Christopher Kruegel. Host-Based Intrusion Detection. In *Handbook of Information Security, John Wiley and Sons, ISBN 0-471-64833-7.* December 2005.

[76] Christopher Kruegel. Internet Security. In *The Industrial Communication Technology Handbook, CRC Press, ISBN 0-8493-3077-7.* February 2005.

[77] Christopher Kruegel. Network Security and Secure Applications. In *The Industrial Information Technology Handbook, ISBN 0-849-31985-4, CRC Press.* May 2004.

Edited Volumes

[78] Georg Carle, Falko Dressler, Richard Kemmerer, Hartmut Koenig, and Christopher Kruegel. Perspectives Workshop: Network Attack Detection and Defense *Dagstuhl Seminar Proceedings 08102, ISSN: 1862 - 4405.* March 2008.

[79] Christopher Kruegel. Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM). *ACM Special Interest Group on Security, Audit, and Control (SIGSAC), ISBN 978-1-59593-886-2.* December 2007.

[80] Christopher Kruegel, Richard Lippmann, and Andrew Clark. Proceedings of the 10th International Symposium on Recent Advances in Intrusion Detection. *Lecture Notes in Computer Science (LNCS), Vol. 4637, Springer Verlag, ISBN 978-3-540-74319-4.* September 2007.

[81] Diego Zamboni and Christopher Kruegel. Proceedings of the 9th International Symposium on Recent Advances in Intrusion Detection. *Lecture Notes in Computer Science (LNCS), Vol. 4219, Springer Verlag, ISBN 3-540-39723-X.* September 2006.

[82] Klaus Julisch and Christopher Kruegel. Proceedings of the 2nd International Conference on Intrusion and Malware Detection and Vulnerability Assessment. *Lecture Notes in Computer Science (LNCS), Vol. 3548, Springer Verlag, ISBN 3-540-26613-5.* July 2005.

[83] Giovanni Vigna, Erland Jonsson and Christopher Kruegel. Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection. *Lecture Notes in Computer Science (LNCS), Vol. 2820, Springer Verlag, ISBN 3-540-40878-9.* September 2003.

Theses

[84] Christopher Kruegel. Malicious Code Analysis. Habilitation Thesis, Technical University Vienna, 2006.

[85] Christopher Kruegel. Network Alertness - Towards an adaptive, collaborating Intrusion Detection System. PhD Thesis, Technical University Vienna, 2002.

[86] Christopher Kruegel. Jini connectivity for home and building automation - a case study for EIB. Technical University Vienna, 2000

5 Professional Activities

Journal Editorial Board

1. Associate Editor, International Journal of Information Security, Springer Verlag.

Conference/Program Chair

1. 5th ACM Workshop on Recurring Malcode (WORM), 2007
2. 10th International Symposium on Recent Advances in Intrusion Detection (RAID), 2007
3. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2005

Program Committee Memberships

1. 16th Network and Distributed System Security Symposium (NDSS), 2009
2. International Conference on Information Security and Cryptology (ICISC), 2008
3. ACM Conference on Computer and Communications Security (CCS), 2008
4. European Conference on Computer Network Defense (EC2ND), 2008
5. 13th European Symposium on Research in Computer Security (ESORICS), 2008
6. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2008
7. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2008
8. Trust Conference (TRUST), 2008
9. IEEE Symposium on Security and Privacy, 2008
10. Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET), 2008
11. 17th International World Wide Web Conference (WWW), Security, Privacy, Reliability, and Ethics Track, 2008
12. European Workshop on Systems Security (EuroSec), 2008
13. 15th Network and Distributed System Security Symposium (NDSS), 2008
14. International Conference on Information Security and Cryptography (ICISC), 2007
15. ACM Conference on Computer and Communications Security (CCS), 2007
16. European Conference on Computer Network Defense (EC2ND), 2007
17. 12th European Symposium on Research in Computer Security (ESORICS), 2007
18. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2007
19. International Conference on Security and Cryptography (SECRYPT), 2007
20. Mathematical Methods, Models and Architectures for Computer Networks Security (MMM-ACNS), 2007
21. 16th Usenix Security Symposium, 2007
22. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2007
23. International Conference on Networking and Services (ICNS), 2007
24. IEEE Symposium on Security and Privacy, 2007
25. 16th International World Wide Web Conference (WWW), Security, Privacy, Reliability, and Ethics Track, 2007
26. 2nd Workshop on Dependability Aspects on Data WArehousing and Mining applications (DAWAM), 2007

