



REPORT

WORLD CYBER SECURITY TECHNOLOGY RESEARCH SUMMIT

BELFAST 2011



About CSIT

The Centre for Secure Information Technologies (CSIT) is an innovation and knowledge centre (IKC) based at Queen's University of Belfast's, Institute of Electronics, Communications and Information Technology (ECIT) in the Northern Ireland Science Park, Belfast. With the total funding in the region of £30M over five years, CSIT is creating the security infrastructure needed to safeguard trustworthiness of digital information, both at home and in the workplace. The centre brings together research specialists in complementary fields such as data encryption, network security systems, wireless enabled security systems and video analytics. CSIT is looking at both information and people security and is focused on securing hyperconnected networks and transport corridors.

About Belfast 2011

The World Cyber Security Technology Research Summit, Belfast 2011, brought together experts in the field of cyber security from leading research institutes, government bodies and industry throughout the world.



Photograph of (most) attendees:

Left to right: Stephen Wray (CSIT), Andrew Tryer (TSB), George Redpath (Tyco International), Michael Loughlin (CSIT), You Sung Kang (ETRI), Chris Rampton (Home Office), Maire O'Neill (CSIT), Michael Kirton (CESG), Sandy Bird (Q1 Labs), Mark Crosbie (IBM), Duncan Curry (Qosmos), Paul Millar (CSIT), Philip Mills (CSIT), Ian Bryant (MOD), Colin Kerry (BAE Systems), Bill McCluggage (Cabinet Office), Robert Heathman (EPSRC), Mike Corcoran (DSTL), Sakir Sezer (CSIT), Chris Firth (Thales), Chris Ensor (CESG), Phil Sutton (MOD), Eul Gyu Im (Hanyang University Korea), Virgil Gilgor (Cylab), David Maxwell (InvestNI), John McCanny (CSIT), Dong Kyue Kim (Hanyang University Korea), Godfrey Gaston (CSIT), Patrick Traynor (Gorgia Tech University), Michael McVeigh (Seven Technologies), Steve Orr (NISP Connect), Tony Bull (Thales), Erfan Ibrahim (EPRI), John Bumgarner (US Cyber Consequences Unit), Tony Dyhouse (QinetiQ & ICT KTN), Gavin McWilliams (CSIT), David Callaghan (Thales).

Executive Summary

The protection of cyber space, including the Internet and mobile platforms, is vital as the exploitation of cyber space vulnerabilities continues to cost individuals, governments and industry dear. The World Cyber Security Technology Research Summit, Belfast 2011 has collected views from experts in the field of cyber security on current and future issues in cyber security, and has agreed a collective strategy for further cyber security research.

Discussion of current cyber security threats in the Summit highlighted that these come from a variety of sources and spaces, are multilateral, multipurpose, sophisticated and self-learning, and are difficult to attribute to their originator. It was noted that cyber attacks are increasingly instigated against diverse targets, such as individual users, research, government and military establishments, and national infrastructure.

A wide range of future cyber security requirements were suggested and deliberated. The development of a set of scientific foundations for cyber security was proposed, enabling a better understanding of emerging security threats introduced by new technologies and new attack scenarios. Adaptive cyber defence is required in order to address the evolutionary process of cyber space and cyber threats. This will involve

enhancement of system awareness enabling early attack detection and self configuration to defend against an attack and the development of self-learning cyber systems. Smart systems, such as smart utility grids, were identified as a field in which cyber attacks would grow and where cyber security research is critical. The mobile space was highlighted as vulnerable to cyber attacks, which would increase as usage of this space increases. Discussion also focussed on the awareness that, in order to develop effective defence against cyber attacks, cyber security technology research must be combined with consideration of other influences on cyber space, such as the economics of cyber space, societal issues such as trust, the development of global cyber space policies and use regulations, the requirement for innovative cyber security education and the necessity for usable cyber security with human-oriented security policies and tools.

The collective research strategy identified four research themes critical to the ongoing creation of cyber security defences:

1. **Adaptive Cyber Security Technologies** - research objectives in this area would include the development of self-learning cyber security technologies; self-awareness in cyber systems; the establishment of feedback in cyber systems to learn from cyber attacks
2. **Protection of Smart Utility Grids** - research aims in this field could comprise: smart grid requirements gathering methodology; protection technologies for smart grids components; secure technologies for smart grid communications;

smart grid and home area network integration that provides for the privacy and security of collected information; development of smart grid standards

3. **Security of the Mobile Platform and Applications** - research in this space should target not only malicious applications, but also mobile cyber security problems introduced by the configuration and use of mobile networks, including network availability, mobile web browsers and caller authentication
4. **Multi-faceted Approach to Cyber Security Research** - research must take into account social behavioural norms and societal desires in cyber space, cyber space policies, the impact of cyber and other legislation and the economics of cyber space and cyber security.

