CURRICULUM VITAE

NAVEEN SASTRY

EDUCATION

2001–2006: University of California, Berkeley. Ph.D. in Computer Science. GPA 3.921. Dissertation: "Verifying Security Properties in Electronic Voting Machines." Advised by Dr. David Wagner.

1996–2000: Cornell University, College of Engineering. B.S. in Computer Science with departmental honors and magna cum laude. GPA 4.03 in major, 3.91 overall (A+ = 4.3).

RESEARCH EXPERIENCE

2004–2006: *Graduate student researcher, University of California, Berkeley. Developing techniques for designing secure electronic voting machines. This includes analyzing existing systems, presenting new architectures for easier verification, and software verification techniques.*

Summer 2004: Research Intern, Microsoft Corporation. Redmond, Washington. Worked on using language-based tools to harded managed code applications against attacker exploitation of resources through unintened code paths.

2001–2004: Graduate student researcher, University of California, Berkeley. Studied security challenges for sensor networks. Developed TinySec, a link layer security architecture for the Berkeley Mica family of motes. Created a secure authentication protocol to establish location claims inside regions.

2001: Graduate student researcher, University of California, Berkeley. Worked on the Recovery Oriented Computing (ROC) project Analyzed system software recovery and reliability issues and developed a fault injection test to find reliability problems in software. My work was described in Scientific American.

1997–2000: *Undergraduate researcher, Cornell University. Worked on extensible Java compilers, IP Telephony.*

TEACHING EXPERIENCE

January 2005–May 2006: University of California, Berkeley. Mentored two undergraduate students to enable security for the new generation of Mica wireless sensor networks. Taught them the fundamentals of research, such as documenting work, developing effective metrics for success, and problem selection.

Spring 2003: University of California, Berkeley. Graduate student instructor for C.S. 170, an upper division algorithms course. Taught two sections per week, held twice weekly office hours, and developed weekly homework problems. Rated 4.1 / 5.0 for teaching effectiveness by students; additional rating details at `http://hkn.berkeley.edu/student/nsurvey/tas/Sastry_Naveen.html`.

Spring 2000: Cornell University. Teaching Assistant for C.S. 211, a sophomore level class teaching programming and data structures. Taught one section per week and a weekly review session for the entire class.

WORK EXPERIENCE

June 2006–present: *Consultant, Dust Networks, Hayward, CA. I developed efficient and secure wireless* networking communication protocols. My role is the chief security advisor to ensure the protocols are secure against all attacks.

December 2006: Consultant, California Secretary of State's Voting System Technology Assessment Advisory Board (VSTAAB). Produced a report (`http://www.cs.berkeley.edu/~nks/papers/diebold-sos06.pdf`) analyzing the security implications of the Diebold AccuBasic Interpreter.

Summer 2004: *Research Intern, Microsoft Research, Redmond. Investigated techniques to prevent* exploitations in managed code applications that access unintended resources.

2000–2002: Software Architect, Intelligent Markets Corporation, San Francisco. Designed and implemented reliable communication architecture and data model for a distributed bond trading system.

Summer 1999: Intern, Microsoft Corporation, Redmond. Developed simulator and harness to profile DirectPlay networking API.

Summer 1998: Intern, Microsoft Corporation, Redmond. Developed SQL Server replication demonstration applications.

HONORS & AWARDS

2004: Best student paper, ACM Workshop on Wireless Security for "Security Considerations for IEEE 802.15.4 Networks." October 1, 2004.

2003: *Recognized for valuable contributations as a Graduate Student Instructor, Department of Electrical* Engineering and Computer Science, University of California, Berkeley.

2002: Best student presentation, SHAMAN Workshop, June 2002.

2000: graduated Cum Laude, with honors from Cornell University.

2000: Tau Beta Pi Honor Society.

1996–2000: Dean's List, Cornell University.

PUBLICATIONS

Reprints are available at `http://www.cs.berkeley.edu/~nks/`.

PEER-REVIEWED CONFERENCE AND WORKSHOP PAPERS

"Designing Voting Machines for Verification," N. Sastry, T. Kohno, and D. Wagner. *Proceedings of USENIX Security Symposium 2006*, August 2006.

"Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract)," D. Molnar, T. Kohno, N. Sastry, and D. Wagner. *IEEE Security and Privacy*, May 2006.

