The Information Security Group
A Brief History

Royal Holloway
University of London

A Brief History of the Royal Holloway Information Security Group
The Early Years

In the early 1980s, the University of London was re-structured to decrease the number of small colleges. Royal Holloway College merged with Bedford College to form Royal Holloway and Bedford New College, but the re-structuring of Mathematics did not follow the university plan.

In the restructuring of Mathematics it was decided that each college should be the University's research centre for one (or more) branches of the subject, and many of the mathematicians were transferred to Royal Holloway with the justification that it would become the centre for discrete mathematics/combinatorics. At that time Fred Piper, who was head of Mathematics at Westfield College (which subsequently merged with Queen Mary College to become Queen Mary and Westfield College), and one of his ex-PhD students Henry Beker, who was a visiting professor at Westfield, had just published their book Cipher Systems. As a result, Fred was asked to direct the discrete mathematics research effort at Royal Holloway with cryptography as one of the focal points.

Fred and Henry transferred to Royal Holloway and Bedford New College in 1985. In order to help establish cryptography, by then an emerging academic discipline, the College provided one new position to the Mathematics department, which was filled by Peter Wild, also an ex-PhD student from Westfield. They were soon joined by Sean Murphy, an SERC funded RA, and a number of PhD students working on topics ranging from cryptography and coding theory to block designs. Simultaneously cryptography was growing in 'popularity', and Royal Holloway was building important strategic relationships with a number of companies. (For example, the position of Head of Mathematics at Racal Comsec was held by a succession of five people who obtained PhD degrees under Fred Piper's supervision. The first of these was Henry Beker, and the second was Chris Mitchell who, in 1985, moved from Racal Comsec to Hewlett Packard Laboratories in Bristol).

In 1987 a number of companies came to Royal Holloway to discuss the possibility of introducing an MSc in Cryptography. Fortunately (with hindsight!) it was felt that this would be too 'narrow', and that a degree in the wider area of Information Security would be more beneficial to industry, and produce more students for Royal Holloway. However, such a broader vocational degree, aimed at producing information security professionals, required staff with much wider interests than simply cryptography.

The first step towards the move from a group of specialist mathematical cryptographers to include more general computer science/information security researchers was to recruit Chris Mitchell from Hewlett Packard in 1990. Chris was appointed as head of the Computer Science Department. This was very rapidly followed by the appointment of Dieter Gollmann as a second computer scientist and Sean Murphy as a Lecturer in Information Security (a shared appointment between Mathematics and Computer Science and the first appointment with Information Security in the title).

The transfer of Chris from HP to the ISG was significant for many reasons. In addition to the ISG recruiting a leading research worker who has played a central role in all its activities, it also led to the foundation of an annual one day Colloquium on Information Security. This colloquium, now known simply as HP day, was essentially a dowry from HP to the ISG to build on an already well established partnership. The experience of working in industry that Chris brought to the ISG and the engagement with practitioners that HP day represents symbolise the two vital ingredients that have enabled the ISG to fulfil Fred's vision of providing the academic support that industry wants.

After considerable consultation with our (ever increasing number of) industrial partners, the MSc in Information Security was launched in October 1992. In some sense this might be regarded as the starting point for the ISG. However at that stage the group only had a very informal structure. Chris was Head of Computer Science, Fred was Head of Mathematics, and decisions were based on friendly agreements rather than formal processes. Furthermore the group consisted of five friends who frequently met for lunch etc., and so there was no need for formal meetings.

Developing and launching this MSc is certainly the greatest single achievement of the ISG, and all the staff at Royal Holloway who have been involved in the growth and development of this course over the last 16 years are enormously proud of the achievements of its many graduates. The MSc was the first of its kind anywhere in the world. From its inception it has always been aimed at meeting the needs of the real world, and the ISG has continued to maintain and develop its strong links with industry and commerce.

One indication of these links with the 'outside world' is the fact that the MSc has always relied on 'outside' lecturers to cover areas where we had no expertise, and to ensure industrial relevance. Indeed, in the early years Chez Ciechanowicz, who later joined the ISG and became MSc programme director, was one of the first!

In the first year the MSc had 7 full-time students and 3 part-timers, one of whom was Andreas Fuchsberger. Andreas subsequently became a research assistant, running the first ISG Lab, sponsored by HP, and later still came back as a lecturer. Having a small number of students enabled the establishment of a family atmosphere with close working relationships between staff and students. During this first year, Pauline Stoner was appointed as Fred's PA and became a focal point for the students to discuss their problems. As the number of students increased Pauline played a crucial role in helping to maintain that family atmosphere.

As the MSc grew in the mid 1990s, the ISG's theme of Academia and Industry in Harmony was developing. One of our main partners was Zergo, founded by Henry Beker, who introduced a structured Information Security training programme on which members of the ISG lectured. This led in 1994 to the Introduction of the Postgraduate Diploma in Information Security, based on courses offered by Zergo and an MSc level dissertation supervised by Royal Holloway academics.

In July 1995, after completing his five-year appointment period, Chris ceased to be Head of Computer Science. This had serious consequences for the ISG, as it necessitated the formalisation of many of the ad hoc agreements about the ISG made between Chris and Fred. At the same time, numbers on the MSc were increasing dramatically, and a case was made for a new lecturer. Chez was appointed in 1996 but, although he was

appointed as a Lecturer in Information Security, he was appointed to the Mathematics Department and not as a joint appointment. At this time John Austen was contracted as a consultant to enhance the MSc by adding the Computer Crime module. In the same year the ISG's research links to industry were enhanced by the establishment of the (part time) Vodafone Chair of Telecommunications, which was filled by Michael Walker.

It is interesting to note that, in order to justify Chez's appointment, the ISG had to accept a target of 30 MSc students. In fact, at the height of the dotcom era we had over 250 MSc students. Luckily for project supervisors and exam markers, numbers later stabilized at about 150!

Eventually, in 1998, all responsibility for Information Security activities was transferred to the Mathematics department. By this point Dieter had left the ISG for a research position at Microsoft Research, but Chris and Sean formally transferred to Mathematics.

