The Research of the Information Security Group

Jason Crampton
Director of Research
Information Security Group
Royal Holloway, University of London

11th February 2013

1 Introduction

Royal Holloway, University of London (RHUL) is an academic centre of excellence in cyber security, one of eight such centres in the UK recognized by GCHQ (Government Communications Headquarters). Most of the research in information and cyber security at RHUL is undertaken by members of the *Information Security Group* (ISG), which is one of the largest academic information security groups in the world. The ISG is also one of the oldest groups of its type, having worked on cryptography since the mid-1980s and taking its current name in 1990. It was the first institution in the world to offer a masters degree (or indeed any other degree) in information security, accepting its first students in 1992. There are now over 2000 alumni of the course, many working in senior information security roles in government and industry.

The ISG is a department within the School of Mathematics and Information Security at RHUL, having its own Director (Prof. Keith Martin) who reports directly to the Head of the School. The ISG employs sixteen full-time and two part-time members of staff (Fuchsberger and Ng), all of whom are actively involved in information and cyber security research. Some members of the group focus almost entirely on academic research, while others—notably Cid, Ciechanowicz, Fuchsberger, Mayes, Mitchell, Paterson and Price—maintain strong links with industry and undertake industrial research and consultancy. Of the sixteen full-time academics, seven are full professors. The ISG is privileged to have several distinguished visiting professors, including Henry Beker, Whitfield Diffie, Paul Dorey, Dieter Gollmann, David Naccache and Richard Walton, who are among the most prominent academics and industry figures in information security research. The activities of the ISG are supplemented by the research of Prof. Simon Blackburn, Dr James McKee and Prof. Rüdiger Schack, who are officially members of the Mathematics Department. There is also increasing collaboration between the ISG and the Department of Computer Science, in particular the Theory of Computing and Computer Learning groups.

2 Research Activities

The ISG was founded by a group of mathematicians and computer scientists with interests in cryptography, and research in this area remains an important part of the ISG's activities. It has expertise in cryptanalysis (Blackburn, Cid, Murphy and Paterson), combinatorial

cryptography (Blackburn, Martin and Ng), quantum information theory and cryptography (Schack), provable security (Paterson) and message authentication codes (Mitchell).

The pioneering recent work of Paterson (EPSRC Leadership Fellowship "*Cryptography: Bridging Theory and Practice*") examines the weaknesses of implementations of secure protocols and seeks to develop appropriate models for reasoning about the security of those implementations. Paterson's work has considered SSH [8], IPsec [29, 30] and SSL/TLS [52], all protocols that are very widely used and generally assumed to be secure. His work ensures that the ISG maintains a high profile and reputation for innovation in modern cryptographic research.

Blackburn and Martin's recent EPSRC-funded work on key predistribution in sensor networks ("*Effective Key Management for Wireless Sensor Networks*") uses innovative mathematical models to efficiently administer keying material in lightweight *ad hoc* networks [9, 47, 48]. In fact, some of the earliest work on combinatorial designs for key predistribution [51] was undertaken Mitchell and Piper at the ISG. Other research of a combinatorial nature includes the work of Blackburn and Ng on codes that have applications in privacy protection and digital rights management [10, 11]. Ng's recent work focused on the provision of trust and privacy in the area of announcement schemes in vehicular ad hoc networks [18, 42]. She has collaborated with internal and external colleagues in several publications in this area.

Murphy helped develop the field of differential cryptanalysis [39] and, together with Cid, has written a widely-cited book on the cryptanalysis of the advanced encryption standard [20]. Cid continues to work on novel algorithms and techniques for cryptanalysis [6, 7], as well as exploring novel cryptographic mechanisms [19] and applications of game theory to system security [59].

Walter is an expert in fast algorithms for exponentiation—a vital operation in many public-key cryptosystems [64]. His recent work has focused on the development of algorithms that can operate on platforms with very limited computational resources [63].

