MANISH MEHTA *M.S., CISSP, PH.D.*

1405 Marshall St. # 408, Redwood City, CA 94063 ▪ (816) 616-6699 ▪ jobs@manishmehta.com

Objective

Seeking a challenging opportunity in Network Security and Cryptography field.

Profile

- Extensive knowledge and experience with Networking protocols, Internet security paradigms, Application Security, and Cryptography.
- Several research papers in prestigious research Journals and Conferences.
- 7+ years of research and teaching experience in network security related fields.
- Certified Information Systems Security Professional (CISSP)
- Ph.D. in Computer Science at UMKC with Network Security and Cryptography concentration.
- Recipient of several honors for outstanding academic and research records.
- Excellent interpersonal, written communication, and verbal communication skills.

Skills

Protocols:	TCP/IP suite, OCSP, SMTP, HTTP, OSPF, BGP 4, IGRP, RTP, H.323 suite.
Security:	Web Application Security, PKI, IPSec, VPN, SSL/TLS, SSH, RSA, ECC, Diffie-Hellman, PGP.
Tools:	OPNET, CSIM, CPLEX, Maple, Matlab.
Platforms:	Linux, Unix, Windows 9x/NT/2000/XP.
Languages:	C, C++, Java, Assembly x86, Perl, Shell Scripting.
Web:	PHP, JavaScript, JDBC, RMI
Certificate:	CISSP, Java programming.

Education

- **Ph.D. in Computer Science**, Sept. 2006, University of Missouri – Kansas City, USA.
  GPA: 4.0 / 4.0.
  Research interests: Network security/Cryptography, Application Security, Protocols, Software Engineering.
- **M.S. in Computer Science**, May 2002, University of Missouri – Kansas City, USA.
  GPA: 3.93 / 4.0
- **B.E. in Computer Engineering,** May 1999. University of Mumbai, India.
  GPA : 4.0 / 4.0

Experience

Sr. Software Engineer II, Tumbleweed Comm., Redwood City. (Oct. 2006 – Present)
Design and development of Digital Certificate Validation suite in mainly C++ on Windows, Linux, and Solaris platforms. Key contributor to FIPS 140-2 certification for the crypto module of the software suite.

Security Research Consultant, Fishnet Security, Kansas City. (Mar. 2005 – Dec. 2005)
Consultant for all aspects of network and applications security issues. Performed a number of network and web application security assessment. Research and development of security tools.

Instructor, UMKC (Jan. 2001 – May 2005)
Teaching courses covering all aspects of networking, system and network administration, and network security to undergraduate students with senior standing. Building network security labs for hands-on training.

Graduate Intern, Saint Luke's Hospital, Kansas City (May 2001 – Dec. 2001)
Single-handedly designed and developed a protocol for secure transfer of healthcare data.

Visiting Lecturer, University of Mumbai, India. (Jul. 1999 – Dec. 1999)
Conducted Classes and Practical Lab sessions for course Computer Methodology and Algorithms.

Systems Engineer, Salinkar Consultants, Mumbai, India. (Jun. 1997 – May 1999)
Setup, Maintenance and Troubleshooting of Computer Networks. Installation and maintenance of Network Operating Systems and Network Software.

Major Projects

FIPS 140-2 Certification
Key Contributor, Tumbleweed Communications, Redwood City (Oct. 2006 – Present)
Prepared the crypto module of Digital Certificate Validation suite to meet FIPS 140-2 certification requirements and managed the module during the certification process.

Secure Data Transfer Protocol
Project Leader, Saint Luke's Hospital, Kansas City (May 2001 – Dec. 2001)
Designed and Implemented a proprietary protocol for secure data transfer between two networks. Also developed a Digital Certificate Server to manage the Certificates required for authentication. Implemented a Proxy server to deal with firewall and NAT.

Secure BINGO Game Project
Project Leader, UMKC (Sep. 2000 – Dec. 2000)
A secure multiplayer online game implemented in Java, involving Cryptographic Commitment for secure communication. Project was developed to highlight the security related problems in online gaming.

Presentations

Web Application Security, UMKC (Feb. 2006)
Presented various security aspects of web applications, demonstrated a number of real-life attacks, and discussed future research opportunities in the field.

Authentication and Key Establishment, UMKC (Apr. 2004)
Presented the solution to authentication and key establishment problem in Wired, wireless, and sensor environment.

Intrusion Detection, UMKC (Feb. - May 2003)
A series of presentations on various aspects of Practical Intrusion Detection.

IPSec, VPN and Key Management in the Internet, UMKC (Apr. 2001)
Basics of Internet Protocol and need for IPSec, IPSec Architecture. Illustrated IPSec modes, Virtual Private Networking, IKE architecture, ISAKMP framework, IKE key exchanges.

Selected Publications

- Huang, D.; Mehta, M.; Van de Liefvoort, A.; Medhi, D., *Modeling Pairwise Key Establishment for Random Key Predistribution in Large-Scale Sensor Networks*, IEEE/ACM Transactions on Networking, Oct. 2007.
- Mehta M., Harn L., *Efficient One-time Proxy Signatures*, IEE proceedings of Communications, 2005.
- Harn L., Mehta M., Hsin W., *Integrating Diffie-Hellman Key Exchange into the Digital Signature Algorithm (DSA)*, IEEE Comm. Letters, March 2004.
- Harn L., Hsin W., Mehta M., *Authenticated Diffie-Hellman Key Agreement Protocol using Single Cryptographic Assumption*, IEE proceedings of Communications, August 2005.
- Mehta M., Huang D., *RINK-RKP: A Scheme for Key Predistribution and Shared-Key Discovery in Sensor Networks*, IEEE IPCCC, April 2005.
- Huang D., Mehta M., Medhi D., Harn L., *Location-aware Key Management Scheme for Wireless Sensor Networks,* ACM SASN' 04, October 2004.
- Huang D., Mehta M., *A Secure and Energy-efficient Pairwise Key Establishment Protocol for Sensor Networks,* IEEE IPCCC, April 2005.

Honors

- Distinguished Dissertation Fellowship, UMKC (2005-2006)
- Dean's Doctoral Fellowship, UMKC. (2004 - 2005)
- Dean's Outstanding Student Award, UMKC. (2002 - 2003)
- Dean's Doctoral Fee Waiver Fellowship, UMKC (2002 - 2003)

Affiliations

ISC^2 (2005 - Present)
President, India Student Association, UMKC. (2002 - 2003)
Student Member, IEEE. (2002 – present)

References

Available upon request.
