Brief list of Academic Writings by Selwyn Russell

(Up to December 2002)

1. Publications

Referred Journals Sole Author:

S. Russell, “Planning for the EDI of Tomorrow Using Electronic Document Authorization”, in “Computer Security, IFIP/SEC'93: Discovering Tomorrow”, Elsevier Science Publishers, pp. 243-51.

S. Russell, “Paradigms for Verification of Authorization at Source of Electronic Documents”, in “Computers and Security”, October 1993, Volume 12, Number 6, pp. 542-49.

S. Russell, “Audit-By-Receiver Paradigms for Verification of Authorization At Source of Electronic Documents”, in “Computers and Security”, February 1994, Volume 13, Number 1, pp. 59-67.

S. Russell, “Controlling Separation of Duties to Prevent Electronic Document Fraud”, in EDPACS, June 1994, Volume 21, Number 12, pp. 6-15.

S. Russell, “Foiling an Attack by an Insider and Wire Tapper in Collusion”, in EDPACS, June 1995, Volume 23, Number 1, pp. 1-17.

S. Russell, “Foiling Active Network Impersonation Attacks Made in Collusion with an Insider”, in “Lecture Notes in Computer Science 1029, Cryptography: Policy and Algorithms”, 1995, Elsevier Publishers, pp 301-12.

S. Russell, “A k-th Order Carmichael Key Scheme for Shared Encryption”, ACM SIGSAC Review, December 1996.

S. Russell, “Multisignature Algorithms for ISO 9796”, ACM SIGSAC Review, December 1996.

Published Conference Proceedings Sole Author:

S. Russell, “Paradigms for Verification of Authorization at Source of Electronic Documents In an Integrated Environment”, in Proceedings of the IEEE 8th Computer Security Applications Conference, San Antonio, Texas, December 1992, pp. 133-39.

S. Russell, “Audit by Receiver Paradigms for Verification of Authorization At Source of Electronic Documents”, in Proceedings of the 16th Australian Computer Science Conference, February 1993, Brisbane, pp. 173-80.

S. Russell, “Planning for the EDI of Tomorrow Using Electronic Document Authorization”, in Proceedings of IFIP Sec/93, May 1993, Toronto, Canada, pp. 237-45.

S. Russell, “Making EDI Secure in an Automated World”, in Proceedings of the 5th Canadian Computer Security Symposium, May 1993, Ottawa, Canada, pp. 549-56.

S. Russell, “Transparent Cosignatures for Electronic Documents”, in IEEE 9th Computer Security Applications Conference, December 1993, Orlando, Florida, pp. 82-91.

S. Russell, “Implementing Separation of Duties with Transparent Cosignatures”, in Proceedings of the 6th Canadian Computer Security Symposium, May 1994, Ottawa, Canada, pp. 361-74.

S. Russell “Implementing Separation of Duties with an AI Cosignature Controller”, in “Pre-Proc. of the First Cryptography: Policy and Algorithms Conference”, July 1995, Brisbane, pp. 143-48.

S. Russell “Foiling Active Network Impersonation Attacks Made in Collusion with an Insider”, in “Pre-Proc. of the First Cryptography: Policy and Algorithms Conference”, July 1995, Brisbane, pp. 235-48.

S. Russell, “Fast Checking of Individual Certificate Revocation on Small Systems'”, in IEEE 15th Computer Security Applications Conference, December 1999, Scottsdale, Arizona.

S. Russell, “Re-engineering Key Establishment Protocols for M-commerce”, Proc of First Workshop on Information Security Applications, Seoul, 24-25 November 2000.

S.Russell, “Structures of Digital Certificates for M-Commerce”, Sixth CDMA International Conference, Seoul, 30 October - 2 November 2001.

S. Russell, “Implementing Certificate Validation Servers for Improved M-Commerce Performance”, Wireless Networks And Emerging Technologies - WNET '02 Symposium, IASTED International Conference on Wireless and Optical Communications, Banff, Canada, 17 – 19 July 2002.

S.Russell, “Recursive Certificates: a New Paradigm for PKI Certificates”,
Proceedings of Second International Workshop for Asian Public Key Infrastructure, 30 October - 1 November 2002, Taipei, Taiwan.

Joint Author:

Selwyn Russell and Peter Craig “Privacy Enhanced Mail Modules for ELM”, in Proc. of the ISOC Symposium on Network and Distributed System Security, February 1994, pp. 21-34.

Quarterly Research reports for Korea Telecom, 1997-2000, my components being

1. Security in Third Generation
2. Security Requirement of Third Generation Wiireless
3. Investigation into Threats and Requirements
4. Security Requirements and Architecture
5. Random Numbers and Public Key Ciphers
6. Public Key Infrastructure
7. Certificate Management
8. Public Key Infrastructures for Wireless
9. Certificate Management in the Wireless Environment
10. PKI Architecture for Third Generation Wireless
11. Certificates for Wireless

Gaskell, G., Looi, M., Boyd, C., Russell, S. and Dawson, E., "A Proposed Security Architecture for Third Generation Wireless Systems", ICISC’98, Korea, December, 1998.

Course notes on Public Key Infrastructure for Standards Australia, May / June 2000 (three authors):

- Public Key Authentication Framework
- Deploying a PKI
- Current Initiatives

GateKeeper II Documentation for Government of Australia August 2000. (4 authors)

S Russsell and E Dawson, “Public Key Infrastructure for Future Wireless Networks”, Fifth CDMA International Conference, Seoul, 22-25 November 2000.

"Global Public Key Infrastructure: A Report for the Telecommunications Advanced Organisation (TAO) of Japan", April 2001, for the Global PKI project sponsored by TAO Japan. (five authors)

S Russell and J Smith, "On Optimal Public Key Certificates for M-Commerce", First International Workshop for Asian PKI, Daejeon, Korea, 19 – 20 October 2001.

S. Russell, E. Okamoto, E. Dawson, J. Lopez, "Improving Performance in Global PKI using Virtual Certificates and Synthetic Certificates", Proceedings of the 2002 Symposium on Cryptography and Information Security, Shirahama, Japan, 29 Jan – 1 Feb 2002, Institute of Electronics, Information and Communications Engineers of Japan.

S. Russell and M. Yao, "Application of Agent Technology to Certificate Objects", Proceedings of the 2002 Symposium on Cryptography and Information Security, Shirahama, Japan, 29 Jan – 1 Feb 2002, Institute of Electronics, Information and Communications Engineers of Japan.

S. Russell and M. Yao, "A New Paradigm for Message Delivery to a Hidden
Entity Using an Emissary Agent", submitted to Seventh IEEE Globecomm 2002, to be held in Taiwan, November 2002.

W. Caelli, K. Chen, E. Dawson, M. Henricksen, J. Lopez, E. Okamoto, S. Russell and J. Smith, "Online Public Key Infrastructure", VII Spanish Meeting on Cryptology and Information Security, Spain, 2002.

VC article in journal

SCIS2003 paper

2. Unpublished Conference Proceedings & Seminars Sole Author:

1993
S Russell, "Security and DCE". QuestNet '93, University of Central Queensland, July 1993.

1994
S Russell, "Secure Logins Across Networks". QuestNet '94, University of Southern Queensland, July 1994.

3. Public Software:

Package to use Z notation with EmTex, Distributed from University of Stuttgart, Germany, March 1993. Now on ftp sites around the world, and included on some CD-ROMs of OS/2 software.

Procedure libraries to extend the usefulness of the Lenstra extended precision software. This includes RSA and El Gamal in conformity with the RSA Public Key Cryptosystem Standards of June 1991.