James M. Galvin, Ph. D.

Experience

Director Strategic Relationships and Technical Standards, Afilias USA, 300 Welsh Road, Horsham, PA 19044. May 2009 through present. Afilias is an Internet infrastructure solutions provider specializing in top-level domain registry services, domain name services (DNS), and discovery services (the Internet of things). Responsible for the technical relationship with strategic customers and partners. Responsible for developing, maintaining, and coordinating Afilias' technical standards, including new standards discovery and qualification, particularly in ICANN and the IETF.

Founder and Principal, *eList eXpress LLC*, 607 Trixsam Road, Sykesville, MD 21784. September 1999 through present. eList eXpress is an email service provider specializing in hosting mailing lists and custom email services.

Chief Technologist, *CommerceNet*, 10050 N Wolfe Road, Cupertino, CA. January 1996 through August 1999. CommerceNet is a not-for-profit membership-based consortium that seeks to ensure an interoperable global electronic marketplace that is trusted by the public. Responsible for all technical activities, including project management, staff, reviewing all publications, and publishing technical analyses and opinions for distribution to CommerceNet's membership.

Senior Computer Scientist, *Trusted Information Systems*, 3060 Washington Road, Glenwood, MD 21738. June 1989 through January 1996. Principal architect and senior technical lead for the design and implementation of Internet infrastructure security services, specifically the Domain Name System (DNS), secure email, network management, and public key infrastructures (PKI). Co-author of the MIME Object Security Services (MOSS) protocol, a secure email protocol. Principal architect of the MOSS reference implementation and senior technical lead for the development. Principal architect of the Privacy Enhanced Mail (PEM) reference implementation (another secure email protocol) and senior technical lead for the development. Co-author of the Simple Network Management Protocol (SNMP) security protocols, both version one and version two.

Senior Software Engineer, *The Wollongong Group*, 1129 San Antonio Road, Palo Alto, CA 94303. March 1988 through May 1989. Senior technical lead for computer security and electronic mail projects. Significant contributions were made to the network management project. I brought X.400 and X.500 expertise to TWG, but I was involved in all OSI activities there, gaining non-detailed experience in all aspects of OSI networking.

Community Committees

BIND10 Steering Committee. Committee is responsible for guiding the development of version 10 of BIND, the most widely deployed DNS implementation. May 2009 to present.

Security and Stability Advisory Committee. Advises the ICANN community and Board on matters relating to the security and integrity of the Internet's naming and address allocation systems. May 2002 to present.

IETF DNS Security Working Group. Served as Chair during its entire tenure developing the first two versions of the DNS Security protocol. March 1993 to December 1999.

Education

Doctor of Philosophy Computer and Information Sciences, June 1988. University of Delaware, Newark, DE 19716. Dissertation Title: Distributed Cryptographic Key Management System.

Master of Science Computer and Information Sciences, December 1986. University of Delaware, Newark, DE 19716.

Bachelor of Science Double Major (Computer Science and Mathematics), May 1982. Moravian College, Bethlehem, PA 18018.

Authored and Published Works

DNS Security: A Historical Perspective. *IETF Journal,* Volume 2, Issue 2, Autumn 2006. Internet Society, Reston, VA.

Donald Eastlake, 3rd. DNS Security Operational Considerations. RFC2541, March 1999.

Donald Eastlake, 3rd. Detached Domain Name System (DNS) Information. RFC2540, March 1999.

Donald Eastlake, 3rd. Storage of Diffie-Hellman Keys in the Domain Name System. RFC2539, March 1999.

Donald Eastlake, 3rd and Olafur Gudmundsson. Storing Certificates in the Domain Name System. RFC2538, March 1999.

Donald Eastlake, 3rd. RSA/MD5 KEYs and SIGs in the Domain Name System. RFC2537, March 1999.

Donald Eastlake, 3rd. DSA KEYs and SIGs in the Domain Name System. RFC2536, March 1999.

Donald Eastlake, 3rd. Domain Name System Security Extensions. RFC2535, March 1999.

Donald Eastlake, 3rd. Secure Domain Name System Dynamic Update. RFC2137, April 1997.