The next major landmark was the award to the College of The Queen's Anniversary Prize for Higher and Further Education of 1998. This prestigious award was given in recognition of the work of the ISG with the following citation:

> *"This pioneering Group provides a unique national resource for the training of information security specialists and the development of highly secure communications and computer systems. It offers world-leading independent expertise in a field of crucial importance where trust and integrity are paramount."*

This had the effect of further raising the profile of the ISG. At the same time the need for Information Security was gaining wider recognition, and numbers on the MSc further increased, justifying an increase in ISG staff.

Certainly, the success of the MSc and the subsequent expansion of the group have provided the resources to enable the ISG to make a contribution to the field of information security. But perhaps its greatest asset consists of its students and alumni. Students from a wide variety of backgrounds have brought their different experiences and insights to the MSc to enhance the learning experience for all. And our alumni, now spread throughout the world and in many different companies and enterprises, have continued to support the ISG and contribute to its work.

Given that Fred's initial brief was to build a discrete mathematics research centre, it is not surprising that the initial growth of the ISG and its taught MSc was accompanied by an equal expansion in research activity with, initially, concentration on some of the mathematical aspects of cryptography. Another 'founder' member of the ISG was Mike Burmester. Mike was a finite geometer who had his interest aroused by the cryptography research going on around him. As well as attracting numerous Greek students, Mike was an additional member of the team for supervising projects. He also established a prolific research partnership with Yvo Desmedt (who became a Visiting Professor), and was the ISG's informal 'ambassador' at many international conferences.

The ISG has always been and continues to be a centre for research in mathematical cryptography. Simon Blackburn and Steven Galbraith, both now Professors of Mathematics, began their careers as research assistants in the ISG in the 1990s. However, the group's research has diversified over the years and, as the CVs of current

members of the ISG show, now covers an impressively wide range of Information Security topics. In parallel with the MSc, the early PhD programme in mathematical cryptography and discrete mathematics thrived and expanded into other (mathematical and computer science) areas related to information security. Members of the ISG have supervised well over 100 successful PhD students.

Changes and developments have multiplied rapidly since 2000, and this brief history does not attempt to list all the developments over the last eight years. We conclude by simply listing a few of the most important developments in that time:

- The ISG grew dramatically from the year 2000. The number of full time academic appointments rose to 20; there have been 8 visiting professors and more than 20 post doctoral research assistants. In addition the number of PhD students registered at a given time rose to about 60.
- The range of courses offered as part of the Masters degree has continued to expand. In 1992 there were 4 core and 4 options modules. Between 1996 and 2008 the following modules have been added
    1. Legal and Regulatory Aspects of Electronic Commerce
    2. Security Technologies
    3. Computer Crime
    4. Smart Cards/Tokens Security and Applications
    5. Software Security (development funded by Microsoft)
    6. Trusted Computing (development funded by the EU as part of the Open Trusted Computing project)

  In 2008, development work started on two optional modules to cover Forensics and Penetration Testing, with an intended start date of 2009/10.
- In order to accommodate the need of students with interests focused on e-commerce, an MSc in Secure Electronic Commerce was introduced in 1999. As part of its introduction, there was a need to introduce a course on legal aspects of security, and we were very fortunate to be able to persuade Robert Carolina to begin his association with the group by teaching this course. This MSc ran for five years, and was then restructured to become the “Secure Digital Business” pathway through the Information Security MSc, to which Robert still contributes.
- The Smart Card Centre was founded in October 2002 by Royal Holloway, Vodafone and Giesecke & Devrient. It is a testimony to the reputation of the ISG that the largest mobile operator in the world and one of the largest global card manufacturers, chose to found the centre at Royal Holloway. Six years on the Smart Card Centre has established its own reputation and fulfilled the founders’ primary objective of creating a worldwide centre of excellence for training and research in the field of smart cards, applications and related technologies.
- In 2003 a Distance Learning (DL) version of the technical pathway of the MSc was launched through the External Programme of the University of London, thereby opening up a totally new market for the ISG. Apart from a small time-lag, the DL and campus versions of the MSc are essentially the same. Within the first few years the total number of registrations at any given time grew to its current level of 200 students and the first DL students graduated in 2005.
- In 2008 as a response to industry demands, ISG introduced Block Mode delivery for a substantial proportion of the MSc. In this mode students attend the lectures for a module in an intensive 5-day period. They then complete the exercises and further reading at their own pace. With all the various delivery modes now available, we have developed a totally flexible way of studying the MSc over an

extended period. Furthermore, anyone needing to refresh their knowledge, or to clock up some CPD credits, can enrol for a single module (with or without the corresponding examination).

- We now have the support of a large and impressive group of distinguished Visiting Professors.
- Laboratory facilities for the students have improved dramatically since the early days, and the ISG now has its own highly complex computing environment that needs undivided attention from a full-time Network Manager and supporting System Administrator.

Information Security Group
Royal Holloway
University of London

Egham, 21st July 2008

ISG Members – Past and Present

Academic Staff

Professor Simon Blackburn BSc (Bristol) DPhil (Oxon)
Simon Blackburn received his BSc in Mathematics from Bristol University in 1989 and his DPhil in Mathematics from Oxford University in 1992. From 1992 to 1995, he was a Research Assistant in the Department of Mathematics at Royal Holloway, specialising in Stream Ciphers. From 1995 to 2000, he was an EPSRC Advanced Fellow. He is currently a Professor in Pure Mathematics. His research interests include combinatorics, group theory and cryptography.

