

ERSIN UZUN

School of Information and Computer Science
University of California, Irvine 92697-3430
<http://www.ics.uci.edu/~euzun/>
euzun@ics.uci.edu
(949) 335 2235

Objective:

A research internship in security and privacy or a related topic.

Education:

2006 – Present

[University of California, Irvine](#)
[School of Information and Computer Sciences](#)
PhD in Networked Systems

G.P.A.: 3.99/4.00

Related Courses: Cryptography & Computer Security, Computer & Network Security, Group Communication Security, Advanced Networks, Computational Complexity, Ubiquitous Computer Interaction, Quantitative Research Methods.

2004 – 2006

[University of California, Irvine](#)
[School of Information and Computer Sciences](#)
M.S. in Networked Systems

G.P.A.: 3.98/4.00

Related Courses: Computer Networks, Internet Technology, Database Management Systems, Fault Tolerant Computing, Network Optimization, Data Compression, Distributed Computer System.

1999 - 2004

[Bilkent University](#), Ankara
BS in Computer Science and Engineering

Related Courses: Operating Systems, Algorithms and Data Structures, Introduction to Probability, Statistics for Computer Science, Automata Theory and Formal Languages, Network Security.

Research Experiences:

Research Assistant, [University of California Irvine](#), California, September 04 - now

- Research Topics: computer and communication security, privacy, usability and usable security.

Visiting Researcher, [INRIA](#), Rhone-Alpes, France, September 07 – December 07

- Designed and developed a new transient authentication based method to stop outgoing spam in enterprise networks.
- Worked on improving the pair wise communication security in multi-stage sensor networks.

Intern Research Engineer, [Nokia Research Center](#), Helsinki, Finland, June 06 – December 06

- Analyzed the Security and usability of secure pairing methods under standardization process and researched on new user interaction models, secure pairing methods and improvements over the standards.
- Designed and developed an open-source test framework for comparative usability analysis of distributed security applications.
- Did feasibility research in using ID-Based Cryptography to secure DTN communications.

Other Experiences:

Teaching Assistant, [University of California Irvine](#), California, September 04 – April 06

- Assisted faculty in various teaching responsibilities including active classroom teaching and individual tutoring, preparation of the course material and grading.
- Assisted Courses include Distributed Systems, Network Security and Cryptography, Data Structures and Algorithms, Introduction to Computer Organization

Summer Intern, [Garanti Technology T.A.S.](#), Istanbul, Turkey, July 02 - September 02

- Designed and implemented software to standardize the client mailboxes on Microsoft Exchange Server 5.5 for migration compatibility.
- Worked in a team that administered enterprise network infrastructure.

Part Time Network Administrator, [Bilkent Computer Center](#), Ankara, Turkey, September 01 - June 02

- Administered the network in computer center labs.

Testing & Employee Training Coordinator, [Ericsson](#), Istanbul, Turkey, June 00 - September 00

- Testing the E-Forms system for full deployment.
- Coordinating and instructing the employee training sessions for the new system.

IT Deployment Technician, Ericsson, Istanbul, Turkey, June 99 - September 99

- Worked in standardizing the site hardware and software for worldwide compatibility under the specifications of Ericsson Worldwide Standard Office Environment project.
- Set up of the VPN based inter-site secure communication channels.

Publications:

- Claude Castelluccia, Ersin Uzun, "SUSTAIN: Stopping Outgoing Spam using Transient Authentication", Manuscript Under Preparation
- Claudio Soriente, Gene Tsudik, Ersin Uzun, "Secure Pairing of Interface constrained Devices", to appear in [International Journal on Security and Networks](#), Vol.4 No.1, 2009.
- Michael T. Goodrich, Michael Sirivianos, John Solis, Claudio Soriente, Gene Tsudik, Ersin Uzun, "Using Audio in Secure Device Pairing", to appear in [International Journal on Security and Networks](#), Vol.4 No.1, 2009.
- Claudio Soriente, Gene Tsudik, Ersin Uzun. "BEDA: Button Enabled Device Pairing", [International Workshop on Security for Spontaneous Interaction \(IWSSI 2007\)](#) and [UBICOMP 2007](#) workshop proceedings.
- Claudio Soriente, Gene Tsudik, Ersin Uzun. "HAPADEP: Human-Assisted Pure Audio (Secure) Device Pairing" Under Submission.(Available as [E-Print Report 2007/093](#))
- Kari Kostiaainen, Ersin Uzun, "Framework for Comparative Usability Testing of Distributed Applications", [extended abstract in Security User Studies: Methodologies and Best Practices Workshop in CHI'07](#). ([Technical Report](#), Nokia Research 2007)
- Ersin Uzun, Kristiina Karvonen, N. Asokan, "Usability Analysis of Secure Pairing Methods", [USEC'07](#) . ([Technical Report](#), Nokia Research 2007).
- Michael T. Goodrich, Michael Sirivianos, John Solis, Gene Tsudik, Ersin Uzun, "Loud And Clear: Human-Verifiable Authentication Based on Audio", [IEEE ICDCS'06](#).
- A.A. Selçuk, E. Uzun, M.R. Pariente, "A Reputation based Trust Management System for P2P networks", [IEEE/ACM CCGRID 2004](#). ([Technical Report](#), Bilkent University 2004), ([Extended Journal version](#) is to appear in [International Journal of Network Security](#), Vol.6, No.3, PP.235-245)

Computer Skills:

Java, C++, PHP, SQL, Pascal, Fortran, LISP, HTML, Verilog, x86 Assembly, MIPS Assembly, Windows 98&2K&XP&2003 server, Linux, Unix, MS-DOS, Xilinx

Sample Unpublished Projects:

- Developing an open-source [usability testing framework](#) for distributed applications.
- Developing and emulating a DDOS and IP spoofing resistant network architecture: [SANALDA](#)
- [Survey Report](#) on group key distribution schemes for secure multicast in mobile ad-hoc networks.
- [Report](#) on MPEG-4 ALS and comparison of lossless audio compression products.
- Limiting some system calls of the Linux kernel to signed binaries only - with C
- Implementing a differential cryptanalysis attack on the FEAL-8 cipher - with C.
- Peer-to-Peer Network Simulator (to use in P2P researches) - with JAVA.
- Addition of inter process&thread communication and process synchronization to [GeekOS](#) - with C.
- Online Turkish Interactive Movie Database - with PHP & MSSQL
- Mail client & HTTP server - with JAVA
- Animation creation program - with JAVA and GL4JAVA
- Parser and interpreter for a predicate calculus language - with Yacc and Lex
- Multiplayer Mission Risk Game over TCP/IP - with JAVA
- Interactive English Learning & practice program - with JAVA
- MIPS like processor simulator - with Verilog

Academic Fellowships & Awards:

- Multi-year fellowship awarded by UCI
- Academic success scholarship awarded by Bilkent University.
- Certificate of Excellence awarded by Golden Key International Honor Society.
- 7 Academic High Honor Student Certificates awarded by Bilkent University.