The Smart Card Centre[1] (SCC) has been part of the ISG since 2002. It began as a collaboration between academia and industry, originally attracting funding from Vodafone and Giesecke & Devrient. The research of the centre is concerned with smart cards, smart tokens, and the associated systems and applications. The SCC is at the forefront of academic research in its areas of interest, SCC researchers (Hancke, Markantonakis and Mayes) having published around 100 peer-reviewed publications since the centre's formation. Current research areas of particular interest include RFID security [35, 36, 40, 43], near field communications [31, 32], and new models of smart card ownership [1, 2].

The ISG also conducts research into socio-technical and organisational aspects of information security, two broad and rapidly expanding disciplines that include many topics of crucial importance to the science of cyber security. The research in this area is led by Coles-Kemp, with Price and Pavlovic also having interests in this area. In 2008 Coles-Kemp was part of a team that was awarded the the VOME project (*Visualisation and Other Methods of Expression*) that was concerned with both the social (people, on-line privacy and consent [22]) and the organisational (design principles for on-line services and personal information management [23, 60]). This project pioneered visual research methods and other forms of engagement and data collection [21] that enabled grounded social science research to take place in a wide range of demographics. Coles-Kemp has subsequently been awarded a further three grants—funded by AHRC, EPSRC and the EU and worth in excess of £1,000,000—to use and extend

[1] `http://www.scc.rhul.ac.uk/`

these research methods in a variety of areas including criminal justice and family welfare, organisational security and public service delivery.

The research of the ISG has a strong focus on the security of systems and technologies, including the foundations of trust (such as key management infrastructures and trusted computing), the development of secure, large-scale applications and systems (such as workflow management systems, mobile telephone networks, computational grids and national infrastructure), and to applications (such as payment systems and identity management systems).

Paterson as principal investigator, with co-investigators Crampton and Price, worked on the EPSRC-funded project "*Novel Security Architectures and Policy Management Techniques for e-Science*". This work considered the use of alternative key management techniques to support security services in computational grids [27, 44]. Paterson, with various co-investigators from the ISG, also acquired funding in excess of £1,000,000 as part of the International Technology Alliance, funded by the US Department of Defense and the UK Ministry of Defence. This funding has supported research in the security of systems of systems and led to work on the security of MANETS [34], information flow [61] and risk-based access control [28], and currently supports work on cryptographic mechanisms for protecting the security of hybrid coalition networks.

Mitchell has a wide range of research interests, encompassing authentication [16, 41] and identity management [5], MAC algorithms [37, 38], network security [14] and trusted computing [17]. Tomlinson shares Mitchell's interest in trusted computing [33, 66] and mobile networks, having been principal investigator on the EPSRC-funded project "*Instant Knowledge: Secure Autonomic Business Collaboration*" and the recipient of funding from the Mobile VCE project.

Wolthusen has a wide range of interests including biometrics [45], network security [34] and forensics [3]. He is recognised internationally as an expert in critical infrastructure protection and has published widely in this area [49, 50]. He was co-chair of the programme committee for CRITIS (International Workshop on Critical Information Infrastructure Security) in 2007 and 2008. He is the principal investigator on the EU-funded project "*Internet of Energy*" worth almost £500,000.

Pavlovic has an exceptionally diverse range of interests in cyber security, including mathematical models of trust [53, 55], the application of formal methods [58] and game theory [56] to information security, and quantum cryptography [54]. His recent work [56, 57], questioning Kerckhoffs' Principle that there is no security by obscurity, has received considerable interest and funding. He is the director of ASECOLab at RHUL, for which he has secured substantial funding, some of which supports two post-doctoral research assistants and five PhD students.

Cavallaro joined the ISG in January 2012, bolstering our expertise in distributed systems security. Cavallaro has worked previously as a post-doctoral research assistant with the influential researchers Prof. Christopher Kreugel and Prof. Giovanni Vigna at University of California (Santa Barbara) and Prof. Andy Tanenbaum in Amsterdam. His work focuses on malware and program analysis [12, 46, 62] and tools for identifying potential vulnerabilities in programs [13, 67].

Crampton's work has a broad range of interests in authorization and access control, including the design of models for access control [15, 65], languages for specifying authorization policies [26], authorization and the enforcement of business rules in workflow management systems [24], and cryptographic access control mechanisms [25]. He is co-investigator, with Prof. Gutin and Prof. Cohen from Computer Science, on an EPSRC-funded grant to study the problems related to the enforcement of complex business and security rules in workflow

systems.