In bringing together experts in the cyber space, it is the ambition of the Summit that its output will influence the development of cyber security and particularly that the proposed research strategy may give direction to future cyber security research. Future World Cyber Security Technology Research Summits will be held on an annual basis and will be able to assess recent changes in cyber security and put forward revisions in proposed cyber security research strategies to address these.

Introduction

In this, the inaugural, World Cyber Security Technology Research Summit, we have brought together experts in the field of cyber security from leading research institutes, government bodies and industry throughout the world. **Our aim is to share views on current issues in cyber security, explore future security requirements and agree a methodology for cyber security investigation to address these.**

The protection of cyber space grows in importance on an almost daily basis. Attacks in cyber space, ranging from hits on individuals to strikes on national infrastructures, are increasing in frequency and sophistication. The exploitation of cyber space vulnerabilities has become a global business with a revenue that presently outweighs that of cyber security efforts. **In this environment, it is critical that cyber security research is coordinated to address not only current but also envisaged security threats, and that such research is influenced by government policy and industry capability.**

In this research summit, hosted by the Centre for Secure Information Technology (CSIT) at Queen's University Belfast, we consider cyber space, particularly the Internet, of 5-10 years time, envision potential security threats and mitigation tactics, and put forward a strategy for future cyber security research.

1.1 Opening Addresses

The Summit was opened by Professor Peter Gregson, Vice Chancellor of The Queen's University of Belfast, who welcomed the delegates to CSIT at Queen's, noting the good cross section of delegates both internationally and by sector. He commented on the main focus of the Summit, to develop a 'DAVOS-style' activity around cyber security, enabling sharing of information on current and future cyber security matters, and the leadership role of CSIT in bringing cyber security experts together to meet this challenge. He expressed the hope that this would be one of many such Summits, becoming part of an international strategy for cyber security.



Prof Peter Gregson

Danny Kennedy, Minister for Employment and Learning, then addressed the Summit, welcoming the delegates to Belfast. He spoke of the increasing role in our lives played by cyber security and how crucial it is that we have systems and strategies in place to secure data etc. He stated that "it is a great honour for the University and, of course, the city of Belfast, to host the inaugural World Cyber Security Technology Research Summit, and thus play a part in helping to develop an international strategy on cyber security."



Danny Kennedy, MLA

Morning Session Review

In this session government officials, security analysts and industry leaders delivered presentations giving an international perspective on emerging cyber security issues and the vision of tomorrow.

2.1 Presentations

2.1.1 Chris Ensor, Technical Director, CESG : What are the emerging threats to UK cyber space?

Chris joined GCHQ in 1989 after completing his degree in Microelectronics and Computing at University College of Wales Aberystwyth. He began his career in the department working on high assurance 'compusec' developments before turning his attention to more practical solutions to governments business needs, and in particular it's secure use of the Internet. In order to encourage interoperable secure e-mail solutions he delivered a number of proof of concept systems which were deployed within UK Government and NATO, the latter being an entertaining trilateral effort with France and Germany. He is one of 4 IA Technical Directors at CESG and is responsible for developing and maintaining the organisation's role as the National Technical Authority. He was a founder member of the Institute of Information Security Professionals, and is currently Head of Profession for Information Assurance at GCHQ. He is currently working to extend IA best practice across Government.

The main message expressed in this presentation was that, when considering cyber security, particularly for information systems, we need to consider all possible sources of threats, e.g. users and hackers, and all possible threat spaces, e.g. cyber and physical spaces. It was explained that within government establishments a spectrum of threats must be considered: cleaners, couriers etc. who exploit opportunistic situations, e.g. computers left on, passwords on post-it notes; home enthusiasts who use publically-available hacking tools and bugs; skilled

hackers who develop new hacking tools and find new software bugs; organised crime e.g. massive scale, blackmail, bribery, etc.; foreign powers who have resources to introduce vulnerabilities that they can exploit later. **It was also indicated that users can sometimes pose as much a risk as malicious threats.** The existence of different threat spaces was discussed and the danger of focusing on just cyber space was highlighted. For example mobile phones not only 'live' in cyber space, but also in physical space, RF space where signals can be intercepted, and 'society' space - all of these need to be protected, blocking one will mean attackers will move to another.

