Bennet Yee

CURRICULUM VITAE

Jun 2003

Department of Computer Science & Engineering, Mail Code 0114
University of California at San Diego
9500 Gilman Drive
La Jolla, CA 92093, USA.
Phone: (858) 534-4614
FAX: (858) 534-7029
E-mail: `bsy@cs.ucsd.edu`
Web Page: `http://www.cs.ucsd.edu/users/bsy/`

Research areas

- *Computer security:* Secure distributed systems; electronic commerce; intellectual property protection; electronic payment protocols; secure computer hardware engineering; mobile code security.
- *Cryptography:* Authentication; encryption; key distribution; message authentication; integrity of computation; privacy of computation.

Education

Carnegie Mellon University

- Ph.D in Computer Science, September 1994. Thesis title: *Using Secure Coprocessors*. Thesis supervisor: Prof. D. Tygar.

Oregon State University

- B.S. with honors, dual major. Subjects: Mathematics, Computer Engineering. June 1986.

Achievements and awards

- National Merit Scholarship. 1981.
- National Semiconductor Corp. Faculty Development Program Award—1996. One of four inaugural recipients.
- NSF CAREER award, 1998.

Research Grants and Gifts

- National Semiconductor Faculty Development Award, 1996. A gift of $40,000.
- IBM Corp. Research equipment support: secure coprocessor cards for research use, 1997–present.
- Intel Corp, 1997. An equipment grant of approx $200,000. (Four co-PIs.)
- U. S. Postal Service. Research contract of $76,790 to investigate the security of Multi-Line Optical Character Recognition mail sorting machines.
- NSF CAREER award, 1998. A grant of $205,000 split over four years.
- NEC Corp, 1998. A gift of $12,000.
- Microsoft Corp, 2000. A gift of $60,000.
- Office of Naval Reearch. "Understanding Mobile Code and Secure Execution Environments", 2001. $1,000,000 over five years.

Memberships and Professional Activities

- Reviewed grant proposals for the National Science Foundation ITR program, June 2000; June 2002.
- Invited participation in the National Science Foundation's "Setting a National Research Agenda: A Workshop on Research Issues in Security, Privacy, and Trust", February 2002.
- Program chair for the Third USENIX Workshop on Electronic Commerce.
- Program committee member for the following conferences: Second USENIX Workshop on Electronic Commerce; Fifth ACM Conference on Computer and Communications Security; Financial Cryptography '99; 19th IEEE International Conference on Distributed Computing Systems; Internet Society's Network and Distributed Systems Security Symposium, 2000; Internet Society's Network and Distributed Systems Security Symposium, 2001; Usenix Security, 2002; Usenix Technical Conference, 2003.
- Invited participation in the National Academy of Engineering's Fifth Annual Symposium on Frontiers of Engineering.
- Reviewed papers for ACM Transactions on Computer Systems, IEEE Transactions on Software Engineering, IEEE Internet Computing Magazine, ACM Transactions on Software Engineering and Methodology, Third International Workshop on Information Security, International Journal of Electronic Commerce, ACM SIGCOMM Computer Communication Review, IBM Systems Journal.
- Refereed papers for USENIX Technical Conference, ACM Symposium on Principles of Distributed Computing, ACM SIGPLAN Conference on Programming Language Design and Implementation, ACM Symposium on Operating System Principles, IEEE Transactions on Information Theory.

- Reviewed grant proposals for the University of California's MICRO program, and for the Research Grants Council of Hong Kong.
- Member, Tau Beta Pi honor society
- Member, Eta Kappa Nu honor society
- Member, Phi Kappa Phi honor society
- Member, Association for Computing Machinery
- Member, International Association for Cryptologic Research

Consulting

Tektronix Corp. 1979–1981.

International Business Machines. Summer 1991. Summer 1997.

Bellcore Postgraduate Education. Spring 1992.

United States Postal Service. 1993–1994.

