

Jonathan Herzog

2 Linbrook Rd., West Hartford CT 06107 • jherzog@jonathanherzog.com
Electronic version available at: <http://www.jonathanherzog.com>

Professional Experience

Principal Architect *2014 – Present* *Akamai Technologies*
Senior Architect
Architect

Internal advocate for security and system safety. Analyzed systems for technical risks and hazards; advised executives and developers regarding feasible remediations. Created and delivered ongoing company-wide training on hazard analysis and safety practices for complex systems.

Co-founder *2012 – 2021* *Amy Herzog Designs*

Engineering ‘half’ of two-person startup. Responsible for development and maintenance of profitable webapp from inception to sale. Use of test-driven development, CI/CD processes, and cloud-based deployment enabled single-person ‘team’ to develop new features while supporting 31K users.

Technical Staff *2009 – 2014* *MIT Lincoln Laboratory*

Analysis, development and standardization of group-keying protocols; security analysis of tactical communication systems; development of new cryptographic algorithms; empirical test and evaluation of privacy-preserving database systems. PI for two projects; software developer on three projects. Authored four conference publications and one IETF RFC. Organized 13-week course on all aspects of cyber security.

Consultant *2006 – 2009* *Jonathan Herzog Consulting*

Sample projects: evaluation of proprietary cryptographic algorithms; review of open-source cryptographic libraries; guidance with regard to use of security protocols.

Associate Professor, CS *2006 – 2008* *Naval Postgraduate School*

Teaching: Algorithms & data structures; programming languages & OOP (Java, Python, OCaml, Perl, Erlang, Ada, Prolog, and assorted development tools); cryptography & cryptographic protocols.

Cryptographer *1997 – 2006* *The MITRE Corporation*

Cryptographic analysis and development. Author of 18 conference and journal publications; developer on 2 software projects. Influenced standard for SSHv2; advised both NSA and Air Force. Proposed and managed three tasks with combined budget of \$600K and combined staff of 5 researchers.

Education

PhD	MIT	Computer Science	2002 – 2004
MS	MIT	Computer Science	2000 – 2002
BS	Harvey Mudd College	Mathematics	1993 – 1997

**Journal
Publications**

- [1] USING FOURIER TRANSFORMS TO UNDERSTAND SPECTRAL LINE SHAPES. *Journal of Chemical Education*, 72(3):210–214, 1995. Joint work with Ernest Grunwald and Colin Steel.
- [2] GENERALIZED k -MATCHES. *Statistics and Probability Letters*, 38:167–175, 1998. Joint work with Christopher McLaren and Anant Godbole.
- [3] STRAND SPACES: PROVING SECURITY PROTOCOLS CORRECT. *Journal of Computer Security*, 7(2/3):191–230, 1999. Joint work with F. Javier Thayer and Joshua D. Guttman.
- [4] A COMPUTATIONAL INTERPRETATION OF DOLEV-YAO ADVERSARIES. *Theoretical Computer Science*, 340:57–81, June 2005.
- [5] SOUNDNESS AND COMPLETENESS OF FORMAL ENCRYPTION: THE CASES OF KEY-CYCLES AND PARTIAL INFORMATION LEAKAGE. *Journal of Computer Security*, 17(5):773–797, 2009. Joint work with Pedro Adão, Gergei Bana, and Andrej Secdrov.
- [6] UNIVERSALLY COMPOSABLE SYMBOLIC SECURITY ANALYSIS. *Journal of Cryptology*, 24(1):83–147, 2011. Joint work with Ran Canetti.
- [7] AUTOMATED ASSESSMENT OF SECURE SEARCH SYSTEMS. *ACM SIGOPS Operating Systems Review*, 49(1):22–30, January 2015. Joint work with Mayank Varia, Benjamin Price, Nicholas Hwang, Ariel Hamlin, Jill Poland, Michael Reschly, Sophia Yakoubov, and Robert K. Cunningham.