The UK National Security Risk Assessment were then discussed and the development of a National Security Strategy, published in April 2011. This highlights that cyber security embraces both the protection of UK interests in cyber space and also the pursuit of the wider UK security policy through exploitation of the many opportunities that cyber space offers.

Cyber defence recommendations were also presented, including the need to understand threats, consider all possible threat sources and spaces, reduce system vulnerability, maintain situation/network awareness to decrease attack impact and the possibility of pursuing threats in cyber space.

2.1.2 William Barker, Chief Cyber Security Advisor, NIST, Dept of Commerce : US perspective



William (Curt) Barker Associate Director and Chief Cybersecurity Advisor, NIST Information Technology Laboratory. Mr. Barker is directly responsible for planning, directing, and implementing the policies and programs of the NIST cybersecurity program. He also conceives and implements strategic plans and executive direction to ensure that the scientific and technical activities promote the mission and goals of Lab/Program and NIST. Mr. Barker is also Acting Chief of NIST's Information Access Division and is the Department of Commerce Lead for the National Strategy for Trusted Identities in Cyberspace. He was recently assigned to the Department of Commerce Office of Policy and Strategic Planning as head of the Cybersecurity and Privacy Coordination Office. He was also recently Chief of the Information Technology Laboratory's Computer Security Division. Prior to becoming Division Chief, Mr. Barker was Program Manager for NIST Personal Identity Verification activities. He managed development of the HSPD #12-mandated Federal Information Processing Standard 201 and several NIST recommendations and guidelines that implement the FIPS. Mr Barker previously managed development of several NIST guidelines required by FISMA and is participating in the development of a number of NIST cryptographic publications. He has worked in the information security field since 1966. Before joining NIST, Mr. Barker worked in National Security Agency information

assurance organizations, and subsequently held private sector positions of Vice President and Director of Independent Research and Development at two information assurance companies: PE Systems and Trusted Information Systems.

In this presentation, the US cyber security situation was discussed from organisational and threats perspectives. The large number of US cyber security efforts was noted, along with the efforts to bring these together into a coordinated response, in line with the US cyber security review which identified the need for a national security initiative and strategy. From a threat perspective, it was observed that threats are increasingly multilateral, multipurpose and sophisticated, and becoming ever more difficult to attribute to their source. **The role of the National Institute of Standards and Technology (NIST) in cyber security was discussed, highlighting NIST's plans to focus on innovation, increasing research and collaboration, and accelerating transition to practice, in accordance with recommendations of the US national security strategy.**

Views and recommendations were then presented on the Cyber Security Industry Alliance (CSIA) strategic priorities, i.e. inducing change in the current cyber security situation, developing scientific foundations of cyber security, maximising cyber security research impact and accelerating transition of research to practice. With regard to inducing change, the opinion was expressed that in the near time we should apply what we already know e.g. using applications that use 'least privilege', and in the long term we should look to measure the effectiveness of designed-in security and work on the automation of network configuration and status discovery and monitoring. In developing cyber security

scientific foundations, it was suggested that a comprehensive ontology of cybersecurity concerns should be developed and that the outputs of this should be used to evaluate research and application priorities in this space. To maximise the impact of cyber security research it was proposed that at present we should focus on national priorities, e.g. health, IT, smart grid, and in the longer term we should seek to understand future threats. To accelerate transition of research to practice we should focus on the development of international cyber security standards as an impetus to getting research into the marketplace, along with workable mechanisms to handle conformance to the standards.

2.1.3 Eul Gyu Im, Korea Hanyang University : Korea's perspective on emerging threats



Eul Gyu Im received the BS and the MS degrees in computer engineering from Seoul National University, Korea in 1992 and 1994, and the PhD degree in computer science from the University of Southern California in 2002. He is currently an assistant professor at the division of Computer Science and Engineering in Hanyang University. Previously, he served as a senior researcher at the National Security Research Institute. His research interests include network security, malicious software analysis and SCADA security.