Professor Mike Burmester BA (Athens) Dott Mat (Rome, La Sapienza)
Mike is currently a Professor at Florida State University. He is a co-director of SAIT Laboratories, a Center of Academic Excellence in Information Assurance Education as designated by the National Security Agency. Until 2001 he was a Reader in the Information Security Group. His research interest include cryptography, network security, security of pervasive/ubiquitous systems, privacy/anonymity, Watermarking/Fingerprinting and MANETs. Currently he is working on distributed sensor network security, multi-domain trust management, secure RFID systems, secure routing in MANETs and border surveillance

Carlos Cid BSc PhD (UnB, Brazil)
Carlos Cid received his PhD in Mathematics from the University of Brasilia, Brazil, in 1999. After working for a short period as a lecturer in Brazil, he spent a year as a postdoctoral researcher at RWTH-Aachen, Germany. Between 2001 and 2003, he worked as a software engineer for an Irish start-up where he was involved in the design and development of hardware security modules and network security appliances. He joined the Information Security Group in October 2003 as a postdoctoral research assistant to work on the EPSRC-funded project “Security Analysis of the Advanced Encryption Standard (AES)”. He is currently a RCUK Academic Fellow. Carlos has a broad interest in the area of Information Security, in particular cryptography.

Zbigniew ‘Chez’ Ciechanowicz BSc PhD (London) Course Director, Information Security Group
Chez received his BSc (Hons) in Pure Mathematics in 1975 from the University of London, and his PhD degree in Mathematics (also from the University of London) in 1980. He then worked at the National Physical Laboratory for five years specialising firstly in compiler validation, then in cryptography and digital signatures. He ended his stay at the Laboratory holding the rank of Senior Scientific Officer. His next appointment was as a

full-time lecturer in the Computer Science Department of Royal Holloway, his main area of interest being cryptography. Between 1989 and 1995, Chez worked as a consultant at Zergo Ltd, and his main areas of interest there were risk analysis and security management. Whilst at Zergo, he performed numerous security reviews for large Government departments and industrial institutions throughout Europe and the States. He was a principal author of Zergo's own risk analysis method. Between 1996 and 2003, he was the editor of the Elsevier Information Security Technical Report, and is currently still on the editorial board. For an extended period Chez went on secondment to the Information Security Group as a Teaching Fellow, and also as Programme Director for the MSc in Information Security. In 1997 he became a founder member of the British Computer Society's ISEB Information Security Management Certificate Board and sat on the Board until 2004. Chez became a permanent member of the Information Security Group in 2001. He has also served as a member of $(ISC)^2$'s CBK Review Committee. Whilst at Royal Holloway, Chez has been involved in a number of high profile consultancy activities including security studies for TfL's Oyster Card.

Lizzie Coles-Kemp BA (Hull) MSc (London)
Lizzie Coles-Kemp was awarded a BA (Hons) in Scandinavian Studies and Linguistics from the University of Hull in 1988. She worked as a UNIX software trainer and translator. In 1991, she joined the Swedish security software company, Dynamic Software AB, eventually becoming director of the UK subsidiary, DynaSoft Ltd. In 1997, Lizzie left DynaSoft to become global IT Security Officer for the British Council and completed the MSc in Information Security at Royal Holloway. She now subcontracts as a part-time Lead Assessor for Lloyds Register Quality Assurance (LRQA). She contributes to the distance learning version of the MSc in Information Security, tutoring in Security Management and Standards and Evaluation Criteria and module leading for Secure Electronic Commerce and Other Applications. Lizzie was appointed as a Lecturer in 2007 and contributes to the BSc/MSc in Biomedical Informatics which is a collaborative programme between St George's, University of London, Kingston University and Royal Holloway. Her academic research areas are currently risk assessment, organization theory, complex adaptive systems theory applied to decision-making and management systems. Lizzie is completing a PhD in information security management at King's College, London.

Jason Crampton BSc (Manchester) MSc PhD (London)
Jason Crampton was awarded a BSc (Hons) in Mathematics from the University of Manchester in 1986. He worked as a maths teacher for several years and then for a trade union developing software for the collection, recording and reporting of subscription income. He completed a part time MSc in Computer Science in 1996 and a PhD in 2002, both at Birkbeck, University of London. He joined the Information Security Group as a lecturer in 2002 and became a Reader in Information Security in 2007. His research interests include role-based access control and the application of discrete mathematics to computer security. He has published over 40 papers in refereed conferences and journals. He is an associate editor of ACM Transactions on Information and System Security.

Alex Dent M.Maths (Oxon) PhD (London)
Alex Dent received his undergraduate degree from St. Peter's College, Oxford, in 1998 and his doctorate from Royal Holloway in 2001. At the end of his doctorate, he joined the staff of the Information Security Group as a research assistant for the NESSIE algorithm evaluation project. During this project, he was part of the team responsible for evaluating the security of a series of public-key cryptosystems and the result of his work directly influenced the contents of several security standards. In 2004, he was awarded a prestigious EPSRC Junior Research Fellowship, one of ten awards made that year, to continue his research on the theory of provable security in public-key encryption schemes. In 2006, he was employed as a full-time lecturer at Royal Holloway. His main research interests are in the theory of provable security and how this theory can be applied to public-key cryptosystems.

Andreas Fuchsberger BSc MSc (London) EUR ING CEng MBCS CITP CISSP-ISSAP
Andreas is primarily an Information Security Technologist for the Connected Information Security Group (CISG) of Microsoft. Prior to that he was a full-time academic member of staff in the Information Security Group. He has over 18 years of experience in teaching IT security architecture, design and programming. Over the years Andreas has lectured in the areas of network, computer and software security. He has published articles on programming and network security, intrusion detection/prevention and vulnerability analysis. From 1999 until 2000 he was employed as a principal Consultant for ISS until he joined eSecurity Inc as Technical Manager for EMEA. He rejoined the ISG in 2003. He received a BSc (Hons) in Computer Science in 1992 and an MSc in Information Security in 1993, both from Royal Holloway, University of London. Andreas holds CISSP and ISSAP credentials of $(ISC)^2$. He is a registered Chartered Engineer (CEng) of the Engineering Council UK as well as a EUR ING of Fédération Européenne d'Associations Nationales d'Ingénieurs (FEANI). Andreas is still a part-time lecturer for the ISG.