**Conference
Publications**

- [1] STRAND SPACES: WHY IS A SECURITY PROTOCOL CORRECT?. In: *1998 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, May 1998. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
- [2] HONEST IDEALS ON STRAND SPACES. In: *Proceedings of the 11th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1998. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
- [3] STRAND SPACE PICTURES. In: *Proceedings, Workshop on Formal Methods and Security Protocols*, June 1998. Co-located with LICS’98. Joint work with F. Javier Thayer Fabrega and Joshua D. Guttman.
- [4] MIXED STRAND SPACES. In: *Proceedings of the 12th IEEE Computer Security Foundations Workshop*. IEEE Computer Society Press, June 1999. Joint work with F. Javier THAYER Fábrega and Joshua D. Guttman.
- [5] THE DIFFIE-HELLMAN KEY-AGREEMENT SCHEME IN THE STRAND-SPACE MODEL. In: *16th Computer Security Foundations Workshop*, pages 234–247, Asilomar, CA, June 2003. IEEE CS Press.
- [6] A COMPUTATIONAL INTERPRETATION OF DOLEV-YAO ADVERSARIES. In: Roberto Gorrieri, editor, *Proceedings, Workshop on Issues in the Theory of Security (WITS’03)*, pages 146–155, April 2003. Co-located with ETAPS 2003.
- [7] PLAINTEXT AWARENESS VIA KEY REGISTRATION. In: Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 548–564. Springer-Verlag, August 2003. Joint work with Moses Liskov and Silvio Micali.
- [8] TRUST MANAGEMENT IN STRAND SPACES: A RELY-GUARANTEE METHOD. In: David Schmidt, editor, *Programming Languages and Systems: 13th European Symposium on Programming*, number 2986 in LNCS, pages 325–339. Springer, 2004. Joint work with Joshua D. Guttman, F. Javier Thayer, Jay A. Carlson, John D. Ramsdell, and Brian T. Sniffen.

- [9] PROGRAMMING CRYPTOGRAPHIC PROTOCOLS. In: Rocco Nicola and Davide Sangiorgi, editors, *Trustworthy Global Computing (TGC 2005)*, volume 3702 of *Lecture Notes in Computer Science*, pages 116–145. Springer-Verlag GmbH, April 2005. Joint work with Joshua D. Guttman, John D. Ramsdell, and Brian T. Sniffen.
- [10] SOUNDNESS OF ABADI-ROGAWAY LOGICS IN THE PRESENCE OF KEY-CYCLES. In: *Proceedings of the 10th European Symposium On Research In Computer Security (ESORICS 2005)*. Springer, September 2005. Joint work with Pedro Adao, Gergei Bana, and Andre Scedrov.
- [11] UNIVERSALLY COMPOSABLE SYMBOLIC ANALYSIS OF MUTUAL AUTHENTICATION AND KEY EXCHANGE PROTOCOLS. In: *Proceedings, Theory of Cryptography Conference (TCC)*, March 2006. Joint work with Ran Canetti.
- [12] ROBBING THE BANK WITH A THEOREM PROVER (ABSTRACT). In: *Security Protocols Workshop*, volume 5964 of *Lecture Notes in Computer Science*, page 17. Springer, 2007. Joint work with Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ronald L. Rivest, and Ross Anderson.
- [13] ON THE ROBUSTNESS OF COGNITIVE NETWORKING MECHANISMS TO MALICIOUS INSIDERS. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Joint work with Gabriel Wachman and Dan Liu.
- [14] A COMPREHENSIVE KEY MANAGEMENT ARCHITECTURE FOR SMALL UNMANNED AIRCRAFT SYSTEMS AND OTHER TACTICAL APPLICATIONS. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Distribution authorized to U.S. Government agencies and their contractors. Joint work with Roger Khazan, Adam Petcher, and Daniil Utin.
- [15] USABLE IDENTITY MANAGEMENT FORTACTICAL DEVICES. In: *Proceedings, Military Communications Conference (MILCOM 2011)*. IEEE Communications Society, November 2011. Distribution authorized to U.S. Government agencies and their contractors. Joint work with Sophia Yuditskaya and Roger Khazan.
- [16] A TEST-SUITE GENERATOR FOR DATABASE SYSTEMS. In: *High Performance Extreme Computing Conference (HPEC)*, pages 1–6. IEEE, September 2014. Joint work with Ariel Hamlin.

Standards

- [1] USE OF STATIC-STATIC ELLIPTIC CURVE DIFFIE-HELLMAN KEY AGREEMENT IN CRYPTOGRAPHIC MESSAGE SYNTAX. Request For Comments (RFC) 6278, June 2011. Joint work with Roger Khazan.

Technical Reports

- [1] FORMAL METHODS APPLIED TO SPACECRAFT SUBSYSTEMS. Technical report, Harvey Mudd College, 1997. Joint work with Erin Conley and Everett Bull.
- [2] A COMPARISON OF CERTIFICATE VALIDATION METHODS FOR USE IN A WEB ENVIRONMENT. MITRE Technical Report MTR98B0000093, The MITRE Corporation, November 1998. Joint work with Shimshon Berkovitz.
- [3] A STRAND SPACE ANALYSIS OF THE SSH VERSION 2 PROTOCOL. MITRE Product MP98B0000056, The MITRE Corporation, January 1999. Joint work with Joshua D. Guttman and Fred Chase.
- [4] A SAYING-LOGIC ANALYSIS OF CORE DNS SECURITY. MITRE Product MP99B0000039, The MITRE Corporation, 1999. Joint work with Fred Chase and Joshua D. Guttman.
- [5] THE SECURE DNS PROTOCOLS. MITRE Product MP99B0000035, The MITRE Corporation, July 1999. Joint work with Fred Chase.
- [6] SOME SECURITY CONCERNS REGARDING PPP-EAP-TLS. MITRE Product MP00B0000019, The MITRE Corporation, August 2000.