27. Workshop on Secure Software Engineering (SecSE), 2007
28. 8th International Conference on Information and Communications Security (ICICS), 2006
29. International Conference on Software Engineering Advances (ICSEA), 2006
30. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2006
31. International Conference on Information System Security (ICISS), 2006
32. International Conference on Security and Cryptography (SECRYPT), 2006
33. 9th International Symposium on Recent Advances in Intrusion Detection (RAID), 2006
34. International Conference on Networking and Services (ICNS), 2006
35. ICSE Workshop on Software Engineering for Secure Systems (SESS), 2006
36. Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2006
37. IEEE Symposium on Security and Privacy, 2006
38. International Conference on IP and Web Applications (ICIW), 2006
39. IEEE International Conference on Security and Privacy for Emerging Areas in Communication Networks (Securecomm), 2005
40. International Conference on Information System Security (ICISS), 2005
41. 3rd ACM CCS Workshop on Rapid Malcode (WORM), 2005
42. 8th International Symposium on Recent Advances in Intrusion Detection (RAID), 2005
43. International Conference on Networking and Services (ICNS), 2005
44. ICSE Workshop on Software Engineering for Secure Systems (SESS), 2005
45. 12th Network and Distributed System Security Symposium (NDSS), 2005
46. Workshop on Privacy Respecting Incident Management (PRIMA), 2005
47. Workshop on Safety, Reliability, and Security of Industrial Computer Systems (WSRS), 2004
48. 7th International Symposium on Recent Advances in Intrusion Detection (RAID), 2004
49. Workshop on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA), 2004
50. 6th International Symposium on Recent Advances in Intrusion Detection (RAID), 2003
51. 8th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2001

Journal Reviewer

ACM Transactions on Information and System Security (TISSEC), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Knowledge and Data Engineering, IEEE Transactions on Computers, IEEE Transactions on Fuzzy Systems, IEEE Security and Privacy Magazine, IEEE Internet Computing, IEEE Signal Processing Letters, IEEE Journal on Selected Areas in Communications, International Journal of Computers and Applications, International Journal of Information Security, International Journal of Innovative Computing, Information, and Control, International Journal of Internet Protocol Technology, Journal of Communications and Networks, Journal of Computer Networks, Journal of Computer Science and Technology, Journal of Computer Security, Journal of Machine Learning, Journal of Pattern Analysis and Applications, Journal of Systems and Software, AI Communications, Computer Journal, Software Experience and Practice.

6 Teaching

1. **Operating Systems**
   25 undergraduate students; Winter 2008; *University of California, Santa Barbara*

   The focus of the class is on the design and implementation issues associated with operating systems. The lectures introduce the basic principles of operating system design. This includes process management, virtual memory management, file systems, and input/output handling. The accompanying lab requires students to make modifications to the Minix operating system.

   I was the principal instructor for this course. In particular, I was responsible for teaching lectures and for managing the practical lab exercises. While previous classes used Nachos for the practical part, I designed and introduced a completely new set of lab exercises that are built upon Minix. On a scale from 1 (best) to 5 (worst), the students rated the class with 1.3 (the department average is 2.2) and the teacher's performance with 1.2 (the average is 2.0).

2. **Internet Security**
   200 bachelor students; 2001, 2005-2008; *Technical University Vienna*

   This course provides an introduction to computer security, with an emphasis on security related to distributed systems and the Internet. The focus is on principal network protocols (e.g., TCP/IP) and applications (e.g., web, mail, domain name service) that are used on the Internet today. The course also includes a number of practical lab assignments where participants are required to apply their knowledge.