The presentation commenced with a brief summary of recent cyber attacks on Korean targets, including worm and distributed denial of service (DDoS) attacks on government establishments, military sites and national infrastructures. From these, it was concluded that cyber attacks on Korean system control and data acquisition (SCADA) systems, or smart grid systems, were of great concern due to the damage that these could cause. Security risks specific to smart grid systems were highlighted, including their use of bidirectional communication which can be used for attacks, use of commercial hardware and software in smart grid devices making them difficult to protect as system information and vulnerabilities are publically available, the increased number of access points of these systems and the increased connectivity among smart grid devices providing a variety of attack paths, and the geographical distribution of smart devices increasing the difficulty of monitoring and managing them.

Smart grid systems have a raised possibility of cyber attacks and such attacks can destroy critical infrastructure, the need for smart grid cyber security is therefore imperative.

The Korean smart grid cyber security research plan was then discussed. This has as its vision the establishment and operation of a smart grid system safe from cyber security threats. The objectives are to provide cyber safety by developing security technologies, such as monitoring, encryption, and authentication technologies, for smart grid systems. Strategies which will be deployed are security technologies development through analysis of related works and the establishment of a smart grid reference system with built-in cyber security. Such a system is under construction on Jeju Island, providing a smart grid test bed of 6000 households. Further research directions for secure

smart grid systems have been identified, including analysis of Korean and international security models for such systems, analysis of smart grid cyber standards, verification and commercialisation of smart grid security technologies by application to the Jeju Island smart grid test bed, leading to smart grid system architecture and security technologies which are compatible within Korea and with international standards.

2.1.4 John Bumgarner, CTO, US Cyber Consequences Unit : An international outlook



John is a retired US Army special operations veteran turned professional hacker with decades of experience in various disciplines of security. His private sector certifications include CISSP, GIAC (Gold), and dual Masters degrees in Information Systems Management and Security Management. The U.S. Cyber Consequences Unit (US-CCU) is an independent, non-profit (501c3) research institute. It provides assessments of the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks. It also investigates the likelihood of such attacks and examines the cost-effectiveness of possible counter-measures. The mission of the US-CCU is to provide America and its allies with the concepts and information necessary for making sound security decisions in a world where our

physical well-being increasingly depends on cyber-security

This presentation provided a forecast of future technological developments and emerging cyber security threats.

One of the threats area discussed centred around 'smart' systems, including smart utility grids and smart cars. It was posited that this technology was in its infancy and cyber security threats and privacy issues in this area will continue to grow over the next couple of decades. For smart utility grids, we not only need to look at threats to the primary utilities industries i.e. electricity, gas and water, but we also need to consider possible attacks on green energy sources, e.g. wind, wave etc. A major cyber attack against these utilities could cause significant consequences. To prevent these disruptions we need to be able to detect and respond to a cyber incident before significant damage is caused to the grid infrastructure. Utilities will deploy massive networks of smart meters and any cyber incident that disrupts these devices will also cause significant problems. Current smart meters have little security, but future ones will need to have a more robust cyber security design (e.g. embedded firewalls) to mitigate the impact of cyber attacks. It was also indicated that, to be truly efficient, smart grids will need to network with home appliances - this not only increases the possible attack vectors, but will also give rise to utilities collecting personal usage information (PU) about peoples' lives, which will raise privacy alarms with both customers and legislative bodies.

The looming threat to smart-enabled and environmental-friendly cars was also discussed. It was suggested that a fleet of intelligent cars could be infected with malware and that a smart car could be attacked when it syncs to an owner's home network, and that electric cars

could be hacked whilst connected to a charging system.

Other threat areas discussed included ID systems where it was noted that federation between countries to use the same ID from country to country will be desirable and this could present cyber security and privacy threats. The use of biometrics is not straightforward, as these do not have 100% accurate or usability and can be stolen.

The increasing threat area of DDoS attacks was highlighted, noting that there are various types and levels of these attacks. It was stated that these attacks will evolve into ones that utilise self-learning capabilities. For example, automated tools will gather information from the Internet about a potential target, then customise an attack based on that information and continually monitor the target to determine if additional modifications are needed. This examination of how cyber attack tools will change will also force cyber defences to follow suit. For example, there will be a need for 'polymorphic defences' to be developed. These defensive applications will need to think for themselves, by learning from attacks and making their own decisions to change a network security to properly defend against the attack.

Health-related devices were discussed as a future threat area that needs to be addressed. For example, Bluetooth enabled teeth, presently used primarily for hearing problems, but which could also be used to communicate with mobile phones, could be hacked and turned into listening devices or internal speakers resonating random sounds. Several more critical devices (e.g. pacemakers and insulin pumps) were mentioned which have security risks that could expose patients to life-threatening cyber attacks.

