

# Adam J. Slagell, CISO

---

## CONTACT INFORMATION

Adam J. Slagell  
2321 Phinney Dr  
Champaign, IL 61821, USA

Mobile: (217) 390-3837  
E-mail: adam@slagell.info  
WWW: www.slagell.info

## ACTIVITIES & RESEARCH INTERESTS

Security Architecture  
Security Assessment & Analysis  
Education & Outreach  
R&D Team Leadership  
Project Management  
Community Building

Data Sanitization & Anonymization  
Intrusion Detection  
Security Visualization  
Applied Cryptography  
Honeynets  
Collaborative Security

## EDUCATION & CERTIFICATIONS

**International Information System Security Certification Consortium (ISC)<sup>2</sup>**

Certified Information Systems Security Professional (CISSP), 2009 (No: 355514)

**University of Illinois at Urbana-Champaign, Illinois, USA**

Master of Science, Department of Computer Science, 2003 (GPA: **4.0/4.0**)

- Thesis: *A Simple, Portable and Expandable Cryptographic Application Programming Interface*
- Advisor: Dr. Klara Nahrstedt

**Northern Illinois University, Illinois, USA**

Master of Science, Department of Mathematics, 2000 (GPA: **4.0/4.0**)

Bachelor of Science, Department of Mathematics, 1999 (GPA: **4.0/4.0**)

## RESEARCH GRANTS

- National Science Foundation (NSF) Research Grant, 1032889, **Co-Principal Investigator**, \$3M, 2010–2013.
- National Science Foundation (NSF) Research Grant, GENI award through BBN, **Principal Investigator**, \$227K, 2009–2012.
- National Science Foundation (NSF) Research Grant, 0524643, **Principal Investigator**, \$400K, 2005–2008.
- Office of Naval Research (ONR) Research Grant through the National Center for Advanced Secure Systems Research (NCASSR), DAT, **Principal Investigator**, \$220K, 2006–2007.
- Office of Naval Research (ONR) Research Grant through the National Center for Advanced Secure Systems Research (NCASSR), SLAGEL, **Principal Investigator**, \$156K, 2005.
- Office of Naval Research (ONR) Research Grant through the National Center for Advanced Secure Systems Research (NCASSR), SIFT, **Senior Personnel**, \$500K, 2004–2006.

## ACADEMIC EXPERIENCE

*Chief Information Security Officer & Senior Security Engineer*

**Jun. 2003—**

National Center for Supercomputing Applications

University of Illinois at Urbana-Champaign, Illinois, USA

- **Principal Investigator** for (1) NSF GENI award to develop operational security program and agreements; (2) NSF Cyber Trust log anonymization project (CNS-0524643); (3) NCASSR (ONR funded center) Palantir: Data Analytics and Tools project; and (4) NCASSR System Log Anonymization for Greater Exchange of Logs (SLAGEL) project
- **Co-Principal Investigator** and sub-award PI for NSF SDCI project, Enhancing Bro for Operational Network Security Monitoring in Scientific Environments (CNS-1032889)
- **Project Manager** for NCASSR Security Incidents Fusion Tools (SIFT) project and Cyber Integrator Shell Tool development
- **Project Team Lead** and Security Architect for the Blue Waters petascale supercomputer
- **Sr. Researcher** for the National Center for Digital Intrusion Response and Cyber-investigation Law Enforcement Wizard project

- **Research Staff** on NCASSR Mithril project, Secure Email List Service (SELS) project, Secure Group Communication protocol development, and PKI/CKM scalability study

*Teaching Assistant*

**Aug. 2000–Aug. 2001**

Department of Computer Science

University of Illinois at Urbana-Champaign, Illinois, USA

- (1) Conducted classes, (2) created exams, quizzes and assignments, (3) managed course news-group, and (4) held office hours

*Teaching Assistant and Tutor*

**Jan. 1997–Aug. 2000**

Department of Mathematics and College of Engineering

Northern Illinois University, Illinois, USA

- Teaching assistant for math 101 and finite math
- Official tutor for College of Engineering for calculus I–III and differential equations
- (1) created quizzes and assignments, (2) graded, and (3) held office hours

