CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

Queen's University Belfast

BELFAST 2016

6th World Cyber Security Technology Research Summit

#BELFAST2016

REPORT

www.csit.qub.ac.uk

About CSIT

The Centre for Secure Information Technologies (CSIT) is the UK's National Innovation and Knowledge Centre (IKC) for cyber security, based at Queen's University Belfast. CSIT was awarded a Queen's Anniversary Prize for Higher and Further Education in 2015.

With a multidisciplinary team of over 80 people (academics, researchers, engineers and business staff) CSIT is industry focused, accelerating the commercial exploitation of cyber security innovation. CSIT has acted as the nucleating point for the emerging Belfast cyber cluster that has seen almost 1000 new jobs created in recent years. CSIT has spun out 6 new companies (Titan IC Systems, Activ Wireless, Sensurity, Liopa, Sirona Technologies and Cognition Video), is actively involved in coordinating a number of European Research programs (Horizon 2020) and has extensive links internationally.

Established in 2009, with initial core funding from EPSRC, Innovate UK, Invest NI and Queen's University Belfast, CSIT has a proven track record of success and in 2015 further 'phase 2' core funding of £5M from EPSRC/Innovate UK and £9M from Queen's was announced. This will enable CSIT to leverage a further £38M over the next 5 years.

About Belfast 2016

Running on 15-16th March, Belfast 2016 was CSIT's 6th World Cyber Security Technology Research Summit. Part of the Summit's uniqueness is its bringing together of the international research community alongside industry leaders, government policy makers, start-ups and SMEs from around the world. For researchers and technologists the event focused on how new ideas and innovations can be scaled successfully to have a positive global impact on cyber security. The speaker line-up was extensive and represented research, suppliers, investors, customers, integrators, large and small companies, not for profit and government.

Attendees pictured outside the Ulster Museum, location for the Summit Gala Dinner

Executive Summary

Scale was the theme for CSIT's 6th World Cyber Security Technology Research Summit. This has a number of dimensions. When CSIT received funding for its successful Phase 2 proposal in 2015 funders Innovate UK, the Engineering and Physical Sciences Research Council and InvestNI strongly encouraged the Centre not just to build on its successes in the previous 5 years but to continually enhance its ambitions in terms of the scale and level of activity and impact, not only in its research and research leadership but also in strongly raising the bar in promoting innovation and growth in the area of cyber security across the UK.

This is manifesting itself in quite a number of ways not least the appointment of new staff covering academic, engineering and commercial activities to (a) further enhance research activities (b) further enhance the translation of the results of this research into new products and services and (c) most importantly to promote widespread economic growth in the very important area of cyber security.

The Summit once again attracted a high calibre of senior speakers from a diverse range of organisations including Department of Justice Northern Ireland, GCHQ, RSA, D-Wave Systems, Intel Security, Amadeus Capital Partners, Security Innovation, Netronome, SRI International, Digital Shadows, NCC Group, A10 Networks, Akamai, Infosys, Roke Manor, Equiniti, The Shadowserver Foundation, Surevine, WhiteHat Security, Pentech Ventures, PwC and Analytics Engines.

The Summit began with GCHQ's Chris Ensor outlining the scale of the cyber security problem faced by the UK and globally. This has resulted in the Government increasing investment to £1.9 billion over the next five years including the establishment of the new National Cyber Security Centre (NCSC), a more public facing one stop shop for supporting UK businesses and critical national infrastructure in the fight against cyber attacks.

RSA's Michael Brown highlighted the need to operationalise the new cybersecurity paradigm in three ways: fix the disconnect between cyber-policies and operational execution, adopt a deep and pervasive level of true visibility everywhere within the enterprise at scale, and finally scaling resources to meet the ever expanding attack surface introduced by cloud, IoT, IP enabled drones, connected and autonomous vehicles and industrial control systems.

The benefits and threats presented by quantum computing were addressed by Dr. Colin Williams from D-Wave Systems and Dr William Whyte from Security Innovation. Dr Williams explained that while the classic story of quantum computing being a threat to existing public domain infrastructure security is to a certain degree true the worldwide effort now of developing post-quantum cryptosystems should introduce a certain degree of immunity. That being the case they can turn to considering quantum computers as having some benefit to cyber security. Dr Whyte highlighted the need for a secure updating system agile enough for crypto algorithms with a minimal reliance on hardware for application messages, and hardware support for post-quantum secure update.

From an end-user board level perspective Equiniti CEO Guy Wakely highlighted that many organisations still view cyber-attacks as 'Taboos'. He argued that companies need to collaborate more; need to be open about what's happening, need to share experiences, need to leverage the resources of academia and the broader computer science environment to make sure these cyber-attacks don't hit.

Finally Stuart Murdoch, CEO and Founder of Surevine highlighted the challenges of scaling a cyber security company in the UK where the culture and funding climate necessitates organic growth rather than the venture capital fuelled trajectory seen in Silicon Valley. The retention of skills in the UK is a significant challenge as is countering short-termism driven by high salaries available in the Valley.