3 Esteem Indicators

The ISG is held in high regard by the academic community, as evidenced by the involvement of its members in editorial and review work. In particular, members of the group sit on the editorial boards of many influential journals in information security: *Designs, Codes and Cryptograph* (Cid), *IEEE Communications Letters*, *The Computer Journal*, *Designs, Codes and Cryptography*, *International Journal of Information Security* and *Information Management and Computer Security* (Mitchell[2]); and *Journal of Cryptology* (Paterson). Paterson is co-editor-in-chief of the book series *Information Security and Cryptography* published by Springer. Senior members of the group are each asked to join between five and ten conference programme committees every year, with other members of the group also accepting similar invitations on a regular basis. Paterson was chair of the programme committee for Eurocrypt 2011, one of the two premier conferences in this area. The ISG has also hosted a number of academic conferences in recent years, including Pairing 2008, CARDIS 2008, SCC 2010, WISTP 2012 and InTrust 2012; and this year will host IDMAN 2013 and ESORICS 2013 (for which Crampton will be programme co-chair).

4 Facilities

The ISG facilities include a security lab, a virtual penetration testing lab, and two labs hosted by the SCC. The security lab hosts a number of platforms (running a variety operating systems) on a segregated and configurable network. The platforms in the lab are fully configurable and the lab has a range of network hardware available, including firewalls, routers and switches.

The virtual penetration testing lab is available to all students and is accessible from general purpose computer labs. The lab consists of a number of servers and services running on virtual machines with various vulnerabilities pre-seeded and a penetration testing toolkit. Students learn about penetration testing within this "closed" environment and are able to develop their penetration testing skills without risk to production systems.

A virtual server hosting platform is also provided to give students and staff the capability of hosting services and servers in the datacenter. This has been used for computationally expensive operations as well as for development and demonstrations of security software, particularly where multiple servers and operating systems are often required, or are client-server based. This platform has been used to develop proof-of-concept implementations of PhD research, notably by Haitham Al-Sinani for his work on CardSpace/OpenID [4], and by Chunhua Chen in the course of his research on the UbiPass application.

The SCC labs house hardware and software dedicated to the development, testing and analysis of applications for smart cards and RFID tags. The hardware includes smart card and RFID readers, mobile devices, probe station, equipment for side-channel analysis, and configurable logic devices.

[2]Mitchell is co-editor-in-chief of *Designs, Codes and Cryptography* **and a senior editor of *IEEE Communications Letters***

5 Vision and Strategy

The ISG has expanded its range of research interests considerably since its inception. In the last few years, the appointments of Coles-Kemp, Pavlovic and Cavallaro have continued the development of the ISG's "portfolio". The research of the group now embraces many existing and emerging aspects of information and cyber security.

- Coles-Kemp has a wide range of interests in the socio-technical and organisational issues that are widely recognised as being of crucial importance in information and cyber security.
- Wolthusen has recently obtained funding to work on security concerns in smart energy grids.
- Tomlinson conducts research on the privacy concerns that arise in social networks.
- Cid and Pavlovic share an interest in the economics of information security and "rational" security, with a focus on the applications of game theory to cyber security.
- The Smart Card Centre is conducting pioneering research on the security implications of near-field communications.

The ISG is committed to maintaining an innovative and state-of-the-art teaching programme, which, in turn, has informed the research of members of the group. A notable example of the way in which teaching has influenced our research is the work of Paterson on the practical, rather than abstract, vulnerabilities that exist in protocols that are widely used and had been presumed to be secure. The ISG has recently introduced teaching modules on cyber security and economics of security, and a third module that will cover *inter alia* the security implications of outsourcing and the increasing use of personal mobile devices as workplace tools. We expect that the development of these modules, in consultation with our wide range of contacts in industry and government, will inform some of the future research directions of the group.