Steven Galbraith BCMS (Waikato) MS (Georgia Tech) DPhil (Oxon)
Steven Galbraith was awarded a Bachelor in Computing and Mathematical Sciences from the University of Waikato in New Zealand in 1989, a Master of Science from Georgia Tech in the USA in 1991, and a Doctorate from Oxford University in 1996. He has held research positions at the Centre for Applied Cryptographic Research at the University of Waterloo, Canada, and at the Institute for Experimental Mathematics in Essen, Germany. His research interests include computational number theory, computational algebraic geometry and public key cryptography. Steven has recently been awarded an EPSRC Advanced Fellowship entitled "A long view of curves in cryptography".

Hilary Ganley BSc PGCE Dip Comp Sci MSc (London)
Hilary Ganley received her BSc in Mathematics (Hons) from Royal Holloway in 1968. An early career as a teacher of mathematics included posts in England, Scotland and the US. Following a career break, she moved into Computing Science within Higher Education, initially part-time at Glasgow University and then the Open University. For the next 10 years, she was (full-time) Director of the MSc in Information Technology at Glasgow University, an interdisciplinary taught postgraduate course of 160 students and was appointed as Senior Lecturer in 1999. This period involved a major course review and curriculum development word as well as intensive teaching of programming and software development to MSc students. Following the completion of the MSc in Information Security (Distinction) at Royal Holloway, she accepted a role within the Information Security Group to co-ordinate the development of the online version of the MSc in Information Security for distance learning. Following its launch in 2003, this programme now successfully delivers this highly regarded degree programme to students worldwide who are unable to attend the campus programme. Hilary retired from the ISG in 2008.

Kwok Lam BSc (London) PhD (Cambridge)
Kwok obtained his BSc (Hons) in Computer Science at Royal Holloway (1987) and his PhD, also in Computer Science, from Cambridge University. He was appointed as a Lecturer in Computer Science and taught on the MSc between 1992 and 1993. He went on to lecture at the National University of Singapore, eventually started his own company (Privylink) where he employed a range of ex-MSc students. He is currently a professor at Tsinghua University in Beijing.

Professor Dieter Gollmann Dipl.-Ing. Dr.tech. (University of Linz)
Dieter received his Dipl.-Ing. in Engineering Mathematics (1979) and Dr.tech. (1984) from the University of Linz, Austria, where he was a research assistant in the Department for System Science. He was a Lecturer in Computer Science at Royal Holloway, University of London, and later a scientific assistant at the University of Karlsruhe, Germany, where he was awarded the 'venia legendi' for Computer Science in 1991. He rejoined Royal Holloway in 1990, where he was the first Course Director of the MSc in Information Security. He was a Visiting Professor at the Technical University of Graz in 1991, an Adjunct Professor at the Information Security Research Centre, QUT, Brisbane, in 1995, and has acted as a consultant for HP Laboratories Bristol. He joined Microsoft Research in Cambridge in 1998. In 2003, he took the chair for Security in Distributed Applications at Hamburg University of Technology, Germany. He is a Visiting Professor with the Information Security Group at Royal Holloway, a Visiting Professor with the School of Software at Tsinghua University, Beijing, and an Adjunct Professor at the Technical University of Denmark.

Dieter Gollmann is one of the editors-in-chief of the International Journal of Information Security link.springer.de/link/service/journals/10207/ and an associate editor of the IEEE Security & Privacy Magazine http://www.computer.org/security/. His textbook on 'Computer Security' has now appeared in its second edition.

Konstantinos Markantonakis BSc (Lancaster) MSc MBA PhD (London)
Konstantinos received his BSc (Hons) in Computer Science from Lancaster University in 1995, his MSc in Information Security in 1999, his PhD in 2000 and his MBA in International Management in 2005 from Royal Holloway, University of London. His main research interests include smart card security and applications, secure protocol design, Public Key Infrastructures, key management, mobile phone security. Since completing his PhD, he has worked as an independent consultant in a number of information security and smart card related projects. He has worked as a Multi-application smart card Manager in VISA International EU, responsible for multi-application smart card technology for southern Europe. More recently, he was working as a Senior Information Security Consultant for Steer Davies Gleave, responsible for advising transport operators and financial institutions on the use of smart card technology. He is also a member of the IFIP Working Group 8.8 on Smart Cards. He is currently a Reader in the Information Security Group. He continues to act as a consultant on a variety of topics including smart card security, key management, information security protocols, mobile devices, smart card migration program planning/project management for financial institutions and transport operators.

Professor Keith Martin BSc (Glasgow) PhD (London) CMath FIMA
Keith Martin joined the Information Security Group as a lecturer in January 2000. He received his BSc (Hons) in Mathematics from the University of Glasgow in 1988 and a PhD from Royal Holloway in 1991. Between 1992 and 1996 he held a Research Fellowship at the University of Adelaide, investigating mathematical modeling of cryptographic key distribution problems. In 1996 he joined the COSIC research group of the Katholieke Universiteit Leuven in Belgium, working on security for third generation mobile communications. Keith's current research interests include cryptography, key management and wireless sensor network security. Keith played a major role in the development of Royal Holloway's distance learning MSc Information Security and is currently the Director of Graduate Studies. He is an Associate Editor of IEEE Transactions on Information Theory in the area of Complexity and Cryptography.

Keith Mayes BSc PhD (Bath) CEng MIEE
Keith received his BSc (Hons) in Electronic Engineering in 1983 from the University of Bath and his PhD degree in Digital Image Processing (also from the University of Bath) in 1987. During his first degree, he was employed by Pye TVT (Philips) which designed and produced TV broadcast and studio equipment. His PhD was sponsored by Honeywell Aerospace and Defence and, on completion, he accepted their offer of a job. In 1988, he started work for Racal Research Limited (RRL), at a time when Racal owned its core defence business, Chubb, and a small company called Vodafone. During seven years at RRL, he worked on a wide range of research and advanced development products and was accepted as a Chartered Engineer. In 1995, he joined Racal Messenger to continue work on a Vehicle Licence plate recognition system (Talon) and an early packet radio system (Widanet/Paknet). In 1996, Keith joined Vodafone as a Senior

Manager working within the Communication Security and Advanced Development group, under Professor Michael Walker. Early work concerned advanced radio relaying systems and involved participation in international standardisation. Later, he led the Maths & Modelling team and eventually took charge of the 20 strong Fraud & Security group. During this time, he was training in intellectual property and licensing, culminating in membership of the Licensing Executives Society and the added responsibility for patent issues in Vodafone UK. Keith is named inventor on many patent applications. In 2000, following some work on m-commerce and an increasing interest in Smart Cards, he joined the Vodafone International organisation as the Vodafone Global SIM Card Manager, responsible for SIM card harmonisation and strategy for the Vodafone Group. In 2002, Keith left Vodafone to set up his own Telecoms Consulting Company (Crisp Telecom) and in November 2002, he also started as the Director of the Smart Card Centre at Royal Holloway.

