SRINIVAS INGUVA

---

Objective:
A challenging fulltime position involving the creative use of security and internet technologies.

---

Technical Expertise:
Java: Extensive development and architectural experience (including design patterns). Several years experience building enterprise applications using J2EE.
Security: Several years experience using Java security APIs (including JSSE and JAAS). Have worked with cryptographic toolkits including: Baltimore, RSA, OpenSSL.
Other coding skills: XML, SQL, C/C++, JavaScript, Jython, Perl, LDAP
Application Servers: Weblogic, iPlanet, Tomcat, Orion
Systems: Windows, Solaris

---

Education:
* Carnegie Mellon University - Pittsburgh, PA
B.S. in Mathematics/Computer Science, June 1996
* Stanford University - Palo Alto, CA
M.S. in Computer Science, Expected June 2006

---

Work Status:
U.S. Citizen

---

Experience:

Stanford University -- Masters Candidate
Palo Alto, CA
9/04 -
I'm currently enrolled in the Stanford Masters in Computer Science Program., specializing in computer security.

---

IONA Technologies (acquired Netfish Technologies May 2001) -- Technical Staff
Santa Clara, CA
3/99 - 8/04
Worked on various components of IONA's security platform, which provides authentication (including Single Sign On), access control, and PKI services for all IONA products. In particular, IONA's flagship CORBA product and web services integration products are secured using this technology. Our platform supports major security standards including SAML, XKMS, and XML-Signature.
Worked on the design and development of several components of Netfish's high-performance, 100% Java, B2B integration server, including:
* A security module, XDI Secure Gateway, which enables the deployment of a

B2B Server behind an opaque network firewall (disallowing all incoming TCP connections).
* A fine-grained role-based/discretionary access control system for the B2B Server, which is capable of handling complex runtime authentication checking.
* Implementation of a generalized transport layer supporting multiple protocols, including HTTP, FTP, SMTP.
* SSL support (using RSA J-Safe and later Sun JSSE libraries) for outbound messages. Worked with iPlanet, Apache, and IIS web servers.
* Digital signature and encryption support for use by other server components.
* Module for storing and accessing user and group data from an LDAP server. Developed and tested using iPlanet directory server.
Completed work on a new version of the Secure Gateway product, which is independent of the B2B Server. This is the only product on the market capable of supporting the deployment of web applications behind an opaque firewall.

---

Protocol-IT, LLC -- Lead Software Engineer (Pittsburgh, PA)
9/98 - 2/99
Worked on a mobile client/server application implemented in Java and Visual Basic.
Responsibilities included code updating/maintenance, identifying software performance issues as well as handling a large installation.

---

The MITRE Corporation -- Software Systems Engineer (Bedford, MA)
9/96 - 8/98
Worked in an internet technologies group.
Project work included:
* Developing a next generation phonebook application for the MITRE intranet using XML and Java technology.
* Helping design and implement an architecture that enhanced broadcast technology by decoupling the problems of information collection and dissemination.
* Developing database population tools, in Visual Basic and MS Access, for a web- based information service.

---

References available upon request

# Curriculum vitæ

**Hovav Shacham**

## Research Interests

Applied cryptography; systems security.

## Publications

*Thesis*

H. Shacham. *New Paradigms in Signature Schemes.* PhD thesis, Stanford University, Dec. 2005. Nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition.

*Journal papers*

H. Shacham, D. Boneh, and E. Rescorla. Client side caching for TLS. *ACM Trans. Info. & System Security*, 7(4):553–75, Nov. 2004. Standardized by the IETF as RFC 4507.

D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, Sept. 2004.

*Refereed papers, Security*

H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In B. Pfitzmann and P. Liu, eds., *Proceedings of CCS 2004*, pp. 298–307. ACM Press, Oct. 2004.

E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh. SiRiUS: Securing remote untrusted storage. In M. Tripunitara, ed., *Proceedings of NDSS 2003*, pp. 131–45. Internet Society (ISOC), Feb. 2003.

H. Shacham and D. Boneh. Fast-track session establishment for TLS. In M. Tripunitara, ed., *Proceedings of NDSS 2002*, pp. 195–202. Internet Society (ISOC), Feb. 2002. Extended abstract of journal paper above.

H. Shacham and D. Boneh. Improving SSL handshake performance via batching. In D. Naccache, ed., *Proceedings of CT-RSA 2001*, vol. 2020 of *LNCS*, pp. 28–43. Springer-Verlag, Apr. 2001.

*Refereed papers, Cryptography*

H. Shacham and B. Waters. Efficient ring signatures without random oracles. In T. Okamoto and X. Wang, eds., *Proceedings of PKC 2007*, LNCS. Springer-Verlag, Apr. 2007. To appear.