The ISG continues to be energetic in its pursuit of external funding to support its research activities. In the last year alone, members of the group have been involved in funding proposals on topics as diverse as cyber defence (Wolthusen), cyber security (Markantonakis), cartographies for cyber security (Coles-Kemp), trust-building in networks (Pavlovic), and enforcing compliance with business rules in information systems (Crampton), the majority of which have been funded. The ISG is also seeking to establish collaborations with industrial partners to fund PhD studentships; Crampton, Markantonakis, Martin and Paterson have all recently secured funding for postgraduate research students. The CEReS (Consortia for Exploratory Research in Security) call gave rise to a number of new, exciting collaborations between members of the ISG and the Mathematics and Computer Science Departments. Four of the ten proposals that will be considered for CEReS funding, following an initial selection from outline proposals, include one or more members of the ISG.

References

[1] Akram, R. N., Markantonakis, K., and Mayes, K. Application management framework in user centric smart card ownership model. In *WISA* (2009), H. Y. Youm and M. Yung, Eds., vol. 5932 of *Lecture Notes in Computer Science*, Springer, pp. 20–35.

[2] Akram, R. N., Markantonakis, K., and Mayes, K. Firewall mechanism in a user centric smart card ownership model. In *CARDIS* (2010), D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, Eds., vol. 6035 of *Lecture Notes in Computer Science*, Springer, pp. 118–132.

[3] Al-Kuwari, S., and Wolthusen, S. D. On the feasibility of carrying out live real-time forensics for modern intelligent vehicles. In *e-Forensics* (2010), X. Lai, D. Gu, B. Jin, Y. Wang, and H. Li, Eds., vol. 56 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Springer, pp. 207–223.

[4] Al-Sinani, H. S., and Mitchell, C. J. Enhancing cardspace authentication using a mobile device. In *DBSec* (2011), Y. Li, Ed., vol. 6818 of *Lecture Notes in Computer Science*, Springer, pp. 201–216.

[5] Al-Sinani, H. S., and Mitchell, C. J. A universal client-based identity management tool. In *EuroPKI* (2011), S. Petkova-Nikova, A. Pashalidis, and G. Pernul, Eds., vol. 7163 of *Lecture Notes in Computer Science*, Springer, pp. 49–74.

[6] Albrecht, M. R., and Cid, C. Cold boot key recovery by solving polynomial systems with noise. In *ACNS* (2011), J. Lopez and G. Tsudik, Eds., vol. 6715 of *Lecture Notes in Computer Science*, pp. 57–72.

[7] Albrecht, M. R., Cid, C., Faugère, J.-C., and Perret, L. On the relation between the mxl family of algorithms and gröbner basis algorithms. *Journal of Symbolic Computing 47*, 8 (2012), 926–941.

[8] Albrecht, M. R., Paterson, K. G., and Watson, G. J. Plaintext recovery attacks against SSH. In *IEEE Symposium on Security and Privacy* (2009), IEEE Computer Society, pp. 16–26.

[9] Blackburn, S. R., Etzion, T., Martin, K. M., and Paterson, M. B. Distinct difference configurations: Multihop paths and key predistribution in sensor networks. *IEEE Transactions on Information Theory 56*, 8 (2010), 3961–3972.

[10] Blackburn, S. R., Etzion, T., and Ng, S.-L. Prolific codes with the identifiable parent property. *SIAM Journal of Discrete Mathematics 22*, 4 (2008), 1393–1410.

[11] Blackburn, S. R., Etzion, T., and Ng, S.-L. Traceability codes. *Journal of Combinatorial Theory, Series A 117*, 8 (2010), 1049–1057.

[12] Cavallaro, L., Saxena, P., and Sekar, R. On the limits of information flow techniques for malware analysis and containment. In *DIMVA* (2008), D. Zamboni, Ed., vol. 5137 of *Lecture Notes in Computer Science*, Springer, pp. 143–163.

[13] Cavallaro, L., and Sekar, R. Taint-enhanced anomaly detection. In *ICISS* (2011), S. Jajodia and C. Mazumdar, Eds., vol. 7093 of *Lecture Notes in Computer Science*, Springer, pp. 160–174.

[14] Chen, C., Mitchell, C. J., and Tang, S. Ubiquitous one-time password service using the Generic Authentication Architecture. *Mobile Networks and Applications to appear* (2013).

[15] Chen, L., and Crampton, J. On spatio-temporal constraints and inheritance in role-based access control. In *ASIACCS* (2008), M. Abe and V. D. Gligor, Eds., ACM, pp. 205–216.