Professor Chris Mitchell BSc PhD (London) CMath FBCS FIMA
Chris Mitchell received his BSc (1975) and PhD (1979) degrees in Mathematics from Westfield College. Prior to his appointment in 1990 as Professor of Computer Science at Royal Holloway, he was a Project Manager in the Networks and Communications Laboratory of Hewlett-Packard Laboratories in Bristol, which he joined in 1985. Between 1979 and 1985, he was at Racal-Comsec Ltd. (Salisbury, UK), latterly as Chief Mathematician. He helped found the Information Security Group in 1990, and, in 1992, played a part in launching the MSc in Information Security. His research interests mainly relate to Information Security and the applications of cryptography.

Chris has played an active role in a number of international collaborative projects including Open Trusted Computing, a current EU 6th framework Integrated Project; the Mobile VCE Core 2 and Core 3 programmes; four EU 5th Framework projects (SHAMAN and PAMPAS on mobile security, USB_Crypt dealing with novel security tokens, and the Finger_Card project combining smart cards and biometrics); and two EU ACTS projects on security for third generation mobile telecommunications systems (USECA and ASPeCT). He is currently convenor of Technical Panel 2 of BSI IST/33, dealing with security mechanisms and providing input to ISO/IEC JTC1/SC27, on which he has served as a UK Expert since 1992. He has edited 10 international security standards and published well over 200 research papers. He is a member of Microsoft's Trustworthy Computing Academic Advisory Board, the DoCoMo Euro-Labs Advisory Board, and the editorial boards of The Computer Journal and the International Journal of Information Security. He continues to act as a consultant on a variety of topics in information security.

Professor Sean Murphy BA (Oxon) PhD (Bath)
Sean Murphy received a BA in Mathematics from Oxford University in 1985 and a PhD in Mathematics from the University of Bath in 1989. He has been at Royal Holloway since 1988 and is currently a Professor of Mathematics. His research interests centre on cryptology. He was a member of the

European NESSIE project for evaluating cryptographic standards and of the executive committee of ECRYPT, the European Network of Excellence in Cryptology. He is a co-author of the books *Cryptography: A Very Short Introduction* and *Algebraic Aspects of the Advanced Encryption Standard*.

Siaw-Lynn Ng BSc (Adelaide) PhD (London)
Siaw-Lynn Ng was awarded a BSc (Hons) degree in Mathematics and Computer Science from the University of Adelaide in 1995 and a PhD in Mathematics from Royal Holloway in 1998. She was a postdoctoral research assistant at Royal Holloway from 1998 to 2001. Her research interests include combinatorics, finite geometry and their applications in information security. Siaw-Lynn was appointed as a lecturer in 2001.

Professor Kenny Paterson BSc (Glasgow) PhD (London)
Kenny Paterson obtained his BSc (Hons) in 1990 from the University of Glasgow and a PhD from the University of London in 1993, both in mathematics. He was a Royal Society Fellow at the Swiss Federal Institute of Technology, Zurich, from 1993 to 1994, investigating algebraic properties of block ciphers. After that, he was Lloyd's of London Tercentenary Foundation Fellow at the University of London from 1994 to 1996, working on digital signatures. He joined the mathematics group at Hewlett-Packard Laboratories, Bristol, in November 1996, becoming project manager in 1999. His technical work there involved him in international standards setting, internal consultancy on a wide range of mathematical and cryptographic subjects, and intellectual property generation. He joined the ISG in 2001. Kenny's research interests span a wide range of topics: cryptography and protocols, network security, sequences, coding theory and information theory.

Professor Fred Piper BSc PhD (London) ARCS DIC CEng CMath FIET FIMA FICA MBCS CISSP CISM
Director of External Relations, Information Security Group
Fred Piper was appointed Professor of Mathematics at the University of London in 1975 and has worked in information security since 1979. In 1985, he formed a company, Codes & Ciphers Ltd, which offers consultancy advice in all aspects of information security. He has acted as a consultant to over 80 companies including a number of financial institutions and major industrial companies in the UK, Europe, Asia, Australia, South Africa and the USA. The consultancy work has been varied and has included algorithm design and analysis, work on EFTPOS and ATM networks, data systems, security audits, risk analysis and the formulation of security policies. He has lectured worldwide on information security, both academically and commercially, has published more than 100 papers and is joint author of *Cipher Systems* (1982), one of the first books to be published on the subject of protection of communications, *Secure Speech Communications* (1985), *Digital Signatures - Security & Controls* (1999) and *Cryptography: A Very Short Introduction* (2002). Fred has been a member of a number of DTI advisory groups. He has also served on a number of Foresight Crime Prevention Panels and task forces concerned with fraud control, security and privacy. He is currently a member of the Scientific Council of the Smith

Institute, the Board of Trustees for Bletchley Park and the Board of the Institute of Information Security Professionals. He is also a member of (ISC)^2's European Advisory Board, the steering group of the DTI's Cyber Security KTN, ISSA's advisory panel and the BCS's Information Security Forum. In 2002, he was awarded an IMA Gold Medal for "services to mathematics" and received an honorary CISSP for "leadership in Information Security". In 2003, Fred received an honorary CISM for "globally recognised leadership" and "contribution to the Information Security Profession". In 2005 he was elected to the ISSA Hall of Fame. In 2008 he was elected to the InfoSecurity Europe Hall of Fame and to be a Fellow of (ISC)^2.