INDUSTRIAL  
EXPERIENCE

*Web Developer (Graduate Assistant)*

**Aug. 2001–May 2003**

Engineering Career Services

University of Illinois at Urbana-Champaign, Illinois, USA

- (1) Maintained web pages, perl scripts and server, (2) designed and implemented new web content, and (3) assisted with miscellaneous software and hardware needs per request

*Full-time Summer Intern*

**May. 1999–Aug. 1999**

IBM, Santa Teresa Labs, California, USA

- Learned Perl, Javascript and HTML to create a web interface to a database
- Imported IMS test cases from a mainframe into a CMVC library in order to organize them into a version tracking system
- Executed test cases on EC machines to ensure proper transfer to the new system

SUMMARY OF  
SELECTED  
RESEARCH  
PROJECTS

*XSEDE: Extreme Science and Engineering Discovery Environment*

XSEDE is the follow-on grid computing project to the TeraGrid. Funded by the NSF, XSEDE integrates services and resources at several high-performance computing (HPC) centers, campuses and labs. The mission of XSEDE is to enhance the productivity of scientists and engineers by providing them with new and innovative capabilities and thus facilitate scientific discovery while enabling transformational science/engineering and innovative educational programs. As a security analyst working under the direction of the XSEDE CSO, my goal is perform a risk assessment and help develop a risk-based operational security program for XSEDE.

*Enhancing Bro for Operational Network Security Monitoring in Scientific Environments*

Bro is an open source intrusion detection system and network traffic analyzer developed by Vern Paxson at Berkeley. Together with ICSI, I am leading an NSF Software Development for Cyber Infrastructure award (1032889) to enhance Bro in several ways and grow the Bro user community to a point of self-sustainability. My role in this project is as the **PI** of the sub-award to NCSA.

*Security for the Blue Waters Petascale Computer*

Here at the National Center for Supercomputing Applications (NCSA), we are building *Blue Waters*, one of the world's fastest supercomputers. This machine will take four years to develop and will go online in 2012. I **lead** the security component; my primary responsibilities are (1) directing all security related project activities, (2) creating the security architecture of the petascale computer, and (3) developing information and cyber security policies.

*GENI Security Program*

GENI is a large NSF initiative, with dozens of participant organizations, which aims to develop a virtual laboratory for at-scale networking experiments. It expands upon concepts developed for PlanetLab, Emulab and others; and we expect it to lead to several innovations in Internet technologies as the largest, most flexible and heterogeneous test bed of its kind. My role as a **PI** on a GENI

award is to develop an operational security program and corresponding set of agreements, using our experience at NCSA with operational security in other federations such as Open Science Grid and Teragrid.

### *CLEW*

CLEW (Cyber-investigation Law Enforcement Wizard) is a prototype tool we developed to assist non-expert law enforcement first responders in analyzing, collecting and archiving intelligence from commodity Windows machines. I was the **principal researcher** on the CLEW project at the NCSA, developing requirements and guiding feature development during my tenure. This technology will hopefully allow law enforcement to handle more cases without the need for a computer expert and allow next steps to be determined earlier during investigations. CLEW focuses on gathering information from email, IM services, and Facebook.

### *Log Anonymization and Information Management (LAIM)*

I was the **Principal Investigator** of an NSF Cyber Trust grant to explore the issues of log anonymization and information sharing. This was a four-year award, and work from the SLAGEL project—described on page 4—formed the foundation of this project. The main results of this project were (1) development of a flexible framework that anonymizes many heterogeneous logs to multiple levels and (2) study of the trade-offs of information loss and utility versus privacy and security.

We developed FLAIM<sup>1</sup> (Framework for Log Anonymization and Information Management) to meet this first goal. FLAIM is an extremely flexible anonymization tool that uses simple XML policies to sanitize various formats of logs (e.g., NetFlows, pcap traces, firewall logs, process accounting data). Not only has it enabled us to perform research on the effects of anonymization by providing the capability of analyzing the effects of fine-grained anonymization policies, it has also been found useful to others who have adopted it as a tool to anonymize their own logs. Some have even adapted and added to FLAIM's capabilities.