[16] Chen, L., and Mitchell, C. J. Parsing ambiguities in authentication and key establishment protocols. *Journal of Electronic Security and Digital Forensics 3*, 1 (2010), 82–94.

[17] Chen, L., Mitchell, C. J., and Martin, A., Eds. *Trusted Computing, Second International Conference, Trust 2009, Oxford, UK, April 6-8, 2009, Proceedings* (2009), vol. 5471 of *Lecture Notes in Computer Science*, Springer.

[18] Chen, L., Ng, S.-L., and Wang, G. Threshold anonymous announcement in VANETs. *IEEE Journal on Selected Areas in Communication Special Issue on Vehicular Communications and Networks 29*, 3 (2011), 605–615.

[19] Choi, S. G., Katz, J., Kumaresan, R., and Cid, C. Multi-client non-interactive verifiable computation. In *TCC* (2013), vol. 7785 of *Lecture Notes in Computer Science*, Springer, pp. 499–518.

[20] Cid, C., Murphy, S., and Robshaw, M. J. B. *Algebraic Aspects of the Advanced Encryption Standard*. Springer, 2006.

[21] Coles-Kemp, L., and Ashenden, D. M. A. Community-centric engagement: lessons learned from privacy awareness intervention design. In *Proceedings of HCI 2012, The 26th BCS Conference on Human Computer Interaction* (2012).

[22] Coles-Kemp, L., and Kani-Zabihi, E. Practice makes perfect: Motivating confident on-line privacy protection practices. In *Proceedings of SocialCom-11* (2011).

[23] Cordoba, J. R., Coles-Kemp, L., and Ahwere-Bafo, J. (Re)-conceptualising e-government: Studying and using patterns of practice. In *Proceedings of Operational Research Society Conference (OR 52), Extended Abstracts OR52* (2010), pp. 32–38.

[24] Crampton, J. A reference monitor for workflow systems with constrained task execution. In *SACMAT* (2005), E. Ferrari and G.-J. Ahn, Eds., ACM, pp. 38–47.

[25] Crampton, J. Practical and efficient cryptographic enforcement of interval-based access control policies. *ACM Transactions on Information and Systems Security 14*, 1 (2011), 14.

[26] Crampton, J., and Huth, M. An authorization framework resilient to policy evaluation failures. In *ESORICS* (2010), D. Gritzalis, B. Preneel, and M. Theoharidou, Eds., vol. 6345 of *Lecture Notes in Computer Science*, Springer, pp. 472–487.

[27] Crampton, J., Lim, H. W., Paterson, K. G., and Price, G. User-friendly and certificate-free grid security infrastructure. *International Journal of Information Security 10*, 3 (2011), 137–153.

[28] Crampton, J., and Morisset, C. An auto-delegation mechanism for access control systems. In *STM* (2010), J. Cuéllar, J. Lopez, G. Barthe, and A. Pretschner, Eds., vol. 6710 of *Lecture Notes in Computer Science*, Springer, pp. 1–16.

[29] Degabriele, J. P., and Paterson, K. G. Attacking the IPsec standards in encryption-only configurations. In *IEEE Symposium on Security and Privacy* (2007), IEEE Computer Society, pp. 335–349.

[30] Degabriele, J. P., and Paterson, K. G. On the (in)security of IPsec in MAC-then-encrypt configurations. In *ACM Conference on Computer and Communications Security* (2010), E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds., ACM, pp. 493–504.

[31] Francis, L., Hancke, G. P., Mayes, K., and Markantonakis, K. Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. In *ICITST* (2009), IEEE, pp. 1–8.

[32] Francis, L., Hancke, G. P., Mayes, K., and Markantonakis, K. Practical NFC peer-to-peer relay attack using mobile phones. In *RFIDSec* (2010), S. B. O. Yalcin, Ed., vol. 6370 of *Lecture Notes in Computer Science*, Springer, pp. 35–49.

[33] Gebhardt, C., Dalton, C. I., and Tomlinson, A. Separating hypervisor trusted computing base supported by hardware. In *Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing* (2010), pp. 79–84.