In conclusion it was acknowledged that there is a variety of existing and emerging areas, which present significant cyber security risks, and it was proposed that there is a need to think about these risks before launching new technologies into the marketplace.

2.2 Panel Discussion Summary

Morning speakers were joined on the panel by: Tony Bull - Thales, Mark Crosbie - IBM, Duncan Curry - Qosmos and Sandy Bird - Q1Labs.

What is the vision of tomorrow?

The views of the panellists were that authentication is critical, classification and monitoring of data and collaboration of industry and academia will be needed for security technologies that implement government cyber security policies, the big challenges are smart cities cyber security, business analytics and how to make better predictions e.g. about usage of utilities, cyber security standards, smart grids and bringing together players in the cyber space.

Questions put to the panel included:

How as vendors and research organisations can we balance the need for standards with business processes in smart grids?

The answers generally indicated that there is a need for standardisation but also diversity to reduce effects of attacks.

How can we influence the smarter society to build-in security and how do standards sit with society?

The resulting discussion ranged over opinions that society is able to accept some risk if there is the opportunity of redress, societal training is required to be able to deal with attacks, there is a need to provide help for mitigating attacks, and pushing responsibility onto the end-user won't work, there is a need to encourage development of a culture of producing software that has less opportunities for attack.

Can we look backwards to learn from our mistakes, to introduce regulation into cybersecurity space?

It was noted that IT systems don't give the same feedback as other systems e.g. cars, humans and that unlike the aircraft industry, there is a lack of feedback into network system architecture and design from security problems to make these better able to address attacks.

Is cyber security a risk/problem or an opportunity?

The general opinion expressed was that cyber security is both, that software will have security holes giving rise to risks and opportunities, a system that allows consumers to make an assessment of the risk should be put in place, the decision to build-in security or not carries risks and economic opportunities.

What is the appropriate role of regulation in cyber security, e.g. the US are thinking of extending regulation from telecoms into the Internet?

Answers indicated that regulation is important, but is only one tool to get security in cyber space, and that in the US there is an argument that the government should pay incentives to improve cyber security rather than instigate regulation and that the government needs to set the baseline and encourage players to meet this and more.

Afternoon Session Review

In this session leaders from academic and research institutes delivered presentations addressing what research there is for tomorrow's threats and are there any gaps which need to be bridged.

3.1 Presentations

3.1.1 Ulf Lindqvist, Program Director, SRI International : Future research agenda



Dr. Ulf Lindqvist is a Program Director in the Computer Science Laboratory of SRI International, an independent, nonprofit research institute. He manages R&D projects in infrastructure security and leads SRI's support for the U.S. Department of Homeland Security Cyber Security R&D Center. Dr. Lindqvist's expertise and interests are focused on the protection of critical infrastructure systems against electronic attacks, in particular analysis and detection of such attacks. He has more than twenty publications, many of which are bridging the gap between theoretical and applied research. He holds a Ph.D. in computer engineering from Chalmers University of Technology in Sweden.

The topics addressed in this presentation were research agendas for cyber security supported by the US government, illustrated by discussion of the US federal cyber security research coordination program. A research agenda was defined as answering a number of questions: where we are today i.e. the current technology and research and important technology gaps and research problems; where do we want to be; what will it take to get us there, how can we divide the problem and time spaces and what resources are

needed; how will we know what we have accomplished i.e. how should we evaluate technologies and validate results and define metrics of success. Important problems were defined as those that require an innovative solution that will make a demonstrable difference in the world.

Discussion moved on to the US federal cyber security research coordination program. The efforts to bring together the various existing research agendas into a cohesive agenda and comprehensive national cyber security initiative were highlighted, and the need to define and develop enduring 'leap-ahead' technology, strategies and programs.

The three-pronged approach of the program was reviewed, namely game changing research and development themes (moving target cyber defence, tailored trustworthy cyber spaces and cyber economic incentives), cyber security science (investigation of the fundamental laws of cyber security, metrics for experimentation) and transition to practice of cyber security research (get results of federally funded research into broad use, matchmaking between partners, test and evaluation for industry, adoption and support).

Final comments included the observation that technical solutions to cyber threats already exist but these are often not applied properly, that training and education in cyber security is lacking, the need for usable security technology, and collaboration between industry, government, academia and users.

