

## David James Brumley

---

### CONTACT INFORMATION

Carnegie Mellon University  
Wean Hall #8116  
5000 Forbes Ave  
Pittsburgh, PA 15213 USA

*Phone:* (412) 334-1330  
*Fax:* (412) 268-5576  
*E-mail:* dbrumley@cs.cmu.edu  
*WWW:* www.cs.cmu.edu/~dbrumley

### RESEARCH INTERESTS

My current work focuses on software security, especially security analysis of binary (executable) code. I am interested in all aspects of security, including network security and applied cryptography, as well as programming languages, compilers, formal methods, and systems.

### EDUCATION

Carnegie Mellon University, Pittsburgh, Pennsylvania  
Ph.D. student in Computer Science. Expected graduation: 2008.  
Advisor: Dawn Song  
Thesis: A Binary-centric Approach to Vulnerability Analysis and Defense  
Research topics: Software Security and Vulnerability Defense  
Selected course work: Graduate Algorithms, Type Systems, Theoretical Cryptography, Logic Programming Languages, Software and Network Security

Stanford University, Stanford, California  
M.S. in Computer Science, April 2003.  
Advisors: Dan Boneh and Monica Lam  
Research topics: Applied Cryptography, Compilers, and Ubiquitous Computing  
Selected course work: Compilers, Advanced Compilers, Topics in Compilers, Cryptography, Topics in Cryptography, Automata Theory

University of Northern Colorado, Greeley, Colorado  
B.A. in Mathematics, May 1998.

Red Rocks Community College, Lakewood, Colorado

### REFEREED PUBLICATIONS

1. David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng. Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications. In the *Proceedings of the IEEE Security and Privacy Symposium*, May, 2008.
2. David Brumley, Juan Caballero, Zhenkai Liang, James Newsome, and Dawn Song. Towards Automatic Discovery of Deviations in Binary Implementations with Applications to Error Detection and Fingerprint Generation. In the *Proceedings of the 16<sup>th</sup> Annual USENIX Security Symposium*, 2007.  
\* **Conference “Best Paper”**
3. David Brumley, Hao Wang, Somesh Jha, and Dawn Song. Creating Vulnerability Signatures Using Weakest Pre-conditions. In the *Proceedings of the 20<sup>th</sup> IEEE Computer Security Foundations Symposium*, 2007.
4. Joseph Tucek, James Newsome, Shan Lu, Chengdu Huang, Spiros Xanthos, David Brumley, Yuanyuan Zhou and Dawn Song. Sweeper: A Lightweight End-to-End System for Defending Against Fast Worms. In the *Proceedings of the 2007 EuroSys Conference*, 2007.
5. Nikita Borisov, David Brumley, Helen Wang, John Dunagan, Pallavi Joshi, and Chuanxiong Guo. A Generic Application-Level Protocol Analyzer and its Language. In the *Proceedings of the 14<sup>th</sup> Annual Network and Distributed System Security Symposium (NDSS)*, 2007.

6. David Brumley, Tzi-cker Chiueh, Robert Johnson, Huijia Lin, Joseph Slember, and Dawn Song. Efficient and Accurate Detection of Integer-Based Attacks. In the *Proceedings of the 14<sup>th</sup> Annual Network and Distributed Systems Symposium (NDSS)*, 2007.
7. James Newsome, David Brumley, Jason Franklin and Dawn Song. Replayer: Automatic Protocol Replay by Binary Analysis. In the *Proceedings of the 13<sup>th</sup> ACM Conference on Computer and Communications Security (CCS)*, 2006
8. David Brumley and Dawn Song. Towards Attack-Agnostic Defenses. In the *Proceedings of the First Workshop on Hot Topics in Security (HOTSEC)*, 2006.
9. David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha. Towards Automatic Generation of Vulnerability-Based Signatures. In the *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, 2006.  
\* **Among top 3 conference papers. Selected by PC for the IEEE Transactions on Dependable and Secure Computing journal.**
10. James Newsome, David Brumley, and Dawn Song. Vulnerability-Specific Execution Filtering for Exploit Prevention on Commodity Software. In the *Proceedings of the 13<sup>th</sup> Annual Network and Distributed Systems Security Symposium (NDSS)*, 2006.
11. David Brumley, Li-Hao Liu, Pongsin Poosankam, and Dawn Song. Design Space and Analysis of Worm Defense Strategies. In the *Proceedings of the 2006 ACM Symposium on Information, Computer, and Communication Security (ASIACCS)*, 2006.
12. David Brumley and Dan Boneh. Remote Timing Attacks are Practical. *Journal of Computer Networks*, 48:701-716, 2005.
13. David Brumley and Dawn Song. Privtrans: Automatically partitioning programs for privilege separation. In the *Proceedings of the 13<sup>th</sup> USENIX Security Symposium*, 2004.
14. Constantine Sapuntzakis, David Brumley, Ramesh Chandra, Nikolai Zeldovich, Jim Chow, Monica S. Lam, Mendel Rosenblum. Virtual Appliances for Deploying and Maintaining Software. In the *Proceedings of the 17<sup>th</sup> Large Installation System Administration Conference*, 2003.
15. David Brumley and Dan Boneh. Remote Timing Attacks are Practical. In the *Proceedings of the 12<sup>th</sup> USENIX Security Symposium*, 2003.  
\* **Conference “Best Paper”**