[34] Gennaro, R., Halevi, S., Krawczyk, H., Rabin, T., Reidt, S., and Wolthusen, S. D. Strongly-resilient and non-interactive hierarchical key-agreement in manets. In *ESORICS* (2008), S. Jajodia and J. López, Eds., vol. 5283 of *Lecture Notes in Computer Science*, Springer, pp. 49–65.

[35] Hancke, G. P. Design of a secure distance-bounding channel for RFID. *Journal of Network and Computer Applications 34*, 3 (2011), 877–887.

[36] Hancke, G. P. Practical eavesdropping and skimming attacks on high-frequency RFID tokens. *Journal of Computer Security 19*, 2 (2011), 259–288.

[37] Knudsen, L. R., and Mitchell, C. J. Analysis of 3gpp-MAC and two-key 3gpp-MAC. *Discrete Applied Mathematics 128* (2003), 181–191.

[38] Knudsen, L. R., and Mitchell, C. J. Partial key recovery attack against RMAC. *Journal of Cryptology 18*, 4 (2005), 375–389.

[39] Lai, X., Massey, J. L., and Murphy, S. Markov ciphers and differential cryptanalysis. In *EUROCRYPT* (1991), D. W. Davies, Ed., vol. 547 of *Lecture Notes in Computer Science*, Springer, pp. 17–38.

[40] Leng, X., Lien, Y., Mayes, K., and Markantonakis, K. An RFID grouping proof protocol exploiting anti-collision algorithm for subgroup dividing. *International Journal of Security and Networks 5*, 2/3 (2010), 79–86.

[41] Leung, A., and Mitchell, C. J. Ninja: Non identity based, privacy preserving authentication for ubiquitous environments. In *Ubicomp* (2007), J. Krumm, G. D. Abowd, A. Seneviratne, and T. Strang, Eds., vol. 4717 of *Lecture Notes in Computer Science*, Springer, pp. 73–90.

[42] Li, Q., Malip, A., Martin, K. M., Ng, S.-L., and Zhang, J. A reputation-based announcement scheme for VANETs. *IEEE Transactions on Vehicular Technology 61*, 9 (2012), 4095–4108.

[43] Lien, Y., Leng, X., Mayes, K., and Chiu, J.-H. Select-response grouping proof and its verification protocol for RFID tags. *International Journal of Intelligent Information and Database Systems 5*, 2 (2011), 101–118.

[44] Lim, H. W., and Paterson, K. G. Identity-based cryptography for grid security. *International Journal of Information Security 10*, 1 (2011), 15–32.

[45] Mairaj, D., Wolthusen, S. D., and Busch, C. Teeth segmentation and feature extraction for odontological biometrics. In *IIH-MSP* (2010), I. Echizen, J.-S. Pan, D. W. Fellner, A. Nouak, A. Kuijper, and L. C. Jain, Eds., IEEE Computer Society, pp. 323–328.

[46] Martignoni, L., Fattori, A., Paleari, R., and Cavallaro, L. Live and trustworthy forensic analysis of commodity production systems. In *RAID* (2010), S. Jha, R. Sommer, and C. Kreibich, Eds., vol. 6307 of *Lecture Notes in Computer Science*, Springer, pp. 297–316.

[47] Martin, K. M. On the applicability of combinatorial designs to key predistribution for wireless sensor networks. In *IWCC* (2009), Y. M. Chee, C. Li, S. Ling, H. Wang, and C. Xing, Eds., vol. 5557 of *Lecture Notes in Computer Science*, Springer, pp. 124–145.

[48] Martin, K. M., Paterson, M. B., and Stinson, D. R. Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. *ACM Transactions on Sensor Networks 7*, 2 (2010).

[49] McEvoy, T. R., and Wolthusen, S. D. Detecting sensor signal manipulations in non-linear chemical processes. In *Critical Infrastructure Protection* (2010), T. Moore and S. Shenoi, Eds., vol. 342 of *IFIP*, Springer, pp. 81–94.

[50] McEvoy, T. R., and Wolthusen, S. D. A plant-wide industrial process control security problem. In *Critical Infrastructure Protection* (2011), J. Butts and S. Shenoi, Eds., vol. 367 of *IFIP Publications*, Springer, pp. 47–56.

