Mike Hamburg

Researcher / Engineer at Cryptography Research, Inc.

San Francisco, California | Computer & Network Security

227 connections

Current	Cryptography Research, Inc.
Previous	Stanford University, Google, Facebook
Education	Stanford University

Summary

I'm a talented, mathematically inclined computer scientist. Most of my experience is in cryptography, embedded systems, and hardware/software/infrastructure codesign. I've also done my share of coding, particularly at Ellington where I wrote an automated trading platform.

Since I earned a PhD and worked at more than half a dozen internships (not all shown), I've designed and prototyped many systems, but I've productized and maintained only a few. This could be an interesting area of growth for my next stage of professional development.

- Proficient in C, C++, Python, Haskell, Perl, x86/AMD64 and ARM/NEON assembly.
- Experience in Java, Objective-C, System Verilog, HTML, Javascript, PHP, Standard ML, O'CaML.
- Cryptographic system design and implementation, from architecture down to math routines.
- Compiler design and implementation.
- Concurrent and parallel systems, with locks, channels, shared memory, transactional memory.
- Strong math background, especially in discrete math (algebra, number theory, combinatorics).
- Experience with real and complex analysis with applications in signal processing.

Experience

Researcher / Engineer

Cryptography Research, Inc.

September 2011 – Present (6 years 6 months)

Architecture and prototyping for several projects. Security, usage model and threat model analysis. Independent security reviews for several customers. Software engineering and debugging support. C, C++, Python, Perl, Haskell, Verilog/SystemVerilog/VP3, assembly, design of special purpose asm and higher-level languages.

PhD Student

Stanford University

2006 – 2011 (5 years)

Cryptography. I also TA'd a class on optimizing compilers.

This would just be in education, but I wanted to add colleagues from my PhD research.

Engineering intern

Google

June 2010 – August 2010 (3 months)

Cryptography in the browser. C++.

Engineering intern
Facebook
June 2009 – August 2009 (3 months)

Designing and implementing spam-fighting tools. C/C++, PHP.

Engineering intern
Apple
June 2008 – August 2008 (3 months)

Product security group. Mostly just a coder. Scripting languages: PHP, Perl.

Engineering intern
Ellington Management Group
June 2006 – August 2006 (3 months)

Designed and coded (most of) an automated trading platform. Java.

Engineering intern
Microsoft
June 2005 – August 2005 (3 months)

Working on filesystem encryption. Some C coding.

Web Developer
Memorial Hospital
June 2003 – August 2003 (3 months)

Writing and maintaining internal web pages. ASP, MSSQL.

Education

Stanford University
PhD, Cryptography
2006 – 2011

Activities and Societies: RUF, SGS

Harvard University
AB, Mathematics and Computer Science
2002 – 2006

Activities and Societies: HRSFA

Volunteer Experience & Causes

Causes Mike cares about:
Civil Rights and Social Action
Economic Empowerment
Education
Environment
Human Rights
Disaster and Humanitarian Relief
Poverty Alleviation

Skills

Cryptography | Security | Embedded Systems | C | C++ | Haskell | Sage math | Python | Multithreaded Development | Digital Circuit Design | Software Engineering | Perl | Programming | Debugging | Linux | Distributed Systems | Algorithms | Software Development

Courses

Stanford University

- Optimizing compilers (TA)
- Cryptography seminar
- Advanced algorithms
- Parallel programming
- Cryptography (TA)
- Computer Security (TA)

Harvard University

- Real Analysis, Topology and Linear Algebra (Math 55)
- Operating Systems
- Complexity Theory
- Randomized Algorithms
- Networking Algorithms
- Peer-to-peer networks
- Cryptography
- Research topics in concurrent programming
- Algebraic number theory
- Algebraic combinatorics
- Graduate commutative algebra
- Combinatorial game theory
- Complex analysis
- Computer Hardware
- Databases
- XML query languages and databases
- Programming languages
- Advanced compiler design

Languages

French

Elementary proficiency

Projects

Ed448-Goldilocks

2014 – 2014

New elliptic curve for bright and glorious future.

Team members: Mike Hamburg

Publications

Elligator: Elliptic-curve points indistinguishable from uniform random strings

ACM/CCS

2013

Two ways to map field elements to even-order elliptic curves over a prime field.

Authors: Dan Bernstein, Mike Hamburg, Anna Krasnova, Tanja Lange

Fast and Compact Elliptic Curve Cryptography
Just an ePrint
May 2012

Montgomery curves over Montgomery fields
Authors: Mike Hamburg

Spatial Encryption
Stanford PhD Thesis
July 2011

Framework for building functional encryption systems with compact ciphertext, by encoding roles and encryption policies to subspaces of an N-dimensional vector space.
Authors: Mike Hamburg

Location privacy via private proximity testing
NDSS
2011

Dan Boneh asked if such a protocol was possible as a random question during a crypto class. I figured out how to do it. Six months later, Arvind et al needed it in a paper.
Authors: Arvind Narayanan, Narendan Thiagarajan, Mugdha Lakhani, Mike Hamburg, Dan Boneh

OpenConflict: preventing real-time map hacks in online games
IEEE SSP (aka Oakland)
2011

A neat trick to prevent map-hacking. Of course, no RTS designer would ever rewrite their network code for something like this, but that's why it's academia.
Authors: Elie Bursztein, Mike Hamburg, Jocelyn Lagarenne, Dan Boneh

The case for ubiquitous transport-level encryption
Usenix Security
2010

Opportunistic encryption of TCP packets. I wrote the security proof, eliminating a security bug or two on the way.
Authors: Andrea Bittau, Mike Hamburg, Mark Handley, David Mazières, Dan Boneh

Symmetric Cryptography in Javascript
ACSAC
2009

Not that you would, but you could.
Authors: Emily Stark, Mike Hamburg, Dan Boneh

Circular-secure encryption from decision Diffie-Hellman
CRYPTO
2008

A completely theoretical solution to a completely theoretical problem.
Authors: Dan Boneh, Shai Halevi, Mike Hamburg, Rafail Ostrovsky

Generalized Identity-Based and Broadcast Encryption Schemes
ASIACRYPT
2008

The paper which eventually became my thesis.
Authors: Dan Boneh, Mike Hamburg

Space-efficient identity-based encryption without pairings

FOCS

2007

Best paper award. We hoped that this would open up ground for new research in crypto, but unfortunately most of the follow-on work I've seen is completely insecure techniques to make it faster.

Authors: Dan Boneh, Craig Gentry, Mike Hamburg