Geraint Price BSc (London) PhD (Cantab)
Geraint Price obtained his BSc in Computer Science from Royal Holloway, University of London in 1994 and his PhD from University of Cambridge in 1999. His PhD dissertation analysed the interaction between Computer Security and Fault Tolerance. From 1999 to 2001, he was a Research Associate within the University of Cambridge, working on projects related to Denial of Service attacks in networks. In November 2001, he joined the Information Security Group as a Research Assistant to work on a project funded by PricewaterhouseCoopers on the future of Public Key Infrastructures. From late 2002 to mid 2004, he worked on a research project funded by the PKI Club at Royal Holloway. In Sept 2004, Geraint was appointed as lecturer in Information Security. His current research interests include Public Key Infrastructures, Authentication and Identity Management, Denial of Service attacks and resilient security.

Matt Robshaw BSc (St. Andrews) PhD (London)
Matt received his BSc (Hons) from the University of St. Andrews and his PhD from the University of London. After finishing his PhD, he worked for more than six years at RSA Laboratories in the U.S. where, during the late 1990's, he was both Principal Research Scientist and manager of the west coast (California) office. After returning to Europe in 1999, he joined the Information Security Group at RHUL and, as Reader in Information Security, contributed to a broad range of activities in the M.Sc., both on-site and as part of the distance learning degree. In 2005, Matt returned to industry and he is currently based in Paris at Orange Labs (previously known as France Télécom Research and Development). There, as Senior Cryptographic Expert within the Middleware and Advanced Platforms group, his activities are focused on the development and deployment of cryptographic techniques for both existing and new applications.

Scarlet Schwiderski-Grosche Diplom-Informatikerin (Germany) PhD (Cambridge)
Scarlet finished her degree in Computer Science at the Technical University of Braunschweig with the degree of "Diplom-Informatikerin" in 1992. She was awarded a PhD in distributed systems technology (on composite event detection in distributed systems) from Cambridge University in 1996. After a one-year postdoctoral research position in Cambridge, Scarlet worked as a

postdoctoral researcher in Darmstadt (Germany) at the GMD - German National Research Centre for Information Technology (now part of Fraunhofer) on biometrics and wireless communication protocols. In August 2001, she joined the Information Security Group to work on an EU-project called SHAMAN (www.ist-shaman.org). Scarlet was appointed as lecturer in Information Security at the beginning of 2003. Her special interests are security in mobile wireless networks, ID management and Biometrics.

Allan Tomlinson BSc (Strathclyde) MSc PhD (Edinburgh)
Allan Tomlinson received his BSc in Applied Physics from Strathclyde in 1981, his MSc in Microelectronics in 1987 and doctorate in 1991, both from Edinburgh. He then joined the Institute of Microelectronics at the National University of Singapore, working on secure NICAM broadcasting and video compression. In 1994, he moved to GI in California to work on the Digicipher II Conditional Access system for digital video broadcasting. Before joining the Information Security Group, he was Principal Engineer at Barco Communications Systems where he was responsible for the development of the “Krypton” DVB Video Scrambler. He also served for a number of years on the DVB Simulcrypt committee. He is currently a lecturer in the Information Security Group.

Professor Michael Walker BSc PhD (London) Dr.rer.nat.(habil) (Tübingen) FREng FIEE CMath FIMA
Michael Walker is the Research and Development Director for the Vodafone Group, the Vodafone Professor of Telecommunications at Royal Holloway and a visiting professor at the University of Surrey. He is responsible for research and development across the Vodafone Group, including the company’s contributions to international standards and protection of its intellectual property. His work is concerned in the broadest sense with wireless and Internet communications. This includes spectrum, radio access, telecommunications networks, security of communications and applications in commerce, transport and other areas. Prior to joining Vodafone, he was Head of Mathematics at Racal Research Ltd, where he led a number of UK and EU collaborative projects on security for mobile communications and designed cryptographic algorithms, security and coding schemes for commercial and military systems. He also acted as a security consultant to a number of financial institutions. Before joining Racal, he was a lecturer at the University of Tübingen where his research interests included finite geometry, groups, combinatorics and coding theory. Professor Walker has been chairman of a number of international standards groups, including 3GPP SA3, which is responsible for the security of the GSM and UMTS mobile communications systems. He is a member of the UK Government Technology Strategy Board, and sits on academic advisory boards at the Universities of Surrey and Warwick.

Professor Peter Wild BSc (Adelaide) PhD (London) Director, Information Security Group
Peter Wild received his BSc (Hons) degree in Pure Mathematics in 1976 from the University of Adelaide and the PhD degree in Mathematics in 1980 from the University of London. He has worked at the Ohio State University, Columbus, Ohio, the University of Adelaide and the CSIRO, Australia. In

1984, he joined Royal Holloway where he is currently employed as a Professor in Mathematics and is the Director of the Information Security Group. He is an Editor-in-Chief of Designs, Codes and Cryptography and is a member of the Scientific Committee of the Knowledge Transfer Network for Industrial Mathematics. His research interests are in combinatorics, design theory, cryptography and coding theory. He has held visiting appointments at the University of Adelaide, the University of Wollongong and Macquarie University, Australia, the University of Hong Kong and the Nanyang Technological University, Singapore. He has acted as a data security consultant for a number of companies offering advice in algorithm analysis, key management and user identification protocols.

Stephen Wolthusen Dipl.-Inform. Dr.-Ing. (TU Darmstadt)
Stephen received his Dipl.-Inform. in computer science in 1999 and completed his PhD in theoretical computer science in 2003, both at TU Darmstadt, Germany, where he was also active as lecturer in the graduate program from 1999 to 2005. From 1999 to 2005, he was with the security technology department at Fraunhofer-IGD, first as a member of the academic staff and then as deputy division chief; he retains an affiliation with the institute as senior scientist. While at Fraunhofer-IGD, Dr. Wolthusen was responsible for the scientific and administrative direction of research projects for both national government agencies and industry and has actively led several international research projects. Since 2005, he also holds an associate professorship at the Norwegian Information Security Laboratory at Gjøvik University College, Norway. Dr. Wolthusen is author of several books, has edited multiple conference proceedings volumes and also holds several German and international patents. He is vice chair of the IEEE Task Force on Information Assurance, a member of the IEEE Standardization Committee on Information Assurance, and a member of IEEE, ACM, the German Gesellschaft für Informatik and the American Mathematical Society. He is also initiator and inaugural program chair of two IEEE conference series on information assurance and on critical infrastructure protection. His primary research interests are in the areas of information assurance and the use of formal methods for modelling, specification and verification as well as models and analytical techniques for the protection of critical infrastructures.