[51] Mitchell, C. J., and Piper, F. C. Key storage in secure networks. *Discrete Applied Mathematics 21* (1988), 215–228.

[52] Paterson, K. G., Ristenpart, T., and Shrimpton, T. Tag size does matter: Attacks and proofs for the TLS record protocol. In *ASIACRYPT* (2011), D. H. Lee and X. Wang, Eds., vol. 7073 of *Lecture Notes in Computer Science*, Springer, pp. 372–389.

[53] Pavlovic, D. Dynamics, robustness and fragility of trust. In *Formal Aspects in Security and Trust* (2008), P. Degano, J. D. Guttman, and F. Martinelli, Eds., vol. 5491 of *Lecture Notes in Computer Science*, Springer, pp. 97–113.

[54] Pavlovic, D. Quantum and classical structures in nondeterminstic computation. In *QI* (2009), P. Bruza, D. A. Sofge, W. F. Lawless, K. van Rijsbergen, and M. Klusch, Eds., vol. 5494 of *Lecture Notes in Computer Science*, Springer, pp. 143–157.

[55] Pavlovic, D. Quantifying and qualifying trust: Spectral decomposition of trust networks. In *Formal Aspects in Security and Trust* (2010), P. Degano, S. Etalle, and J. D. Guttman, Eds., vol. 6561 of *Lecture Notes in Computer Science*, Springer, pp. 1–17.

[56] Pavlovic, D. Gaming security by obscurity. In *NSPW* (2011), S. Peisert, R. Ford, C. Gates, and C. Herley, Eds., ACM, pp. 125–140.

[57] Pavlovic, D. Gaming security by obscurity. *CoRR abs/1109.5542* (2011).

[58] Pavlovic, D., and Meadows, C. Bayesian authentication: Quantifying security of the Hancke-Kuhn protocol. *Electronic Notes in Theoretical Computer Science 265* (2010), 97–122.

[59] Pham, V., and Cid, C. Are we compromised? modelling security assessment games. In *GameSec* (2012), J. Grossklags and J. C. Walrand, Eds., vol. 7638 of *Lecture Notes in Computer Science*, Springer, pp. 234–247.

[60] Pieters, W., and Coles-Kemp, L. Reducing normative conflicts in information security. In *Proceedings of New Security Paradigms Workshop 2011* (2011).

[61] Srivatsa, M., Balfe, S., Paterson, K. G., and Rohatgi, P. Trust management for secure information flows. In *ACM Conference on Computer and Communications Security* (2008), P. Ning, P. F. Syverson, and S. Jha, Eds., ACM, pp. 175–188.

[62] Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R. A., Kruegel, C., and Vigna, G. Your botnet is my botnet: Analysis of a botnet takeover. In *ACM Conference on Computer and Communications Security* (2009), E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds., ACM, pp. 635–647.

[63] Walter, C. A duality in space usage between left-to-right and right-to-left exponentiation. To appear in *Proceedings of CT-RSA* (2012).

[64] Walter, C. D. Fast scalar multiplication for ECC over GF(p) using division chains. In *WISA* (2010), Y. Chung and M. Yung, Eds., vol. 6513 of *Lecture Notes in Computer Science*, Springer, pp. 61–75.

[65] Wei, Q., Crampton, J., Beznosov, K., and Ripeanu, M. Authorization recycling in hierarchical RBAC systems. *ACM Transactions on Information and Systems Security 14*, 1 (2011), 3.

[66] Yau, P.-W., Tomlinson, A., Balfe, S., and Gallery, E. Securing grid workflows with trusted computing. In *ICCS (3)* (2008), M. Bubak, G. D. van Albada, J. Dongarra, and P. M. A. Sloot, Eds., vol. 5103 of *Lecture Notes in Computer Science*, Springer, pp. 510–519.

[67] Younan, Y., Philippaerts, P., Cavallaro, L., Sekar, R., Piessens, F., and Joosen, W. PAriCheck: An efficient pointer arithmetic checker for C programs. In *ASIACCS* (2010), D. Feng, D. A. Basin, and P. Liu, Eds., ACM, pp. 145–156.