Michael L. Wenocur
Cryptographic Engineer
650-799-9796
mwenocur@acm.org
4057 Amaranta Ave
Palo Alto, CA 94306

Summary

- Designed and implemented leading edge cryptographic infrastructure for award winning software systems.
- Knack for solving difficult data security problems by clever use of crypto primitives.
- Intimate understanding of cryptographic protocols, primitives and Public Key Infrastucture.
- Solved hard, practical problems using statistical estimation, data analysis, and probability theory.
- Performance analysis using queueing theory and Monte Carlo simulation.
- Skilled at writing robust code for highly optimized, sophisticated mathematical computations.

Languages: Python, C, C++, Java, R.

Education

Ph.D. Mathematical Statistics, Stanford University (1983).
M.S. Computer Science, Stanford University Honors Coop Program (1988).
B.Sc. Mathematics, Tel Aviv University (1975).

Experience

12/2013-Present: Consultant

- Terradyne: Consulted on data privacy problem.
- Think Big Analytics: Provided expert analysis of the appropriateness and correctness of statistical analysis routines used in an automated HR application written in Java.
- Ongoing work with a start-up in the pharmaceutical retail space.
    - Designed a system to provide digital security and privacy while enabling users to backup on-line with full security.
    - Conducted drug price research and customer survey.

2/2013-11/2013: Pertino Inc: Cryptographic Engineer

Designed and coded cutting edge Public Key Infrastructure (PKI) and TLS ecosystem based on Elliptic Curve Cryptography (ECC) for Linux and Windows featuring:

- Automated certificate and key pair provisioning via WSDL calls to a registration authority.
- Rapid turnover of keys and certificates to minimize key vulnerabilities.
- Increasing certificate trustworthiness by countersigning new certificate requests with expiring keys.

In addition cryptographic strength is enhanced by restricting all full handshakes to using ephemeral keys in ECDSA-ECDHE mode or, for backwards compatibility with RSA based certificate systems, RSA-ECDHE mode.

Technologies: C++, Java, Python, Eclipse, MSVC 10, Git, GitHub.
Cryptography: OpenSSL on Windows and Linux, M2Crypto for Python servers, BouncyCastle for Java

servers, EJBCA PKI by PrimeKey for registering and revoking certificates over an SSH channel.

2/2012-2/2013: Symantec Trust Services Division: Principal Engineer

- Developed analytic model of ECC-based TLS client-server handshake performance. Extracted and cleaned data from Wireshark for data analysis. Constructed visual simulator using JMT toolkit.
- Analyzed cryptographic speed/security tradeoffs for RSA vs. ECC.
- Extended cryptographic infrastructure to generate FIPS 186-3 DSA data and signatures.
- Wrote technical memos describing RSA key generation best practices and weak key checking.
- Designed and prototyped Python based system to test RSA public key factorability against all accessible RSA public keys.
- *Technologies*: C, C++, Python, Java, MSVC, Wireshark, Eclipse, Windows 7, Linux, CVS.
- *Cryptography*: BSAFE library, BouncyCastle, Verisign proprietary certificate signing server.

1/2009-2/2012: Cryptographic Consultant

- Developed FIPS 140 accredited cryptographic module supporting NSA Suite B requirements based on LibTomCrypt. Module enforced key usage and role-based data access constraints.
- Designed method for remotely managing distributed apps with decentralized access control utilizing ephemeral PKI.
- Coded certified modules for ECC fully unified key-exchange, FIPS random number generation, etc.
- Co-authored security white papers.
- *Technologies*: C++, Python, MSVC.
- *Cryptography*: LibTomCrypt, FIPS crypto standards, proprietary script based testing module.

1/2005-12/2008 DartDevices: Data Security Designer and Cryptographic Engineer

- Researched and implemented lightweight, cryptographic library and SSL-like protocol.
- Designed and coded an integrity protected, encrypted file system featuring random access and permissions specific to application instances.
- *Technologies*: C, C++, Python, MSVC, CVS.
- *Cryptography*: Proprietary library with script-based test facility.

1/2003-1/2005: Cryptographic Consultant

- DartDevices: Provided cryptographic design guidance.
- Confirmix: Designed and implemented a prototype proxy-based architecture in Python for digitally signing electronic documents. Security was enhanced by using rapidly expiring keys and certificates and logging user history.
- *Technologies*: Python, C, MSVC, wxpython and numerous Python extension libraries.
- *Cryptography*: Python based cryptographic library.

5/2000-12/2002: Gemstar/Storymail: Cryptographic/Security Engineer

- Automated data extraction in Python from email-based marketing campaign.
- Designed and coded ultra-light cryptographic toolkit.
- Implemented and helped design S3L, a lightweight fully symmetric SSL-like protocol.
- *Technologies*: C, C++, Python, MSVC, CVS.

- *Cryptography*: Storymail cryptographic library.

2/1999-5/2000: Stamps.com: Staff Scientist and Lead Cryptographic Engineer

- Implemented most of the base client cryptographic code. Finished 3 weeks ahead of schedule.
- Implemented cryptographic protocol to shuttle data between servers and IBM 4758/Rainbow cryptocards.
- *Technologies*: C, C++, MSVC.
- *Cryptography*: Microsoft CryptoAPI, IBM cryptographic card emulator, IBM 4758 cryptocard, Rainbow cryptocards, Stamps.com proprietary code.

12/1994-2/1999; RSA Data Security: BSAFE Crypto-C Technical Lead

- Key Contributor to the award-winning BSAFE 3.0 cryptographic library.
- Technical Lead for BSAFE 4.0 completed in a highly compressed schedule.
- *Technologies*: C, MSVC.
- *Cryptography*: BSAFE 3.0 and 4.0, ASN-1, Btest scripting library, RSA, DSA, DH, ECC, etc.

Patents and Publications

- Co-inventor listed in nine patent applications wherein I contributed novel certificate structures, automated certificate provisioning, application data compromise protections, fully symmetric SSL-like protocol, etc.
- List of ten papers available on request.

Certifications

Nine Coursera Certificates including eight from Johns Hopkins' Data Science program.