Addressing the second goal required a two-pronged approach. First, we used FLAIM to empirically analyze how anonymization with different algorithms and on different fields affects certain types of analysis. Most extensively, we examined how anonymization affects intrusion detection. Second, we worked to analyze the security of anonymization policies. Towards this goal, we created a taxonomy of attacks against anonymization schemes, created an adversarial model, mapped that adversarial model into the taxonomy (based upon the types of attacks an adversary can perpetrate), and finally mapped the taxonomy into a predicate logic. This allowed us to test whether a policy is vulnerable to a particular adversary or class of attacks. We were also able to add to this constraints on what can not be anonymized, (e.g., types of anonymization that would destroy utility), and determine if a policy met both the utility and security requirements of a particular scenario.

### *Cyber Integrator Shell Tool*

The prototype Cyber Integrator Shell Tool was designed to capture provenance workflows and metadata for incident response. This was accomplished by collecting important metadata (e.g., hashes and timestamps) of all data sets generated by an incident responder during a typical investigation in such a way that one could reconstruct their complete workflow. This data could then be used not only to bolster the chain of custody, but it would make it easier for one investigator to hand-off work to another investigator without explaining all that they had already done, serving didactic purposes as well. I served as the **project lead**, developing requirements, creating milestones and guiding development towards those goals.

### *NCDIR (National Center for Digital Intrusion Response)*

NCDIR was a collaboration between the FBI and the NCSA. NCDIR's mission was to deliver state-of-the-art technology, experience, and training to improve the response to (and investigation of) the cyber component of national security and criminal matters through a collaboration between NCSA's technology experts and the FBI. I served as the **security architect**, performing a threat and risk assessment and developing security requirements for the systems, networks and software we were creating.

---

<sup>1</sup><http://flaim.ncsa.uiuc.edu>

### *Palantir: Data Analytics and Tools*

*Palantir* was a cyber terrorism/crime investigation framework funded through the National Center for Advanced Secure Systems Research (NCASSR). The goal of *Palantir* was to create a fully integrated cyber investigation system in collaboration with the FBI by leveraging previous NCASSR-supported work. *Palantir* accomplished three important research goals: (1) creating a convenient portal interface to data management services, tool selection, and the audit log repository; (2) providing tools for data analysis, visualization tools that simplify complex data in a graphical format, and data transformation tools for such tasks as format conversions, error correction, and privacy enhancement; and (3) using a secure collaboration environment to support secure communications, virtual investigation teams, group discussion space, information sharing, display sharing, and all the typical capabilities a collaborative environment supports.

I was the **Principal Investigator** of the *Data Analytics and Tools* component, which was concerned with bringing two types of capabilities into the *Palantir* framework. First, we integrated log anonymization technology developed from the NSF funded LAIM project—specifically the FLAIM tool—into the *Palantir* portal environment. This was done by enhancing FLAIM’s capabilities and creating a Liferay portlet wrapper for FLAIM that allowed users to anonymize data on upload [download] to [from] the repository. Secondly, we took the desktop NetFlow-based security visualization tools developed in the SIFT project, and we created web applets from them that are wrapped in Liferay portlets. These web applet versions of the SIFT tools allow data analysis to be done on-the-fly through the portal interface without downloading logs from the repository or installing any software on the user’s local machine.

### *Mithril Project*

The Mithril project focused on the application of survivability research to standard open source software to allow a large scientific research site to continue to operate and serve customers in the face of an extraordinary attack by temporarily and gracefully reducing its level of service while raising its level of security. The current state of the art for large open systems (e.g., scientific and grid computing sites) under such attacks is near-complete shutdown, akin to quarantining a hazardous area and allowing only limited personnel into an area. While such extreme reactions do allow security administrators to get their heads above water and recover from an event, it is clearly undesirable from a customer perspective. We developed a set of integrated security enhancements that not only increases day-to-day security but also allows dynamic, temporary security adaptations in response to a heightened threat level. These enhancements allow a site to maintain a high level of openness and usability during normal periods of operation but respond quickly to increased threat levels with increased security, while continuing to serve key customers. My role in this project was to develop the strategy for correlating events from multiple sources into a single interface.