Microsoft, Qualcomm, Vadem. 1998–2000.

EmailFund, Inc. 1999–2001.

Work Experience

Software Assurance Engineer, Tektronix Corp. 1981–1985. Automated Instrument Compatibility Evaluation group. (Manager: B. Cram). Responsible for design and development of TestPak, a computer-aided testing system for evaluating new products for comformance to various standards; designed and implemented a network protocol fault injection system.

Research Assistant, School of Computer Science, CMU. June 1986–May 1994. Worked with Professors D. Tygar, R. Rashid, and A. Spector on the Strongbox, CAMELOT, Mach, and Dyad systems.

Postdoctoral Research Assistant, School of Computer Science, CMU. May 1994–December 1994. Full time.

Cryptographer / Software Design Engineer, Microsoft Corp. December 1994–January 1996. Full time. Cryptography group. (Manager Dr. A. Cooper). Responsible for cryptanalysis, cryptographic protocol design, security reviews of software.

Assistant Professor, Dept. of Computer Science and Engineering, University of California at San Diego, January 1996–present.

Industrial Impact

- My secure coprocessor work [16] has motivated IBM Research to design and build the IBM 4758, a cryptographic coprocessor card. This product is doing well commercially, and also serves as the

foundation of future research both for the IBM Embedded Cryptographic Systems Group and for my own work. (`http://www.ibm.com/Security/cryptocards/`)
My work on using physical security and cryptographic processing to enhance operating system security and applications security has led in part to the Trusted Computing Platform Association (TCPA—a consortium of companies, including Intel, AMD, and IBM) and the Palladium (Microsoft) efforts. Because secure coprocessors are extremely secure and enable a wide variety of security policies to be enforced—including those that would erode consumers' fair-use rights—some research in these directions have been somewhat controversial.

- My work with the USPS on the use of secure coprocessors (Postal Security Devices are one kind), cryptography, and verification techniques has led to the implementation of the Information Based Indicia Program (IBIP), whereby users are able to print their own stamps using PCs and standard printers. This technology is used by `estamp.com` and `stamps.com`; additional IBIP products are available from other companies such as Pitney-Bowes Inc; more are slated to be introduced soon.
- The Personal Communications Technology (PCT) protocol described in [22] is in use in Microsoft's Internet Explorer and BackOffice for secure communications between web browsers and servers. Elements of PCT has been merged with SSL v3.0 to form IETF's TLS protocol, which is the primary security protocol in use for protecting electronic commerce today.
- My work (with Kobayashi) on Internet-purchased tickets simplified and extended my earlier work on stamps to electronic commerce for venue admissions (e.g., theaters, aquariums, zoos, concert halls) and has resulted in a patent being filed. Our public demonstration at the Birch Aquarium has generated public interest in the technology, and the technology has been licensed by NEC Corp and `records.de`, a German startup company. The demonstration web site has been archived at `http://philby.ucsd.edu/triton/`.

Teaching

- Systems Programming (CSE 30)—Undergraduate course in the CSE Dept. at UCSD. Fall 1996; Fall 1997; Fall 1998; Fall 1999.
- Unix Lab (CSE 80)—Undergraduate course in the CSE Dept. at UCSD. Spring 1996; Winter 1997.
- Operating Systems Architecture and Implmentation (CSE 121)—Undergraduate course on operating system internals. Fall 2000.
- Introduction to Computer Security (CSE 127)—Undergraduate course on computer security, CSE Dept. at UCSD. Winter 2002; Winter 2003. This is a course that I designed.
- Introduction to Computer and Network Security (CSE 190)—Undergraduate course in the CSE Dept. at UCSD, Spring 1998.
- Introduction to Systems Security (CSE 190A)—Undergraduate course introducing systems security concepts, CSE Dept. at UCSD. Spring 1999.
- Advanced Unix Programming (CSE 190)—Undergraduate course on Unix systems programming. Spring 2000.
- Distributed Systems Security (CSE 291)—Graduate seminar on the design of secure distributed systems, CSE Dept. at UCSD, Fall 1996.
- Operating Systems (CSE 221)—Graduate core course in the CSE Dept., UCSD. Spring 1998; Fall 1998; Fall 1999; Winter 2001.