   I was the principal instructor for this course. In particular, I was responsible for teaching lectures as well as for developing and managing the practical lab exercises. I redesigned the curriculum and introduced a new set of practical lab exercises. Since 2006, this class was included into the official student evaluation process. On a scale from 1 (best) to 5 (worst), the overall rating was 1.15 in 2006 and 1.33 in 2007. The department average is 2.0.

3. **Advanced Internet Security**
   50 master students; 2004-2007; *Technical University Vienna*

   This course serves as a continuation of Internet Security. The idea is to explore important areas of computer security such as operating systems security, malicious code, or reverse engineering, which are only touched in the introductory class. As part of the class, students participate in an international security (capture-the-flag) exercise in which they can prove their knowledge of security and system management by competing with peers from other universities.

   I proposed this lecture and introduced it into the computer science curriculum of the Technical University Vienna. For this class, I was the principal instructor and designed the lecture material as well as the practical lab exercises. Unfortunately, there are no official evaluation results available, because the class size is too small.

4. **Einfuehrung in die Technische Informatik (Introduction to Computer Science)**
   600 freshman students; 2004-2007; *Technical University Vienna*

   This course teaches basic aspects of technical computer science. It starts with an introduction to principles of electrical engineering and digital circuits. Starting from simple gates, more complex circuits are introduced until a complete microprocessor is built. Based on this processor, the concepts of operating systems (processes and virtual memory) are studied.

I was supporting faculty for this course. My responsibilities included teaching some lectures and overseeing the practical lab exercises. Since I was not the principal instructor for this class, my performance was not evaluated.

7 Graduated Master and PhD Students (Advisor and Committee Member)

1. Nenad Jovanovic. Web Application Security. Ph.D. Advisor, Technical University Vienna. 2007.
2. Yohann Thomas. Policy-based responses to intrusions through context activation. Ph.D. Committee Member, Universite de l'ENST Bretagne, France. 2007.
3. Andre Arnes. Risk and Security Incident Management. Ph.D. Committee Member, Norwegian University of Science and Technology, Norway. 2006.
4. Davide Balzarotti. Testing Network Intrusion Detection Systems. Ph.D. Committee Member, Politecnico di Milano, Italy. 2006.
5. Sean McAllister. Increasing the Coverage of Web Application Vulnerability Scanners. M.Sc. Advisor, Technical University Vienna. 2008.
6. Clemens Kolbitsch. Extending Mondrian Memory Protection. M.Sc. Advisor, Technical University Vienna. 2008.
7. Andreas Stamminger. Automated Spyware Collection and Analysis. M.Sc. Advisor, Technical University Vienna. 2007.
8. Florian Nentwich. Sicherheitsanalyse von Signatursoftware. M.Sc. Advisor, Technical University Vienna. 2007.
9. Guenther Bayler. Penetrating Bayesian Spam Filters Using Redundancy in Natural Language. M.Sc. Advisor, Technical University Vienna. 2007.
10. Martin Szydlowski. Secure Input for Web Applications. M.Sc. Advisor, Technical University Vienna. 2007.
11. Helmut Petritsch. Understanding and Replaying Network Traffic in Windows XP for Malware Analysis. M.Sc. Advisor, Technical University Vienna. 2007.
12. Manuel Egele. Dynamic Spyware Analysis. M.Sc. Advisor, Technical University Vienna. 2006.
13. David Tischler. WSFW: An Open Source Web Service Firewall. M.Sc. Advisor, Technical University Vienna. 2006.
14. Philipp Vogt. Cross-Site Scripting (XSS) Attack Prevention with Dynamic Data Tainting on the Client Side. M.Sc. Advisor, Technical University Vienna. 2006.
15. Stefan Kals, SecuBat: A Web Vulnerability Scanner. M.Sc. Advisor, Technical University Vienna. 2006.
16. Ulrich Bayer. TTAnalyze - A Tool for Analyzing Malware. M.Sc. Advisor, Technical University Vienna. 2005.
17. Patrick Klinkoff. Extending .NET Code Security to Native Code. M.Sc. Advisor, Technical University Vienna. 2005.