3.1.2 Virgil Gligor, Director, CyLab : The challenges of client side security



Virgil D. Gligor (CYLAB) received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. He taught at the University of Maryland between 1976 and 2007, and is currently a Professor of Electrical and Computer Engineering at Carnegie Mellon University and co-Director of CyLab. Over the past thirty-five years, his research interests ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. Gligor was an editorial board member of several IEEE and ACM journals and the Editor in Chief of the IEEE Transactions on Dependable and Secure Computing. He served as the chair of ACM's Special Interest Group on Security, Audit and Control, and received the 2006 National Information Systems Security Award jointly given by NIST and NSA in the US.

This presentation started with noting that client side cyber security is more difficult than server side, and by giving some axioms of security and particularly usable security. These included: there will always be security vulnerabilities and people to exploit them; there will always be rapid innovation in IT and the need to update systems; there will always be large, complex systems and the security of these will not be fully known; users only understand very simple systems, security technologies and policies; users

have maximum expectations for security, but accept whatever usable security the market provides for free; users expect systems to help them recover from an attack.

A cyber security technology was then discussed, comprising logical machine partitioning. In this, resources of a machine are partitioned into a secure, or 'green', partition, and an insecure, or 'red', partition, using a hypervisor to decide whether a function is red or green. It was noted that the main problem with such a system remains communication between the red and green partitions. Verification of inputs into the partitions is not always possible, and some degree of trust is necessary.

The conclusions given were that there is a need to rethink security architectures for clients to provide truly usable security with human-oriented security policies, tools and aids, clients expect trustworthy spaces which reflect their asset separation goals not that of system designers, and trustworthy communications e.g. a trusted path beyond login and verification of input/output data.

3.1.3 Patrick Traynor, Associate Professor, Georgia Tech : Solving the mobile security threat



Assistant Professor in the College of Computing at Georgia Tech. and earned his Ph.D and M.S. in Computer Science and Engineering from the Pennsylvania State University in 2008 and 2004, respectively, and his B.S. in Computer Science from the University of Richmond in 2002. He is currently a member of the Georgia Tech Information Security Center (GTISC) and co-director of the Converging Infrastructure Security Laboratory (CISEC). His research focuses primarily on security in cellular networks. In particular, exploring the problems that arise as this piece of critical infrastructure is beginning to converge with the larger Internet. However, he is also interested in the systems challenges of applied cryptography and security for the Internet, mobile devices and wireless systems. In general, he is curious in learning about how secure systems are designed, constructed and broken.

In the mobile space security is a big problem, chiefly as a result of rogue applications that are malicious, but other attack avenues are becoming increasingly important, for example network availability and mobile web usage. This issue will only increase due to convergence in mobile architectures and the number of mobile users, 5 billion compared with 1.5 billion on the Internet. Malicious behaviour will simply follow utility - as mobile phones become the dominant computing platform, the expectation must be that they will be regularly targeted.

Specific mobile security issues include: SMS functionality as this can be overloaded resulting in blocking of important SMS messages e.g. emergency messages; use of home location registers (HLR) in mobile networks to deliver calls to a phone as if enough information is sent to a HLR it can be taken down; mobile web browsers as these have limited security

guarantees; lost and stolen phones as current remote wipe technologies are very course and limited; caller authentication as this is not strong and caller ID spoofing is easy.

It was concluded that mobile networks are very different from the Internet, they have different vulnerabilities and bottlenecks and cannot be treated like traditional Internet Protocol networks, malicious behaviour is adapting to use emerging attack scenarios, and mobile security problems are not exclusively malicious but can be due to the mobile network configuration and use pattern.

3.1.4 Erfan Ibrahim, Technical Executive, EPRI : How to secure critical power infrastructure



Erfan Ibrahim is a Technical Executive in the IntelliGrid program area of the Power Delivery & Utilization Sector. He leads the research that focuses on the communications, systems management and cyber security infrastructure for the utility Smart Grid with particular emphasis on Home Area Networks (HAN), Advanced Metering Infrastructure (AMI) and Internet based Wide Area Networking. Before joining EPRI, Dr. Ibrahim founded and managed The Bit Bazaar LLC (TBB), a full service IT and business consulting firm, offering services to clients in the High Tech, Financial Services, and Energy sectors. At TBB Dr.