- [7] A STRAND-SPACE ANALYSIS OF TLS 1.0. MITRE Technical Report MTR 0B00000110, The MITRE Corporation, July 2000. Joint work with Laura Feinstein and Joshua D. Guttman.
- [8] MOBILE IP SECURITY. MITRE Product MP00B063, The MITRE Corporation, November 2000.
- [9] SECURE INTERNET PROTOCOL ANALYSIS CONCLUSIONS. MITRE Product MP 01B0000054, The MITRE Corporation, August 2001.
- [10] UNIVERSALLY COMPOSABLE SYMBOLIC ANALYSIS OF CRYPTOGRAPHIC PROTOCOLS (THE CASE OF ENCRYPTION-BASED MUTUAL AUTHENTICATION AND KEY EXCHANGE). Cryptology ePrint Archive, Report 2004/334, 2004. Joint work with Ran Canetti.
- [11] ROBBING THE BANK WITH A THEOREM PROVER. Technical report, University of Cambridge Computer Laboratory, August 2005. Joint work with Paul Youn, Ben Adida, Mike Bond, Jolyon Clulow, Amerson Lin, Ronald L. Rivest, and Ross Anderson.
- [12] IMPLEMENTING AES ON THE CELLBE. Technical Report NPS-MA-09-001, Naval Postgraduate School, Monterey, CA, January 2009. Joint work with David Canright, George Dinolt, Simson Garfinkel, and Bruce Allen.
- [13] USING ATTESTATION TO LIFT CRASH RESILIENCE TO BYZANTINE RESILIENCE. MITRE technical report, The MITRE Corporation, 2009. Joint work with Jonathan Millen, Brian O’Hanlon, John D. Ramsdell, and Ariel Segall.
- [14] SMALL UNMANNED AIRCRAFT SYSTEMS: KEY MANAGEMENT ARCHITECTURE. Technical report, MIT Lincoln Laboratory, Lexington, MA, August 2011. Joint work with Roger Khazan, Sean O’Melia, Adam Petcher, and Dan Utin.

Theses

- | | |
|-----|---|
| MS | COMPUTATIONAL SOUNDNESS FOR FORMAL ADVERSARIES. Massachusetts Institute of Technology, October 2002. |
| PhD | COMPUTATIONAL SOUNDNESS FOR STANDARD ASSUMPTIONS OF FORMAL CRYPTOGRAPHY. Massachusetts Institute of Technology, May 2004. |
-

Technologies

- | | |
|-----------|--|
| Languages | Ada, C, Erlang, Java, MATLAB, OCaml, Prolog, Python |
| Tools | IDEs, source-control systems, unit-test frameworks, build systems, documentation generators, profilers & debuggers, parser/lexer generators, <i>etc.</i> |
| Other | LaTeX, general-purpose formal-methods tools (SPIN, FDR, Otter, Isabelle, Coq, <i>etc.</i>), cryptographic formal-methods tools (CryptoVerif, EasyCrypt), web frameworks (Django, Pelican), cloud services |
-

Software

CustomFit: Web application to generate custom knitting patterns from user’s measurements and swatch. Written in Python & Django, deployed onto Heroku and AWS. Supported over 30K users.

CPPL: the Cryptographic Protocol Programming Language. A domain-specific language for cryptographic protocols, with associated compiler, built on top of strand spaces and logical programming. Uses external libraries for automated reasoning (Datalog) and cryptographic operations (OpenSSL). Compiler implemented in OCaml.

CPSA: the Cryptographic Protocol Shape Analyzer. An automated analysis tool for security protocols. Efficiently explores possible protocol executions; automatically de-

tests and reports possible attacks. (Distribution limited to government agencies and contractors.) Implemented in OCaml.

AES-GCM on CellBE: Parallelized C implementation of NIST-standardized encryption algorithm (AES-GMC) on newly-introduced architecture (IBM CellBE). Achieved speeds of 10Gb/sec for plain AES, 1Gb/sec for AES-GCM.

Unnamed test-suite generator: Stand-alone application for generating test-suites for databases. Written in Python. Produces synthetic (yet realistic) data, ‘interesting’ queries over that data, and ground-truth answers for each query. Execution is unpredictable to database under test, but completely repeatable for experimental reproducibility. Parallelized and heavily optimized: generates 120GB per core-hour.

AES variant generator: Generates secure random variants of the Advanced Encryption Standard in VHDL.

Awards

IEEE	IEEE Golden Core Award, Meritorious Service Award, Outstanding Community Service Award (twice)
The MITRE Corporation	MITRE Best Paper Award, Program Innovation Award, Program Recognition Award, Spot Award
Harvey Mudd College	High honors, departmental honors
Other	R&D 100 Award, Wikipedia citations: 1, Putnam score: 13