Visiting Professors & Senior Visiting Fellows

Professor Henry Beker BSc PhD (London) BA (Open University) FREng CEng CMath CStat CSci

In 1988, Henry J Beker founded Zergo Limited (which later became Baltimore Technologies plc) and, as Chairman and Chief Executive, steered the company through listings on both sides of the Atlantic and presided over its phenomenal growth. Prior to this, Henry Beker was Managing Director of Racal-Guardata Ltd, having previously held positions of Head of Mathematics Department, Racal Comsec Ltd, and Research Director at Racal Research Ltd. In addition to providing security systems to a number of financial institutions worldwide, Henry Beker has also been very actively involved within various Standards bodies. This includes the American National Standards Institute's work on wholesale and retail banking and the Standards Association of Australia formulating their EFTPOS Standards. He is joint author of *Cipher Systems* (1982), one of the first books to be published on the subject of protection of communications, and *Secure Speech Communications* (1985). From 1987 to 1989, he was Vice-President of the IMA, and was appointed President in 1998. Having relinquished his roles at Baltimore Technologies plc of Chief Executive (in 1999) and Chairman (in 2000), Henry is now devoting more time to his academic, educational and business interests. He was Founding Chairman of the e-Learning Foundation initiative to provide portable computers for every schoolchild in the UK and was instrumental in engaging governmental interest. Henry is Chairman of Bladerunner Ltd, a leading health and fitness company.

Robert Carolina BA (Dayton) JD (Georgetown) LL.M (London) Attorney-at-Law (Illinois, USA), Solicitor (England & Wales) Senior Visiting Fellow

Robert Carolina qualified as a lawyer in 1991 and became an in-house lawyer with an Internet software developer in the US. He then worked in the specialist information technology law practice of Clifford Chance, the world's largest law firm. He was subsequently a Partner at Landwell, the legal services arm of PricewaterhouseCoopers. Robert is now a Principal with Origin Ltd, a solicitors' firm regulated by the Law Society of England and Wales. The firm engages in patent prosecution, technology transfer, IP portfolio analysis and valuation, IP litigation and IT regulatory matters. His practice focuses on legal protection of information technology inventions, technology transfer deals and regulation of information technology systems. He represents inventors, users, purchasers, vendors of IT and telecommunications products and services, and advises on electronic commerce transactions and projects. His clients include early stage businesses, private and public IT and communications companies, as well as major multinational financial institutions, located in Europe and the US.

Professor Whitfield Diffie BSc (MIT) Dr. sc. techn. (hc, ETH Zurich)
Whitfield Diffie, Chief Security Officer of Sun Microsystems, has been at Sun since 1991. Prior to Sun, Diffie was Manager of Secure Systems Research at Northern Telecom, a position he held since 1978. Best known for his 1975 discovery of the concept of public key cryptography, Diffie spent the 1990s working primarily on the public policy aspects of cryptography. His position in opposition to limitations on the business and personal use of cryptography is the subject of a recent book, *Crypto*, by Steven Levy of Newsweek. In addition, Diffie has been featured in articles of multiple publications, New York Times Magazine, Newsweek, Wired, Omni, and Discover as well as on CNN, the Discovery Channel, the BBC and the Japanese TV network NHK. Diffie is a fellow of the Marconi Foundation and author, jointly with Susan Landau, of the book *Privacy on the Line*. Diffie is a graduate in mathematics of MIT and Dr. sc. techn. (hc) of the ETH in Zurich. In 2008 he was awarded an honorary Doctorate of Science at Royal Holloway.

Professor Chris Holloway MA (Cantab) FIEE CEng
Chris Holloway was Chief Architect for the IBM Financial Services Sector. He had global responsibility for the IT architecture to support Banks, Insurance Companies and Financial Markets institutions. Chris was appointed the sector's Technical Strategy Program Manager for Europe, Middle East and Africa (where he co-lead the sector's community of senior IT Architects in Europe and chaired the Global Architecture team for the financial services sector). He served as elected Vice President of the IBM Academy of Technology for EMEA from 2001 to 2003. After 28 years in the Finance Sector, Chris is an acknowledged European authority on transaction security, with 18 patents filed covering the use of smart cards and cryptography, of which 11 have so far been granted. He has designed and implemented pioneering cryptographic solutions for multi-organisation community networks, including for example a stock exchange network designed to interconnect 400 financial institutions, and an inter-bank payments and clearing network for high value transactions. Both of these had smart-cards at the heart of their security solutions. Chris has spoken at many international conferences. He is a Fellow of the Institution of Electrical Engineers; a Chartered Engineer; a member of the Engineering and Physical Sciences Research Council peer review college; a member of the IBM Academy of Technology, and was appointed to the IBM corporate technical executive position of Distinguished Engineer. He retired from IBM in 2008 to pursue a number of charitable activities.

Professor David Naccache PhD (Paris)
David Naccache is a researcher at the Ecole normale supérieure's Computer Science Department and Professor at the University of Paris II (Panthéon-Assas) where he heads a computer forensic MSc Programme. Before joining academia, David directed Gemplus' research labs (now Gemalto). David received his PhD in 1995 from the Ecole nationale supérieure des télécommunications, Paris, and his habilitation thesis from the University of Paris VI in 2004. He has published 70 papers in information security and cryptography, filed 60 patents and served in 45

programme committees. David is currently an advisory Professor at the Beijing JiaoTong University, China, a Forensic Expert by the Court of Appeal, Paris, and a reserve Major (RC). His current areas of interest are public key cryptography and side channel attacks.