### *System Log Anonymization for Greater Exchange of Logs (SLAGEL)*

The SLAGEL project, for which I was the **Principal Investigator**, was funded through the National Center for Advanced Secure Systems Research (NCASSR), and it was the first project I led on the topic of data sanitization. The key deliverables from this project were (1) CANINE (Converter and Anonymizer for Investigating Netflow Events) and (2) Scrub-PA, a processes accounting data anonymizer. Lessons learned from developing these first anonymization tools guided the later development of FLAIM, and they focused our future research in the LAIM project.

### *Security Incidents Fusion Tools (SIFT)*

During the 2004/2005 academic year, I served as the **project manager** for the SIFT project funded by the Office of Naval Research (ONR) through NCASSR. SIFT’s goal was the development of an integrated framework for evaluating the security of an entire computer network on a single screen. In reaching towards this goal, the members of SIFT became leaders in the emerging area of *security visualization*. The project addressed the need to discover security incidents that went undetected by state-of-the-art security tools at the time. Two SIFT tool suites, NVisionIP and VisFlowConnect, leverage human visual cognitive abilities to process log data into knowledge for situational awareness of network security. Visually-presented network data can be scanned quickly; consequently, patterns in complex data rise to the surface and inferences become intuitive.

### *Secure Group Communication*

Together, with other NCSA collaborators, I worked on the design of a new group key management system. We created a scheme requiring less centralization and trust than symmetric key tree schemes but with similar performance. Our performance is only a constant factor slower than the symmetric key tree schemes, but it is asymptotically faster than the other low trust key management schemes (e.g., group Diffie-Hellman).

### *Secure E-mail List Service*

Together with two other NCSA colleagues (Himanshu Khurana and Rafael Bonilla), I worked on the design of a secure email list service. Our paper, titled *SELS: A Secure E-mail List Service*, defines the properties of a secure email list server (e.g., confidentiality, authentication, integrity, anti-spamming, etc) and presents our solution. We were given an honorable mention in Computerworld's inaugural Horizon Awards and appeared in the September, 2005 issue. SELS has since been refined, and a full working version is in use by the Teragrid security incident response team.

#### PROFESSIONAL ACTIVITIES

- Program Chair, 3<sup>rd</sup> Workshop on the Value of Security through Collaboration (SECOVAL '07), in conjunction with the International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm '07)
- TPC member, 2<sup>nd</sup> and 3<sup>rd</sup> Workshop on Information Assurance (WIA '06 & '07), in conjunction with the IEEE International Performance Computing and Communications Conference (IPCCC '06 & '07)
- TPC member, 2<sup>nd</sup> Workshop on the Value of Security through Collaboration (SECOVAL 06), in conjunction with the International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm '06)
- TPC member, 2<sup>nd</sup> Workshop on Secure Knowledge Management (SKM '06)
- TPC member, 1<sup>st</sup> and 2<sup>nd</sup> International Workshop on Cluster Security (Cluster-Sec '05 & '06), in conjunction with the IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGrid '05 & '06)
- TPC member, 1<sup>st</sup> Workshop on Storage Security and Survivability (StorageSS '05), in conjunction with the 12<sup>th</sup> ACM Conference on Computer and Communications Security (CCS), 2005
- TPC member, 1<sup>st</sup> Workshop on Visualization and Data Mining for Computer Security (VizSEC /DMSEC 2004), in conjunction with the 11<sup>th</sup> ACM Conference on Computer and Communications Security (CCS), 2004
- Reviewer for journals: *IEEE Transactions on Information Forensics and Security* (2006), *ACM Computer Communications Review* (2009)
- Chief Judge at the first Midwest Regional Collegiate Cyber Defense Challenge
- National Science Foundation (NSF) panel reviewer (2004, 2008, 2009)
- Member of Sigma Xi research society
- Member of the Information Trust Institute at the University of Illinois at Urbana-Champaign
- CISSP certification with (ISC)<sup>2</sup>
- Thesis advisor for graduate student studying computer security at the University of Illinois at Urbana-Champaign