Donald Eastlake, 3rd and Charlie Kaufman. Domain Name System Security Extensions. RFC2065, January 1997.

ConneXions, Interop Company, ISSN 0894-5926. Publish column after each IETF meeting summarizing security activities during the task force. 1994-1995.

Data Security Letter, Trusted Information Systems, ISSN 1065-9986. Publish column after each IETF meeting summarizing security activities during the task force. 1995-1996.

Jim Galvin, Sandy Murphy, Steve Crocker, Ned Freed. Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted. RFC1847, October 1995.

Steve Crocker, Ned Freed, Jim Galvin, and Sandy Murphy. MIME Object Security Services. RFC1848, October 1995.

James M. Galvin and Sandra L. Murphy. Using Public Key Technology - Issues of Binding and Protection. Proceedings of the Internet Society's 1995 International Networking Conference, June 27-30, 1995.

James M. Galvin and Mark Feldman. MIME Object Security Services: Issues in a Multi-User Environment. *Proceedings of the Fifth USENIX UNIX Security Symposium*, June 5-7, 1995.

Security Awareness Increasing within IETF, *ConneXions-The Interoperability Report*, September 1994, Volume 8, Number 9. Interop, Inc., Mountain View, CA.

James M. Galvin and Keith McCloghrie. Administrative Model for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC1445, April 1993.

James M. Galvin and Keith McCloghrie. Security Protocols for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC1446, April 1993.

James M. Galvin and Keith McCloghrie. Party MIB for Version 2 of the Simple Network Management Protocol (SNMPv2). RFC1447, April 1993.

James M. Galvin, David M. Balenson, Stephen D. Crocker, and Paul C. Clark. Preliminary Discussion: Security Issues of a UNIX PEM Implementation. PSRG Workshop on Network and Distributed System Security, February 11-12, 1993.

James M. Galvin and David M. Balenson. Security Aspects of a UNIX PEM Implementation. 3rd UNIX Security Symposium, September 14-16, 1992.

James R. Davin, James M. Galvin and Keith McCloghrie. SNMP Administrative Model. RFC1351, July 1992.

James M. Galvin, Keith McCloghrie and James R. Davin. SNMP Security Protocols. RFC1352, July 1992.

Keith McCloghrie, James R. Davin and James M. Galvin. Definitions of Managed Objects for Administration of SNMP Parties. RFC1353, July 1992.

Secure Communication Using X.500 Services for X.400 and Privacy Enhanced Mail. Tutorial presented at the 1992 IFIP International Conference on Upper Layer Protocols, Architectures, and Applications, May 27-29, 1992.

The Deployment of Privacy Enhanced Mail. *ConneXions-The Interoperability Report*, October 1991, Volume 5, Number 10. Interop, Inc., Mountain View, CA.

Keith McCloghrie, James R. Davin and James M. Galvin. SNMP Security. *ConneXions-The Interoperability Report*, June 1991, Volume 5, Number 6. Interop, Inc., Mountain View, CA.

James M. Galvin, Keith McCloghrie and James R. Davin. Secure Management of SNMP Networks. *IFIP TC6/WG6.6 Second International Symposium on Integrated Network Management*, April 1-5, 1991.

Components of OSI: The Security Architecture. *ConneXions-The Interoperability Report*, August 1990, Volume 4, Number 8. Interop, Inc., Mountain View, CA.

Privacy Without Authentication. *IFIP WG 6.5 Message Handling Systems and Distributed Applications*, October 10-12, 1988.

Mutation Analysis: A Users View. *Proceedings of the Seventh Annual Micro-Delcon Conference*, March 6, 1984.

Efficient Computer Evaluation of Flowgraphs by Mason-Cebulka Technique. *Proceedings of the Pennsylvania Academy of Science*, Volume 56, March 28, 1982.

M. McAllister, K. Cebulka and J. Galvin. Stochastic Networks, An Evaluation Technique and An Application. *Proceedings of the Pittsburgh Conference on Modeling and Simulation*, Volume 13, Part 2, Computers and Computer Modeling, 1982.