Ibrahim focused on wireless communications, network management, and information security technologies with a particular emphasis on aligning the IT goals of his clients with their business goals for sustained competitive advantage. Prior to establishing The Bit Bazaar LLC, Dr. Ibrahim's career included the following positions: VP of Sales & Marketing at Jyra Research, Product Manager for Network Management at Pacific Bell Network Integration (now AT&T), Science and Math Lecturer at National University, Nuclear Fusion Research Engineer at UCLA and Plasma Physicist at Lawrence Livermore National Lab. Dr. Ibrahim received a Ph. D. in Nuclear Engineering from University of California Berkeley, an MS in Mechanical Engineering from the University of Texas Austin, and a B.S. Honors in Physics from Syracuse University (Suma Cum Laude). Dr. Ibrahim is a Phi Beta Kappa, a Tau Beta Pi, Who's Who Amongst American Colleges & Universities and Who's Who Amongst IT professionals.

The role of EPRI in the IntelliGrid research program was presented. The foundation of this program is the development of an electricity smart grid, and involves smart grid requirements gathering methodology, standards assessment, an information model to facilitate systems integration, a communication technology assessment and a security policy for smart grid applications. The challenge of moving information throughout smart grids was highlighted. There is a need to be able to communicate with meters and users in electricity smart grids, for the proper provision of the electricity particularly in high demand periods. As we move from a small number of electricity suppliers in a network to a larger number of suppliers (e.g. wind etc), the issue of communication will increase. It was put forward that there is a requirement for regulation and standards

to control communications and usage in smart grid architectures, in order to ensure reliable utility supply. It will also be necessary to look at security and privacy issues with integration of smart grids with home area networks (HAN).

The work of EPRI in several smart grid demonstrations was discussed, particularly EPRI's involvement in the National Electric Sector Cyber Security Organisation smart grid program. This has as its strategic focus a 'go to' place for the utility industry to share security vulnerabilities, solutions, and issues with standards. The program objectives are to develop risk mitigation strategies, best practices and metrics, test security technologies, harmonise security requirements, and assess existing power system and cyber security standards.

3.1.5 Sakir Sezer, Research Director, CSIT : Policy and technology for tomorrow's Internet



Sakir Sezer is Director and Head of Network and Cyber Security Research at the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast. He received his Dipl. Ing. in Electrical and Electronic Engineering in 1994 from RWTH Aachen University in Germany, and his PhD in 1999 from Queen's University Belfast in UK. His research is leading major (patented)

advances in the field of high-performance network and content processing and is currently commercialised by Titan IC Systems. He is also co-founder and CTO of Titan IC Systems and a member of various research and executive committees.

The presentation commenced with an indication of the cyber security challenge and how Internet technology had evolved organically over two decades, being developed by many sources including corporations with clear commercial interests. The lack of security in the Internet could be seen as a by-product of a profit-driven Internet industry, the capitalistic nature of the Internet dominating its socialistic/democratic nature compromising user security and privacy. Regulation of the Internet has been suggested mainly by policy makers, for example to control content on the web, and this has given rise to public concerns that regulation will restrict freedom of speech and privacy. The democratising properties of the Internet were discussed, where new media has allowed the sharing of views amongst large communities and the emergence of new voices giving rise to the question is a free and unregulated Internet an integral part of a free democratic society?

In devising options for providing increased security on the Internet, can we learn from a democratic society - in such a society, rules are the foundations that protect individuals' right of freedom, risks to security are assessed aiming for a balance between the preservation of democratic rights and an acceptable level of risk, society adapts to evolutionary changes to its culture and society. Taking a democratic society as an example a holistic approach is expected to provide an effective and sustainable cyber security solution. Such a solution should address the

evolutionary process of cyber space and cyber threats, the wider context incorporating social, political, cultural and financial attributes, and be balanced between the use of technology and regulation. Academia is well placed to address holistic and interdisciplinary research aspects of cyber security, looking ahead beyond current issues and challenges, and exploring unorthodox speculative methods and approaches. As an independent and impartial entity, academia has a major role to play in finding the fine balance between the use of technology and regulation and the posed security threats, questioning established technologies and applications that may, themselves, pose a threat, and recommending cyber security technologies, policies and regulations.

In summary, it was noted that cyber security is a complex problem that cannot be resolved with technology alone, the democratising properties of the Internet are very important and have been the source of innovation and the Internet revolution and cannot be sacrificed at any cost. We must widen our view and understanding of the cyber threat and derive interdisciplinary research that takes into account the social, political, legal and financial aspects of the problem, seeking answers by looking at how similar problems are resolved by various cultures and democratic societies.