18. Thomas Aichinger, Erstellung von Sicherheitsvorgaben fuer einen Secure Viewer und dessen Evaluierung nach Common Criteria (German Language). M.Sc. Advisor, Technical University Vienna. 2003.

8 Current PhD Students

1. Ulrich Bayer, Start Date: 01/2007
2. Manuel Egele, Start Date: 10/2007
3. Christoph Karlberger, Start Date: 07/2007
4. Clemens Kolbitsch, Start Date: 03/2008
5. Andreas Moser, Start Date: 11/2005
6. Martin Szydlowski, Start Date: 10/2007
7. Gilbert Wondracek, Start Date: 10/2006
8. Peter Wurzinger, Start Date: 06/2007

9 Research Grants and Projects

1. **WOMBAT:** Worldwide Observatory of Malicious Behaviors and Attack Threats
   2008 - 2010; *funded by the European Union - 7th Framework Programme*; 379,500 Euro

2. **SECoverer: Finding Security Vulnerabilities in Web Applications**
   2008 - 2010; *funded by the Austrian Research, Innovation, Information Technology Program (FIT-IT)*; 199,080 Euro

3. **FORWARD: Managing Emerging Threats in ICT Infrastructures**
   2008 - 2009; *funded by the European Union - 7th Framework Programme*; 253,911 Euro

4. **Pathfinder: Malicious Code Analysis and Detection**
   2006 - 2009; *funded funded by the Austrian Research, Innovation, Information Technology Program (FIT-IT)*; 217,800 Euro

5. **Web-Defense**: Client-side Protection against Web Attacks
   2006 - 2009; *funded by the Austrian Science Foundation (FWF);* 230,853 Euro

6. **Software Security through Binary Analysis**
   2005 - 2008; *funded by the Austrian Science Foundation (FWF)*; 126,504 Euro

7. **Omnis** - An Open Framework for Pervasive Services
   2005 - 2007; *funded by the Austrian Science Foundation (FWF)*; 123,354 Euro

8. **Solaris and Linux Baseline Security**
   2005; *funded by the Austrian National Bank (OeNB)*; 13,000 Euro

10 Awards

2007

Best Paper Award of the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE) for the paper "Mining Specifications of Malicious Behavior."

2007

Best Student Paper Award of the 10th Information Security Conference (ISC) for the paper "Detecting System Emulators."

2006

Best Paper Award of the 15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR) for the paper "TTAnalyze: A Tool for Analyzing Malware."

2005

Best Paper Award of the Information Technology Security Conference (AusCERT) for the paper "Reverse Engineering of Network Signatures."

2005

Award of the Austrian Federal Economic Chamber (Wirtschaftskammerpreis) for the project "Malware Detection." This project aims to develop novel techniques for the identification of malicious code based on binary analysis.

2000

EIB Scientific Award for an excelling student project in the field of Home and Building Electronic Systems based on the European Installation Bus EIB (for the Master Thesis).

11 Talks (Invited Talks and Conference Presentations)

1. Saner: Composing Static and Dynamic Analysis to Validate Sanitization in Web Applications. Paper presentation at the IEEE Symposium on Security and Privacy. USA, May 2008.

2. Malicious Code Analysis. Invited Talk at the Computer Science Colloquium, Indiana University, Bloomington. USA, March 2008.

3. Still doing IDS research ... after all these years. Presentation at Schloss Dagstuhl: Perspectives Workshop: Network Attack Detection and Defense. Germany, March 2008.

4. Dynamic Malware Analysis. Invited Talk at Seminaire Diwall, Ecole superieure d'electricite (Supelec). France, November 2007.

5. Dynamic Malware Analysis. Invited Talk at the CS Colloquium, KAIST. Korea, September 2007.

6. Malicious Code Analysis. Invited Talk at the RNSA Workshop - Network Monitoring: Identifying and Measuring the Threat. Australia, September 2007.

7. Malicious Code Analysis. Invited Talk at the Computer Science Colloquium, UC Santa Barbara, USA, April 2007.

8. Malicious Code Analysis. Invited Talk at the Computer Science Colloquium, Georgia Institute of Technology. USA, March 2007.

9. Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis. Paper presentation at the Network and Distributed System Security Symposium (NDSS). USA, February 2007.

10. Malicious Code Analysis. Invited Talk at the Computer Science Colloquium, Carleton University, Ottawa. Canada, October 2006.

11. Malicious Code Analysis. Talk at the Habilitation Colloquium, Technical University Vienna. Austria, September 2006.

12. Finding Vulnerabilities in Web Applications. Invited Talk at the TERENA Networking Conference. Italy, May 2006.

13. TTAnalyze: A Tool for Analyzing Malware. Paper presentation at the 15th Annual Conference of the European Institute for Computer Antivirus Research (EICAR). Germany, May 2006.

14. Analyzing and Detecting Malicious Code. Invited talk at the Computer Science Colloquium, University of Mannheim. Germany, December 2005.

15. Malicious Code Analysis: Detecting Metamorphic Worms. Invited talk at the Computer Science Colloquium, Masaryk University. Czech Republic, November 2005.

16. Malicious Code Analysis: Detecting Metamorphic Worms. Invited Talk at the Computer Science Colloquium, Technical University Berlin, Germany. November 2005.

17. Advanced Techniques for Malicious Code Detection. Invited talk at the NATO ASI Workshop. Armenia, October 2005.

18. Polymorphic Worm Detection Using Structural Information of Executables. Paper presentation at the 8th International Symposium on Recent Advances in Intrusion Detection (RAID). USA, September 2005.

19. Characterizing the Behavior and Structure of Malicious Executables. Invited talk at the Special Workshop on Malware Detection. USA, August 2005.

20. Automating Mimicry Attacks Using Static Binary Analysis. Paper presentation at the 14th Usenix Security Symposium. USA, August 2005.

21. Identification of Anomalous System Calls for Intrusion Detection. Invited talk at the Computer Science Colloquium, University of Dortmund. Germany, April 2005.

22. Intrusion Detection and Correlation. Invited talk at the FH Hagenberg. Austria, March 2005.

23. Identification of Anomalous System Calls for Intrusion Detection. Invited talk at the Computer Science Colloquium, TU Munich. Germany, December 2004.

24. Static Analysis of Obfuscated Binaries. Paper presentation at the 13th Usenix Security Symposium. USA, August 2004.

25. Determining the Success of Intrusion Attempts. Paper presentation at the Workshop on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA). Germany, July 2004.

26. Bayesian Event Classification for Intrusion Detection. Paper presentation at the 19th Annual Computer Security Applications Conference (ACSAC). USA, December 2003.

27. Topology-based Detection of Anomalous BGP Messages. Invited Lecture at the Carnegie Mellon University (CMU). USA, September 2003.

28. Using Decision Trees to Improve Signature-based Intrusion Detection. Paper presentation at the 6th Symposium on Recent Advances in Intrusion Detection (RAID). USA, September 2003.

29. Using Decision Trees to Improve Signature-based Intrusion Detection. Research talk at the DoD University Research Initiative (MURI) Meeting. USA, August 2003.

30. Service Specific Anomaly Detection for Network Intrusion Detection. Paper presentation at the Symposium on Applied Computing (SAC). Spain, March 2002.

31. Distributed Pattern Detection for Intrusion Detection. Paper presentation at the Network and Distributed System Security Symposium (NDSS). USA, February 2002.

32. Decentralized Event Correlation for Intrusion Detection. Paper presentation at the International Conference on Information Security and Cryptology (ICISC). Korea, December 2001.

33. An efficient, IP based solution to the 'Logical Timestamp Wrapping' problem. Paper presentation at the 6th International Conference on Telecommunications (ConTEL). Croatia, June 2001.

34. Applying Mobile Agent Technology to Intrusion Detection. Paper presentation at the ICSE Workshop on Software Engineering and Mobility. Canada, May 2001.

35. Jini connectivity for EIB home and building networks - from design to implementation. Paper presentation at the EIB Scientific Conference. Germany, October 1999.

36. Jini Connectivity for EIB Home and Building Networks. Invited talk at the Jini Users Meeting, ETH Zurich. Switzerland, November 1999.