- Computer Security (CSE 227)—Graduate course on systems security, CSE Dept. at UCSD. Spring 1999; Winter 2002; Witner 2003. This is a course that I designed.
- Faculty Research Seminar (CSE 292)—Graduate seminar on various topics. Organizational: coordinated speakers. Fall 1998; Winter 1999; Fall 1999.

Publications: Research Articles

[1] D. Tygar, B. Yee, and A. Spector. StrongBox: A Self-Securing Protection System for Distributed Programs. In *Proc. USENIX Workshop on Computer Security*, 1988.

[2] D. Tygar and B. Yee. Strongbox. In J. Eppinger, L. Mummert, and A. Spector, editors, *Camelot and Avalon: A Distributed Transaction Facility*. Morgan-Kauffman, 1991.

[3] D. Tygar and B. Yee. Strongbox: a system for self-securing programs. In R. Rashid, editor, *Carnegie Mellon Computer Science: A 25-Year Commemorative.* ACM Press and Addison-Wesley, 1991.

[4] D. Tygar and B. Yee. Dyad: a system for using physically secure coprocessors. In *The Journal of the Interactive Multimedia Association Intellectual Property Project.* Volume 1, Issue 1, 1994.

[5] D. Tygar and B. Yee. Secure coprocessors in electronic commerce applications. In *Proceedings of the First USENIX Workshop on Electronic Commerce*, 1995.

[6] D. Tygar, B. Yee, and N. Heintze. Designing cryptographic postage indicia. Invited paper *ASIAN-96.*

[7] H. Gobioff, S. Smith, D. Tygar, and B. Yee. Smart cards in hostile environments. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*, 1996.

[8] J. Camp, M. Harkavy, D. Tygar, and B. Yee. Anonymous atomic transactions. In *Proceedings of the Second USENIX Workshop on Electronic Commerce*, 1996.

[9] S. Belmon and B. Yee. Mobile agents and intellectual property protection. In *Springer Journal on Personal Technologies*, K. Rothermel and J. Baumann eds., Springer Verlag. Volume 2, Number 3, 1998. A preliminary version appeared in *Mobile Agents '98*, Lecture Notes in Computer Science Vol. 1477, K. Rothermel and F. Hohl eds., Springer Verlag, 1998.

[10] B. Yee. A sanctuary for mobile agents. In *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, Lecture Notes in Computer Science, Vol. 1603, J. Vitek and C. Jensen eds., Springer Verlag, 1999. A preliminary version appeared in *Proceedings of the DARPA Workshop on Foundations for Secure Mobile Code*, 1997, and as Technical Report CS97-537, Department of Computer Science and Engineering, University of California at San Diego, 1997.

[11] M. Bellare and B. Yee Forward Security in the Private Key Cryptography. In *Topics in Cryptography—CT-RSA 2003*, Lecture Notes In Computer Science, Vol. 2612, M. Joye ed., Springer Verlag, 2003.

[12] B. Yee Monotonicity and Partial Results Protection for Mobile Agents. Proceedings of the International Conference on Distributed Computing Systems, 2003.

[13] R. Evans, M. Minei, and B. Yee Incomplete higher order Gauss sums. To appear in the Journal of Mathematical Analysis and Applications, Elsevier Science.

[14] E. TSYRKLEVICH AND B. YEE Dynamic Detection and Prevention of Race Conditions in File Accesses. To appear in the 12th USENIX Security Symposium, 2003.

Technical Reports

[15] D. TYGAR AND B. YEE. Cryptography: it's not just for *electronic* mail anymore. Technical Report CMU-CS-93-107, Department of Computer Science, Carnegie Mellon University, March 1993.