X. Boyen, H. Shacham, E. Shen, and B. Waters. Forward secure signatures with untrusted update. In R. Wright, ed., *Proceedings of CCS 2006*, pp. 191–200. ACM Press, Oct. 2006.

S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In S. Vaudenay, ed.,

*Proceedings of Eurocrypt 2006*, vol. 4004 of *LNCS*, pp. 465–85. Springer-Verlag, May 2006.

D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In B. Pfitzmann and P. Liu, eds., *Proceedings of CCS 2004*, pp. 168–77. ACM Press, Oct. 2004.

D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, ed., *Proceedings of Crypto 2004*, vol. 3152 of *LNCS*, pp. 41–55. Springer-Verlag, Aug. 2004.

A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. Sequential aggregate signatures from trapdoor permutations. In C. Cachin and J. Camenisch, eds., *Proceedings of Eurocrypt 2004*, vol. 3027 of *LNCS*, pp. 74–90. Springer-Verlag, May 2004.

D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In E. Biham, ed., *Proceedings of Eurocrypt 2003*, vol. 2656 of *LNCS*, pp. 416–32. Springer-Verlag, May 2003.

D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, ed., *Proceedings of Asiacrypt 2001*, vol. 2248 of *LNCS*, pp. 514–32. Springer-Verlag, Dec. 2001. Extended abstract of journal paper above.

*In Submission*

H. Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86), 2006. Submitted.

H. Shacham. A Cramer-Shoup encryption scheme from the Linear assumption, 2006. Submitted.

*Survey papers*

D. Boneh, C. Gentry, B. Lynn, and H. Shacham. A survey of two signature aggregation techniques. *RSA Cryptobytes*, 6(2):1–9, Summer 2003.

D. Boneh and H. Shacham. Fast variants of RSA. *RSA Cryptobytes*, 5(1):1–9, Winter/Spring 2002.

## Professional Activities

Invited Talks

Pairings in Cryptography Workshop 2005: "Implementing Pairing-Based Signature Schemes."
ECC 2004: "A New Life for Group Signatures," joint work with Dan Boneh and Xavier Boyen.

Journal Board

AIMS Advances in Mathematics of Communications.

PC Member

Eurocrypt 2008; ICDCS 2007 (Security area); ISPEC 2007; PKC 2007; Asiacrypt 2006; Crypto 2006; ACIS 2006; ACM AsiaCCS 2006; Asiacrypt 2005; WISA 2005; ISC 2004.

## Education

| | |
|---|---|
| 10/2005–Present | Weizmann Institute of Science, Faculty of Mathematics and Computer Science. Postdoctoral fellow, supported by a Koshland Scholars Program fellowship. Host: Moni Naor. |
| 9/2000–10/2005 | Stanford University, Department of Computer Science. Ph. D. in applied cryptography and systems security. Advisor: Dan Boneh. Thesis: *New Paradigms in Signature Schemes*, nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition |
| 1/1999–6/1999 | Stanford Program in Oxford. Tutorials in Shakespeare and textual criticism. |
| 9/1996–6/2000 | Stanford University. B. S. in computer science, with distinction and departmental honors; A. B. in English, with distinction. Honors thesis: "Accelerating SSL Performance in Software." |

## Teaching

| | |
|---|---|
| Spring 2006 | Lecturer, Pairings in Cryptography, Weizmann Institute of Science. Designed and taught semester-long graduate two-hour-per-week course at the Weizmann on the mathematics of pairings and the cryptographic systems based on them. Topics included: mathematical background through Weil Reciprocity and Miller's algorithm; identity-based encryption (IBE); constructions based on IBE and hierarchical IBE, with a focus on CCA-secure encryption schemes; digital signatures and their variants; and the composite-order setting. Course website: `http://crypto.stanford.edu/~hovav/pic/`. |
| Spring 2003, Spring 2002 | Teaching Assistant, CS 155: Computer and Network Security, Stanford. Assisted Profs. Boneh and Mitchell in designing an advanced-undergraduate course on computer and network security. Designed and implemented programming assignments now used at Stanford, UT Austin, Toronto, and Northwestern. |

## Awards

| | |
|---|---|
| 10/2006 | Runner up, Arthur L. Samuel Thesis Award, Stanford Department of Computer Science. |
| 8/2006 | Ph. D. thesis nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition. |
| 4/2006 | Koshland Scholars Program postdoctoral fellowship, Weizmann Institute. |
| 5/2000 | Frederick E. Terman Award for Scholastic Achievement in Engineering, Stanford University School of Engineering. |
| 10/1997 | President's Award for Academic Excellence in the Freshman Year, Stanford University. |