3.2 Panel Discussion Summary

What is the research for tomorrow and does this match envisioned need?

Questions put to the panel included:

What is going to change the game in cyber security over the next 10 years?

Opinions on game-changing topics might include basic security education of users and improved security technology from companies, societal changes in source countries of cyber attacks, and that it is a matter of economics, if security causes an increased economic issue, this will lead to solutions.

Has peer pressure a role in getting people to take better security measures?

Answers included that there is some room for social pressure / punishment of people who take security measures e.g. patching and that there could be more impact of name and shame actions on companies than on users.

Collective Research Strategy

The aims of the Summit were threefold: to garner the delegates' observations on current cyber security threats, to envision future cyber security threats and requisite mitigation techniques, and to develop a collective strategy for next generation cyber security research. An overall theme emerged of the multi-faceted nature of cyber security and the consequent requirement for an inter-disciplinary approach. This needs to be combined with greater awareness of cyber security threats, usable cyber security and more innovative and effective ways of providing cyber security education.

In the concluding open session, a discussion of the collective research strategy became a brainstorming of the issues that would need to be addressed to provide an effective and sustainable cyber security solution. Of these, four emerged as research themes critical to the ongoing creation of cyber security defences.

1. Adaptive Cyber Security Technologies

Adaptive cyber security technologies are necessary to address the 'moving target' nature of cyber threats. Such technologies need to be flexible, agile and responsive, enabling them to cope with the network bandwidth of 5-10 years time and be more successful against zero-day attacks. Research objectives in

this area would include the development of cyber security technologies which have self-learning capabilities; self-awareness in cyber systems enabling early attack detection and self-configuration to defend against an attack; the establishment of feedback in cyber systems providing the capability of learning from cyber attacks.

2. Protection of Smart Utility Grids

Smart utility grids have, for a variety of reasons such as their size and accessibility, a raised susceptibility to cyber attacks. Such attacks can destroy national critical infrastructure and the need for smart grid cyber security is therefore imperative. Suggested research aims in this field could comprise: smart grid requirements gathering methodology; protection technologies for components of smart grids such as smart meters; secure technologies for communications in smart grids; integration of smart grids with home area networks (HAN) that provides for the privacy and security of collected information; development of smart grid standards.

3. Security of the Mobile Platform and Applications

In mobile technology, security is a rapidly increasing issue, due to convergence in mobile architectures, mobile phones becoming the dominant web platform and the expanding number of mobile users - 50 billion mobile devices in use by 2020. Research in this space should target not only malicious applications, but also mobile cyber security problems introduced by the configuration and use of mobile networks. Such problems include network availability as this can be compromised, mobile web browsers as these have limited security guarantees, lost and stolen phones as current remote wipe technologies are limited and caller authentication as this is not strong.

4. Multi-faceted Approach to Cyber Security Research

It is realised that technology alone will not suffice in the defence against cyber attacks - other facets of the cyber security issue must be considered. Next generation cyber security research must take into account social, political, legal and economic aspects of this space.

Social behavioural norms in cyber space need to be investigated, societal desires such as trust, safety, freedom and privacy must be examined, and attitudes to cyber security in source countries of cyber attacks should be studied. Cyber space policies, generated and set down by governments, need to be incorporated into cyber security research. Such research should also be used to influence the development of these policies and cyber space use regulations. The impact of cyber and other legislation should be taken into account in researching cyber security and again cyber security research needs to influence the development of such legislation. The economics of cyber security is important, development of effective security may only take place if it is economical to do so, this facet of cyber space needs to be studied and solutions suggested.

The World Cyber Security Technology Research Summit, Belfast 2011 has brought together a range of talent and knowledge in the cyber security field. From this we have been able to put forward a strategy for next generation cyber security research. The ambition of the Summit is that this strategy will help to inform global cyber security research and act as a general driver for cyber security roadmap definition over the coming year. It is our intention to hold future such Summits, where changes in cyber security will be discussed and the proposed collective research strategies will be reviewed and developed.

Trust Values Accountability Education
Awareness Law Deterrents Punishment
Standards Diversity Insider-Threat Smart
Utilities Socio-Economic Economics
Econometrics Interdisciplinary Holistic
Polymorphic Human-Firewall Best-of-
Breed-Alliance Partitioning Game-
changing-R&D Mobile-Malware Democratic
-Society-Model Regulation Enforced-Policy
Freedom-and-Protection Future-Roadmap