#### BOOK CHAPTERS

1. David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Pongsin Poosankam, Dawn Song, and Heng Yin. *Botnet Detection*, volume 36 of Countering the Largest Security Threat Series: Advances in Information Security, chapter Automatically Identifying Trigger-based Behavior in Malware. Springer-Verlag. 2008.
2. David Brumley, James Newsome, and Dawn Song. Sting: An End-to-End Self-Healing System for Defending against Internet Worms. In *Malware Detection*, Springer Publications, 2007.

#### PENDING AND SUBMITTED PUBLICATIONS

1. David Brumley, James Newsome, Dawn Song, Hao Wang, and Somesh Jha. Theory and Techniques for Automated Generation of Vulnerability-Based Signatures. Under submission to the *IEEE Transactions on Dependable and Secure Computing*, 2006.
2. David Brumley, Pongsin Poosankam, Dawn Song, and Jiang Zheng. Automatic Patch-Based Exploit Generation is Possible: Techniques and Implications. Under submission, 2007.
3. David Brumley, Zhenkai Liang, James Newsome, and Dawn Song. Automatic Generation of Multi-Path Vulnerability Signatures. Under submission, 2007.

## PATENTS

1. Apparatuses, Systems, and Methods for Malware Detection and Analysis, and for Protection from Malware. 2006. (Patent Pending.)
2. Generic Application Level Protocol Analyzer. 2005. (Patent Pending with Microsoft)
3. A Cache-Based System Management Architecture with Virtual Appliances, Network Repositories, and Virtual Appliance Transceivers. (Patent Pending. US Application Number 11/007,911, December 8, 2004. US Provisional Application Number 60/528,220, Dec 8, 2003. Expected Issue Date: Spring, 2008. Licensed to moka5.com)

## SELECTED TECHNICAL REPORTS

1. David Brumley and James Newsome. Alias Analysis for Assembly. Carnegie Mellon University School of Computer Science, CMU-CS-06-180. December, 2006.
2. James Newsome, David Brumley, and Dawn Song. Sting: An End-to-End Self-healing System for Defending Against Zero-day Worm Attacks on Commodity Software. Carnegie Mellon University School of Computer Science, CMU-CS-05-191. November, 2005.

## ARTICLES

1. David Brumley. A Crash Course in Managing Security. USENIX ;login, Nov 2001.
2. David Brumley. Solaris security: A comparison between YASSP, Titan, and SANS. Global Information Assurance Certification, Oct 2000.
3. David Brumley. Tracking Hackers Through IRC. USENIX ;login, Nov 1999.
4. David Brumley. Rootkits: How Intruders Hide. USENIX ;login, Sept 1999.

## PROFESSIONAL ACTIVITIES

### *Program Committee Member*

- First European Workshop on System Security (EUROSEC), Glasgow, England, 2008.
- Recent Advances in Intrusion Detection (RAID), Boston, MA, 2008.
- Fifth Conference on Detection and Malware and Vulnerability Assessment (DIMVA), Paris, France, 2008.
- Fifteenth Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA, 2008
- Second Workshop on Security Network Protocols (NPSEC), Santa Barbara, CA, 2006.
- Applied Cryptography and Network Security (ACNS), New York, New York, 2005.
- First Workshop on Secure Network Protocols (NPSEC), Boston, MA, 2005.