#### HONORS AND AWARDS

- Honorable Mention, Computerworld's Inaugural Horizon Awards, 2005.
- Dean's Award, Northern Illinois University, 1999.
- University Fellowship, Northern Illinois University, 1999–2000.
- Stelford Prize, Northern Illinois University, 1999.
- Presidential Honors Science Scholarship, Northern Illinois University, 1996–1998.
- Gail Masters Gallagher Memorial Scholarship, Northern Illinois University, 1997–1999.
- KPMG Peat Marwick LLP Golden Key National Honor Society Scholarship, Northern Illinois University, 1998.
- Alumni Scholarship, Northern Illinois University, 1998-1999.
- Dick and Gay Thomason Scholarship, Zee Service Company, 1995-1999.

#### PUBLICATIONS

##### **Books**

Seigneur, J.M. and **Slagell, A.** (Eds.), "Collaborative Computer Security and Trust Management," IGI Global, Hershey, PA, 2009.

**M.S. Thesis**

**Slagell, A.**, "A Simple, Portable and Expandable Cryptographic Program Interface," *Master's Thesis*, University of Illinois at Urbana-Champaign, May, 2003.

## Journals

**Slagell, A.**, "Thinking Critically about Computer Security Trade-offs," *Skeptical Inquirer*, Vol. 34, No. 4, Jul., 2010.

## Refereed Conference and Workshop Papers

**Slagell, A.**, "Fear, Uncertainty and Doubt: The Pillars of Justification for Cyber Security," *The Amazing Meeting 7 (TAM 7)*, Las Vegas, NV, Jul., 2009.

King, J., Lakkaraju, K., **Slagell, A.**, "A Taxonomy and Adversarial Model for Attacks against Network Log Anonymization", *24<sup>th</sup> ACM Symposium on Applied Computing*, Honolulu, HA, Mar., 2009.

Lakkaraju, K. and **Slagell, A.**, "Evaluating the Utility of Anonymized Network Traces for Intrusion Detection," *4<sup>th</sup> Annual SECURECOMM Conference*, Istanbul, Turkey, Sep., 2008.

**Slagell, A.**, Lakkaraju, K., and Luo, K., "FLAIM: A Multi-level Anonymization Framework for Computer and Network Logs," *20<sup>th</sup> USENIX Large Installation System Administration Conference (LISA '06)*, Washington, D.C., Dec., 2006.

Basney, J., Flanigan, P., Heo, J., Khurana, H., Muggli, J., Pant, M., **Slagell, A.**, and Welch, V., "Mithril: Adaptable Security for Survivability in Collaborative Computing Sites," *Workshop on Enterprise Network Security (WENS '06)*, Baltimore, MD, Sep., 2006.

Yin, X., Yurcik, W., and **Slagell, A.**, "VisFlowCluster-IP: Connectivity-Based Visual Clustering of Network Hosts," *21<sup>st</sup> IFIP TC-11 International Information Security Conference (SEC '06)*, Karlstad, Sweden, May, 2006.

Li, Y., **Slagell, A.**, Luo, K., and Yurcik, W., "CANINE: A Combined Conversion and Anonymization Tool for Processing NetFlows for Security," *10<sup>th</sup> International Conference on Telecommunication Systems, Modeling and Analysis*, Dallas, TX, Nov., 2005.

Lakkaraju, K., Bearavolu, R., **Slagell, A.**, Yurcik, W., and North, S., "Closing-the-Loop in NVisionIP: Integrating Discovery and Search in Security Visualizations," *2<sup>nd</sup> International Workshop on Visualization for Computer Security (VizSEC '05)*, Minneapolis, MN, Oct., 2005.

Luo, K., Li, Y., **Slagell, A.**, and Yurcik, W., "CANINE: A NetFlow Converter/Anonymizer Tool for Format Interoperability and Secure Sharing," *FLOCON — Network Flow Analysis Workshop*, Pittsburgh, PA, Sep., 2005.

Yin, X., Yurcik, W., and **Slagell, A.**, "VisFlowConnect-IP: An Animated Link Analysis Tool for Visualizing NetFlows," *FLOCON – Network Flow Analysis Workshop*, Pittsburgh, PA, Sep., 2005.

