Fredrik Valeur

Computer Science
Harold Frank Hall
Santa Barbara, CA 93106

fredrik@cs.ucsb.edu

EDUCATION

◇ **Ph.D. in Computer Science**, University of California Santa Barabara **June 2006**
Dissertation title: "Real-Time Intrusion Detection Alert Correlation"

◇ **Siv.Ing in telematics**, Norwegian University of Science and Technology, **March 2001**
Thesis title: "NTL: A Network Tool Language for Automatic Integration and Composition of Network Discovery Tools"

RESEARCH INTERESTS

Computer Security, Network Security, Intrusion Detection, Intrusion Detection Alert Correlation, Penetration Testing, Vulnerability Analysis

WORK EXPERIENCE

◇ **Post.Doc. Researcher**, University of California Santa Barabara **2006–2007**

· Performed research in network security and intrusion detection.

· Designed a web application firewall (WaF)

◇ **Graduate Research Assistant**, University of California Santa Barabara **2001–2006**

· Performed research in network security and intrusion detection.

· Designed and implemented an intrusion detection alert correlation system.

PUBLICATIONS

A. AArnes, F. Valeur, G. Vigna, and R.A. Kemmerer. Using Hidden Markov Models to Evaluate the Risk of Intrusions. In *Proceedings of the* 9^{th} *Symposium on Recent Advances in Intrusion Detection (RAID)*, Hamburg, Germany, September 2006. Springer Verlag.

C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Topology-based Detection of Anomalous BGP Messages. In *Proceedings of the* 6^{th} *Symposium on Recent Advances in Intrusion Detection (RAID)*, Pittsburgh, PA, September 2003. Springer Verlag.

C. Kruegel, D. Mutz, W.K. Robertson, and F. Valeur. Bayesian Event Classification for Intrusion Detection. In *Proceedings of ACSAC 2003*, Las Vegas, NV, December 2003.

C. Kruegel, D. Mutz, F. Valeur, and G. Vigna. On the Detection of Anomalous System Call Arguments. In *Proceedings of the* 8^{th} *European Symposium on Research in Computer Security (ESORICS '03)*, LNCS, pages 326–343, Gjøvik, Norway, October 2003. Springer-Verlag.

C. Kruegel, W. Robertson, F. Valeur, and G. Vigna. Static Disassembly of Obfuscated Binaries. In *Proceedings of the* 13^{th} *Usenix Security Symposium*, San Diego, CA, August 2004.

C. Kruegel, F. Valeur, and G. Vigna. *Intrusion Detection and Correlation: Challenges and Solutions*, volume 14 of *Advances in Information Security*. Springer, 2005.

C. Kruegel, Fredrik Valeur, G. Vigna, and R.A. Kemmerer. Stateful Intrusion Detection for High-Speed Networks. In *Proceedings of the IEEE Symposium on Research on Security and Privacy*, Oakland, CA, May 2002. IEEE Press.

D. Mutz, F. Valeur, C. Kruegel, and G. Vigna. Anomalous System Call Detection. *ACM Transactions on Information and System Security*, 2006.

W. Robertson, C. Kruegel, D. Mutz, and F. Valeur. Run-time Detection of Heap-based Overflows. In *Proceedings of the* 17^{th} *Large Installation Systems Administration Conference (LISA)*, San Diego, CA, October 2003. Usenix.

F. Valeur, D. Mutz, and G. Vigna. A Learning-Based Approach to the Detection of SQL Attacks. In *Proceedings of DIMVA 2005*, Vienna, Austria, July 2005.

F. Valeur, G. Vigna, C.Kruegel, and R. Kemmerer. A Comprehensive Approach to Intrusion Detection Alert Correlation. *IEEE Transactions on Dependable and Secure Computing*, 1(3):146–169, July-September 2004.

F. Valeur, G. Vigna, C. Kruegel, and E. Kirda. An Anomaly-driven Reverse Proxy for Web Applications. In *The 21st ACM Symposium on Applied Computing (SAC 2006), Security Track*, Dijon, France, April 2006.

G. Vigna, F. Valeur, and R.A. Kemmerer. Designing and Implementing a Family of Intrusion Detection Systems. In *Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of Software Engineering (ESEC/FSE 2003)*, Helsinki, Finland, September 2003.

G. Vigna, F. Valeur, J. Zhou, and R.A. Kemmerer. Composable Tools For Network Discovery and Security Analysis. In *Proceedings of the* 18^{th} *Annual Computer Security Applications Conference (ACSAC '02)*, pages 14–24, Las Vegas, NV, December 2002. IEEE Press.