"Cryptographic Voting Protocols: A Systems Perspective," C. Karlof, N. Sastry, and D. Wagner. *Proceedings of USENIX Security Symposium 2005*, August 2005.

"Fixing Races for Fun and Profit: How to Abuse atime," N. Borisov, R. Johnson, N. Sastry, and D. Wagner. *Proceedings of USENIX Security Symposium 2005*, August 2005.

" Design and Implementation of a Sensor Network System for Vehicle Tracking and Autonomous Interception," C. Sharp, S. Schaffert, A. Woo, N. Sastry, C. Karlof, S. Sastry, and D. Culler. *European*

Workshop on Wireless Sensor Networks (EWSN'05), January – February 2005.

"TinySec: A Link Layer Security Architecture for Wireless Networks," C. Karlof, N. Sastry, and D. Wagner. *Proceedings of SenSys 2004*, November 2004.

"Security Considerations for 802.15.4 Networks," N. Sastry, and D. Wagner. *ACM Workshop on Wireless Security 2004*, October 2004.

"Distillation Codes and Applications to DoS Resistant Multicast Authentication," C. Karlof, N. Sastry, Y. Li, A. Perrig, and J.D. Tygar. *Eleventh Annual Network and Distributed Systems Security Symposium (NDSS 2004)*, February 2004.

"Secure Verification of Location Claims," N. Sastry, U. Shankar, and D. Wagner. In *ACM Workshop in Wireless Security 2003*, October 2003.

"Scrash: A System for Generating Secure Crash Information," P. Broadwell, M. Harren, and N. Sastry. In *Proceedings of Usenix Security 2003*, August 2003.

"FIG: Fault Injection in GLIBC," P. Broadwell, N. Sastry, and J. Traupman. In *Workshop on Self-Healing, Adaptive and Self-MANaged Systems (SHAMAN)*, June 2002.

POPULAR PRESS

"Secure Verification of Location Claims," N. Sastry, U. Shankar, and D. Wagner. RSA CryptoBytes Technical Newsletter, Spring 2004.

"Self-Repairing Computers," A. Fox, D. Patterson. Scientific American, June 2003.

TECHNICAL REPORTS

"Secure Verification of Location Claims," N. Sastry, U. Shankar, D. Wagner. Technical Report UCB//03-1245, University of California, Berkeley, June 2003.

"Recovery-Oriented Computing (ROC): Motivation, Definition, Techniques, and Case Studies," D. Patterson, A. Brown, P. Broadwell, G. Candea, M. Chen, J. Cutler, P. Enriquez, A. Fox, E. Kiciman, M. Merzbacher, D. Oppenheimer, N. Sastry, W. Tetzlaff, J. Traupman, N. Treuhaft. Technical Report UCB//CSD-02-1175, University of California, Berkeley, March 2002.

PROFESSIONAL ACTIVITIES

External conference submission reviewer for Usenix Security 2003, IEEE Privacy and Security 2004, IEEE International Conference on Mobile Ad-hoc and Sensor Systems 2004, Usenix Operating System Design and Implementation 2004, ACM SigMobile 2004, ACM Conference on Embedded Sensor Systems 2004, 2005 Information Security Conference (ISC), NDSS 2006.

Member of graduate admissions committee, Computer Science Division, University of California, Berkeley for 2004 cycle.

Member of Usenix since 2002.

PRESENTATIONS AND INVITED TALKS

Usenix Security 2006, "Designing Voting Machines for Verification," August 4, 2006.

Cryptography, CS276. UC Berkeley, "Cryptographic Voting Protocols," April 18, 2006.

Graduate Seminar on Sensor Actuator Networks, CS294-11. UC Berkeley, " A Critical Look at Sensor Network Security," November 17, 2005.

Usenix Security 2005, "Fixing Races for Fun and Profit: How to Abuse atime," August 2005.

ACM SenSys, "TinySec: A Link Layer Security Architecture for Sensor Networks," November 4, 2004.

ACM Workshop on Wireless Security, "Security Considerations for IEEE 802.15.4 Networks," October 1, 2004.

Sun Microsystems Labs, "TinySec: A Link Layer Security Architecture for Sensor Networks," April 4, 2004.

Usenix Security 2003, "Scrash: A System for Generating Secure Crash Information," August 2003.

Workshop on Self-Healing, Adaptive and Self-MANaged Systems (SHAMAN), "FIG: Fault Injection in GLIBC," June 2002.