**Slagell, A.**, and Yurcik, W., "Sharing Computer Network Logs for Security and Privacy: A Motivation for New Methodologies of Anonymization," *SECOVAL: The Workshop on the Value of Security through Collaboration*, Athens, Greece, Sep., 2005.

**Slagell, A.**, Li, Y., and Luo, K., "Sharing Network Logs for Computer Forensics: A New Tool for the Anonymization of NetFlow Records," *Computer Network Forensics Research (CNFR) Workshop*, Athens, Greece, Sep., 2005.

Lakkaraju, K., Bearavolu, R., **Slagell, A.** and Yurcik, W., "Closing-the-Loop: Discovery and Search in Security Visualizations," *6<sup>th</sup> IEEE Information Assurance Workshop*, West Point, NY, Jun., 2005.

Khurana, H., Bonilla, R., **Slagell, A.**, Afandi, R., Hahm, H.S., and Basney, J., "Scalable Group Key Management with Partially Trusted Controllers," *4<sup>th</sup> International Conference on Networking (ICN '05)*, Reunion Island, Apr., 2005.

Yin, X., Yurcik, W., and **Slagell, A.**, "The Design of VisFlowConnect-IP: a Link Analysis System for IP Security Situational Awareness," 1<sup>st</sup> *International Workshop on Information Assurance (IWIA '05)*, College Park, MD, Mar., 2005.

Khurana, H., **Slagell, A.** and Bonilla, R., "SELS: A Secure E-mail List Service," *ACM Symposium on Applied Computing (SAC '05)*, Santa Fe, NM, Mar., 2005.

**Slagell, A.**, Wang, J. and Yurcik, W., "Network Log Anonymization: Application of Crypto-PAN to Cisco NetFlows," *NSF/AFRL Workshop on Secure Knowledge Management (SKM '04)*, Buffalo, NY, Sep., 2004.

Basney, J., Yurcik, W., **Slagell, A.**, and Bonilla, R., "Credential Wallets: A Classification of Credential Repositories Highlighting MyProxy," *Telecommunications Policy Research Conference (TPRC '03)*, Arlington, VA, Sep., 2003.

### Invited Conference and Workshop Papers

**Slagell, A.**, and Bonilla, R., "A Survey of PKI Components and Scalability Issues," *Workshop on Information Assurance (WIA 2006)*, Phoenix, AZ, Apr., 2006.

### Technical Reports

Luo, K., Li, Y., Ermopoulos, C., Yurcik, W., and **Slagell, A.**, "Scrub-PA: A Multi-level, Multi-Dimensional Anonymization Tool for Process Accounting," *ACM Computing Research Repository (CoRR)*, Technical Report cs.CR/0601079, Jan., 2006.

**Slagell, A.**, and Bonilla, R., "PKI Scalability Issues," *ACM Computing Research Repository (CoRR)*, Technical Report cs.CR/0409018, Sep., 2004.

**Slagell, A.**, "Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm," *Cryptology ePrint Archive*, Report 2004/011, Jan., 2004.

## REFERENCES

Aaron Falk  
Technical Director  
BBN Technologies  
10 Moulton Street, Cambridge, MA 02138  
Tel: (617) 873 2575; Email: falk@bbn.com

Randal Butler  
Director, Cybersecurity Directorate  
National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign  
1008 NCSA Building, 1205 W. Clark St, Urbana, IL 61801  
Tel: (217) 244-8285; Email: rbutler@ncsa.uiuc.edu

Professor William Sanders  
Director  
Coordinated Science Lab, University of Illinois at Urbana-Champaign  
451 Coordinated Science Laboratory, 1308 West Main St, Urbana, IL 61801  
Tel: (217) 333-0345; Email: whs@uiuc.edu

Von Welch  
Deputy Director  
Center for Applied Cybersecurity Research, Indiana University  
2719 E. 10<sup>th</sup> St, Suite 201, Bloomington, IN 47408  
Tel: (812) 856-0363; Email: vwelch@indiana.edu