Professor Nelson Stephens BSc PhD (Manchester)
Nelson Stephens was awarded his PhD in 1965 on "Conjectures concerning elliptic curves" from the University of Manchester. He has held academic appointments in the UK at the Universities of East Anglia, Oxford, Cardiff and London. He has held visiting research positions at the universities of Paris-Sud, Saarbrücken, Concordia in Montreal, Erasmus in Rotterdam and at the Max-Planck Institute, Bonn. In 1988, he held an Industrial Fellowship with British Telecom. His research interests include information security, algorithms and number theory. He has authored over 60 papers in journals, books and refereed conference proceedings. He now works as a consultant.

Professor Richard Walton CB BSc PhD (Nottingham) BA (Open University) CMath CSc CEng FIMA FIET MBCS AIISP
Richard received his BSc (Hons) and PhD in Mathematics from the University of Nottingham in 1968 and 1971 respectively. He studied with the Open University during the 1980s, taking mainly Electronics courses and received his BA (Hons) in 1987. From 1971 to 1973, he was a lecturer in Mathematics at the North Staffordshire Polytechnic before joining GCHQ as a Mathematician at the end of 1973. His GCHQ career culminated in his appointment in January 1999 to the GCHQ Board as Director CESG, the National Technical Authority for Information Assurance. He held this post until October 2002 when he was seconded to the Cabinet Office for six months to lead the production of a National Strategy on Information Assurance. His earlier posts included Head of the Division, employing most of the GCHQ Mathematicians (1996-1999) and Head of the Mathematical Services Group in CESG (1985-1991). In the 1980s, he initiated many of the changes in CESG's public profile as they started to engage in open fora, both national and international, during the early stages of the development of open standards for computer security. He was the first member of GCHQ to attend open cryptographic conferences (Eurocrypt in 1982; Crypto in 1985). His actions were instrumental in achieving the change of GCHQ policy to publish the early CESG work on Public Key Cryptography. He was appointed CB in the 2003 New Year's Honours list. He is a member of the Defence Scientific Advisory Council, and the IT Sector Panel of the Institute of Engineering and Technology. In 2003, he formed a company, Walton-Mackenzie Limited, which offers consultancy on a variety of Information Assurance topics.

Consultants, Technical & Administrative Staff

John Austen BA FBCS NEBSS
John Austen is a director of QCC InfoSec Training Ltd and Course Director for the Royal Holloway Diploma in Information Security. He was the Head of the Computer Crime Unit, New Scotland Yard, until September 1996. He was a career detective for 30 years, investigating the first major UK computer crime in 1976 and founding the Computer Crime Unit in 1984, the first of its type in the world. He was responsible for the first successful arrests and prosecutions against hackers, organised crime groups and information brokers. He trained all of his own staff, officers from each of the UK Police Forces and latterly police from Eastern Europe on courses held at the National Police Staff College (in Bramshill, Hampshire). John was the first Chairman of the Interpol Computer Crime Committee, serving from 1991 to 1996, and was responsible for the worldwide standardisation of Police procedure. He is a Fellow of the BCS and a member of its Security Committee. He is a consultant to the Government on Computer Security, the Computer Misuse Act and British Standard 7799. He is a scientific expert to the Legal Affairs Committee, Council of Europe, and a contributor to its Recommendation for Criminal Procedural Law on Computer Related Crime. He has been an official advisor to the Governments of the Czech Republic, Poland and Croatia. He joined the ISG as a Consultant in 1996 and delivers the Computer Crime module on the MSc programme.

Tristan Findley BSc (Portsmouth)
Tristan graduated from the University of Portsmouth in 2006 with a BSc in Computer Network Management and Design. He has worked in the IT industry for over six years in various capacities. He is currently focusing on security and networking technologies. He joined the ISG in 2006 as systems administrator.

Mick Ganley BSc PhD (London)
Mick graduated from Royal Holloway in 1968 with a BSc in Mathematics and obtained a PhD in Algebra and Geometry from Westfield College in 1971. He held academic appointments in the Mathematics Departments at York University and Glasgow University, with time spent at Washington State University and the University of Western Australia. His primary research interests were in the areas of combinatorics, geometry, algebra and number theory. In 1987, Mick moved into industry, working for the cryptographic security division of Racal. He was made a Racal Senior Manager and appointed as Head of Consultancy and Security Analysis. His main functions included managing all security analysis, audit and consultancy activities carried out by the security division; liaising with other Racal companies; providing security input from research work, new techniques and conference/press feedback; liaising with CESG and the DTI on various security issues relating to the company and carrying out research work, and presenting results in published papers and at conferences. In 2000, Mick left Racal to take up the position of Director of

Consultancy at Cylink Consultancy Ltd. He left the company in mid-2002 to work as a freelance security consultant. He has a contract with the ISG, including developing Distance Learning (DL) material, and is currently Programme Director for the DL MSc.

Jon Hart BEng MEng (Brunel)
Jon received a joint BEng and MEng in Electronic and Computer Engineering from Brunel University in 2003. He has over nine years' experience in IT support and computer and network security, specialising in LINUX and UNIX platforms. Before joining the ISG as systems administrator, Jon worked in the defence industry for two years as a software engineer.

Pauline Stoner
Pauline joined the Maths Department as a part-time Secretary in January 1992 working for Gar de Barra who was Head of Department, moved to the Personnel Department in October 1992 to work as Personal Secretary to the Head of Personnel. In March 1993, when Fred took over as Head of Department and Director of the ISG, she returned to the Maths Department as PA to Fred and Departmental Secretary where she has been ever since.

ISG - The Beginning

Taewan Park, Auden Jøsang, Peter Wild, Chris Mitchell, Sean Murphy, Paul Andrews
Eddie Hammond, Sae Joon Kim, Raymond Ngai, Andrew Chang, Auden Josang, Torsten Arnold
Dieter Gollmann, Andreas Fuchsberger, Fred Piper, Charles Sibanda

Royal Holloway
University of London