### *Teaching*

- Teaching Assistant for Special Topics in Network & Software Security (CS 18711), Carnegie Mellon, 2005.
- Teaching Assistant for Introduction to Compilers (CS 15411), Carnegie Mellon, Fall 2004.
- Guest Lecturer, Special Topics in Network & Software Security course, Carnegie Mellon, 2003-2007.
- Denial of service attacks. Computer and Network Security course, Stanford, 2002.
- Introduction to computer security. 4 day course at the Universidad Francisco Marroquin, Guatemala, 1999 & 2001.
- Perspectives on distributed denial of service attacks. Computer Systems Seminar, Stanford, 1999.

### *Departmental Activities and Service*

- PhD Admissions Committee, CMU, 2005 & 2006.
- Computer Security Reading Group, CMU, 2005 & 2006.
- Speaking Skills Committee, CMU, 2004-Present.
- Master's Admissions Committee, Stanford, 2002.

*Selected Invited talks*

- Malware Experimentation Panel. *DETER* Community Workshop on Cyber Security Experimentation and Test, 2007.
- Why computer security is hard – examples from cryptography. Network Seminar Series, University of Chicago, 2002.
- Ask the experts. FIRST Annual Conference, 2002.
- Computer security issues in higher education. Colorado Higher Education Computing Organization (CHECO), 2001.
- DDoS attacks. Web Defense Conference, 2000.
- Ask the experts. First Annual Conference, 2000.
- Invited discussions on DDoS. CERT Distributed Attack Tools Workshop, 1999.
- University issues. USENIX Large Installation System Administration Conference (LISA), 1999.
- Computer security response at Stanford. FIRST Technical Colloquium, 1999.

*Internships*

- Symantec Research Labs, Summer 2007. Worked with Tzi-cker Chiueh
- Microsoft Research, Summer 2004. Worked with Helen Wang

SELECTED  
AWARDS &  
HONORS

- Symantec Graduate Fellowship Award, 2007-2008.
- USENIX Security Best Paper Award for “Towards Automatic Discovery of Deviations in Binary Implementations with Applications to Error Detection and Fingerprint Generation”, 2007.
- IEEE Security and Privacy program committee selected “Towards Automatic Generation of Vulnerability-Based Signatures” for recommendation to IEEE Transactions on Dependable and Secure Computing (one of top three conference papers), 2006.
- USENIX Security Best Paper Award for “Remote timing attacks are practical”, 2004.
- Distinguished Visiting Scholar at the Universidad Francisco Marroquin, 1999 & 2001.
- Computer Science Student of the Year, UNC 1998.

PROFESSIONAL  
EXPERIENCE

Computer Security Officer. 1998 - 2002  
Stanford University. Stanford, CA  
Responsible for computer security of Stanford, including policy development, intrusion detection and prevention, hardened OS setup and guidelines, and working with law enforcement. Responded to over 2000 computer security incidents throughout Stanford and the Stanford Hospital.

Network Administrator. 1995 - 1998  
University of Northern Colorado. Greeley, CO  
Responsible for all UNIX machines in IT department, including user systems, SMTP, DNS, HTTP, and other network services. Ported LDAP to AIX.

REFERENCES

<p>Prof. Dawn Song University of California, Berkeley Computer Science Division 675 Soda Hall UC Berkeley, CA 94720-1776 1-510-642-8282 dawnsong@cs.berkeley.edu</p>	<p>Prof. Randal Bryant Carnegie Mellon University 5000 Forbes Avenue Pittsburgh, Pennsylvania 15213-3891 1-412-268-8821 Randy.Bryant@cs.cmu.edu</p>
--	---

Prof. Peter Lee  
Carnegie Mellon University  
5000 Forbes Avenue  
Pittsburgh, PA 15213-3891  
1-412-268-3049  
petel@cs.cmu.edu

Prof. Bruce M. Maggs  
Carnegie Mellon University  
5000 Forbes avenue  
Pittsburgh, PA 15213  
1-412-268-7654  
bmm@cs.cmu.edu

Prof. Somesh Jha  
University of Wisconsin at Madison  
Computer Sciences Department  
University of Wisconsin  
Madison, WI 53706  
1-608-262-9519  
jha@cs.wisc.edu

Additional references available upon request.