[16] B. YEE. Using secure coprocessors. Ph.D. Thesis. Technical Report CMU-CS-94-149, Department of Computer Science, Carnegie Mellon University, May 1994.

[17] J. D. TYGAR, B. YEE, AND N. HEINTZE Cryptographic Postage Indicia. Technical Report CMU-CS-96-113, Department of Computer Science, Carnegie, Mellon University, January, 1996.

[18] M. BELLARE AND B. YEE. Forward integrity for secure audit logs. Technical Report CS98-580, Department of Computer Science and Engineering, University of California at San Diego, 1997.

[19] M. HOHLFELD AND B. YEE. How to migrate agents. Technical Report CS98-588, Department of Computer Science and Engineering, University of California at San Diego, 1998.

[20] M. BELLARE AND B. YEE. Forward Security in Private Key Cryptography. Technical Report 2001/035, International Association for Cryptologic Research eprint, 2001.

[21] M. HOHLFELD, A. OJHA, B. YEE Security in the Sanctuary System. Technical Report CS02-0731, Department of Comptuer Science and Engineering, University of California at San Diego, 2002.

Standards Documents

[22] J. BENALOH, B. LAMPSON, T. SPIES, D. SIMON, AND B. YEE. The PCT protocol. Microsoft Corp, 1995.

Students

Graduated students:

- Stephane Belmon. Joint work [9]. Co-advised with J. Pasquale. M.S. 1999.
- Edward Elliott. M.S. 2000.
- Eugene Tsyrklevich. M.S. 2002.
- Aditja Ojha. M.S. 2003.

Current Ph. D. / M.S. students:

- Genevieve Bartlett. (M.S.)
- Matthew Hohlfeld. (Ph.D.)
- Rahul Lahoti. (M.S.)
- Robert Miller. (M.S.)
- Scott O'Neil. (M.S.)

- Yekaterina Tsipenyuk. (M.S.) I supervised Ms. Tsipenyuk's work as a CalIT^2 fellow in summer 2002 as well as her current M.S. research.
- Poornaprajna Udupi. (M.S.)
- Juliana Wong. (M.S.)

Undergraduate students advised for project course. These students worked on a free implementation of a SSH client `FiSSH` for the Windows platform; it is widely used, and is being distributed from MIT at `http://pgpdist.mit.edu/FiSSH/index.html`.

- Douglas Mak.
- Timothy Chen.

Have also worked with the following who are either currently students or were students at the time of our joint work:

- Howard Gobioff, Carnegie Mellon University. Joint work [7].
- Michael Harkavy, Carnegie Mellon University. Joint work [8].

Invited presentations

1. The Dyad Project. Hong Kong University, 1993.
2. Using Secure Coprocessors. University of California at San Diego, 1995.
3. Using Secure Coprocessors. University of Texas at Austin, 1995.
4. Using Secure Coprocessors. New York University, 1995.
5. Using Secure Coprocessors. Columbia University, 1995.
6. Using Secure Coprocessors. Princeton University, 1995.
7. Using Secure Coprocessors. Massachusetts Institute of Technology, 1995.
8. Overview of Secure Coprocessors. DIMACS DREI'97: Cryptography and Network Security, Princeton, August 1997.
9. The Sanctuary Project. DIMACS DREI'97: Cryptography and Network Security, Princeton, August 1997.
10. Mobile Agents and Security. University of California at San Diego School of Engineering Research Review, February 1999.
11. Secure Coprocessors and Mobile Code. The JASON Group / MITRE, June 2000.
12. The Sanctuary System. National University of Singapore, Jan 2001.
13. Forward Secure Crypto for Mobile Code. National University of Singapore, July 2001.

Patents

- U. S. Patent 5,781,723. B. YEE AND J. BENALOH System and method for self-identifying a portable information device to a computing unit.
- Pending. UCSD Case Number SD 99-115. System and Method for Delivering and Examining Digital Tickets.