OPENING ADDRESSES

David Ford MLA – Minister of Justice Northern Ireland

The Minister thanked CSIT for the invitation to speak at the Summit and said what a pleasure it was to see the good work being done here. He first became aware of the extent of cybercrime when briefed about the work of the Organised Crime Task Force – Cyber Crime sub-group his Department overseas, of which CSIT was a founding member. He highlighted the positive press coverage CSIT has been receiving, including the Queen's Anniversary Prize for Higher and Further Education awarded for its sustained efforts in cyber security.

Minister Ford emphasised that the impact of cybercrime a global. Businesses are concerned about and are experiencing significant internet attacks, with the Police Service of Northern Ireland (PSNI) and the National Crime Agency categorising cyberspace as a priority area. The PSNI are involved in prevention work, facilitating public reporting, and public campaigns such as the 'Get Safe Online' public information and advice website. The PSNI are reporting that the internet has been infiltrated by many types of crime, from online bullying, to criminal emails and texts, all of which are getting more sophisticated. It is his view that security systems must keep pace to deter and track down online criminals. He recognised that organisations such as CSIT and its partners gathered at the Summit work behind the scenes and he thanked and wished them well in their continuing and ongoing work to combat cyber security threats and online crime.

KEYNOTE SPEAKERS

Chris Ensor, Deputy Director National Technical Authority GCHQ

Over the last 5 years the UK Cybersecurity Strategy has dominated Chris' life. In November 2016 a second five-year National Security Strategy will be published along with a further five-year National Cybersecurity Programme. When the Chancellor spoke at GCHQ, one of his colleagues caused a storm on Twitter by quoting the Chancellor as saying "We are not winning". Why did the Chancellor say this? He said it because his comments are evidence based and cybersecurity issues are increasing. The trend is not going down, but the barriers to entry are. The cost of bespoke tools used in attacks is decreasing, while the methods used for attacks are not sophisticated.

The Government is investing £1.9 billion over the next five years. Building blocks include the "10 Steps to Cyber Security" guidance being issued by GCHQ and being taken by organisations as their Bible to protect themselves in cyber space. Chris noted that there is a long way to go in raising awareness. Cyber sense operates on 2 levels with self-assessment tests generally failing because companies have not got the basics right. CISP, Cyber First Programme, Cyber Apprentices, and university training has achieved a lot over the last 3 years. However, as the Chancellor says, the UK has to keep building and the role of GCHQ is key in this process.

The Chancellor outlined 5 major steps to being better able to defend ourselves online. These include internet service providers offering protection by diverting services from suspect IP sites. Notwithstanding, malware being shifted across the UK network requires near, mid and far protection. While the onus is on organisations with a new venture to raise awareness, there is also a need to do more in the mid-space.

There are too many organisations involved. The UK is creating a one-stop Government shop under GCHQ called the National Cyber Security Centre (NCSC); the public face of GCHQ. Work is ongoing to develop NCSC as a major step forward in response to UK security, and in order to reduce the number of brands, in time NCSC will replace CESG.

All of this will be built on people, skills and expertise with the creation of an institute of coding, training programmes, and the maintenance of CPDs to keep professional skills up to speed. School programmes are endeavouring to make the area of cybersecurity less male oriented and encourage female participation, while expanding the Cyber First Programme for national security. In establishing a cybersecurity eco-system, an investment of £165 million from the Cheltenham fund and Cyber Invest is being used to drive innovation in universities.

Industry has to be treated carefully ensuring that critical infrastructure regulation does not stifle innovation. In order to deter attacks, we need to show how we can affect attacks, represented by a far response to deter the threat actor and strong defences so that the UK is not viewed as an easy target.

Michael Brown, Rear Admiral, USN (Ret), VP and General Manager RSA Global Public Sector

Operationalising the New Cybersecurity Paradigm

The theme of Michael Brown's speech was operationalising the new cyber security paradigm. Setting the context involved going back to the US Cyber Strategy of 2007 and the subsequent Obama Review, to which he had dedicated four years of his life. Based on this he talked about what the UK should do – the 'good, bad and uglies'.

His colleague at RSA had spoken at last year's summit on the importance of analytics and visibility into network activity as well as the need to fundamentally rethink how we look at security; that message is as relevant today. RSA President, Amit Yoran, has repeatedly stated: "Our industry has failed in many respects to effectively prevent or even reduce the impact of breaches".

Our industry has failed to move from a singular focus. Breaches are inevitable and faster detection, and more accurate incident scoping, processing, and adjudication are the way forward. No matter how high the walls, adversaries will get through and we need to change our approach. In this regard, scale is the wrong approach. Hadrian's Wall was built to deter barbarians in Roman Britain and according to historians was economically impossible to maintain and fundamentally unsuccessful at keeping adversaries out. We are facing modern barbarians in cyber criminals, 'hacktivists', and other states are trying to do us harm through our digital networks. Taller walls will not solve our problems.

On the importance of scale, in the need to change our approach to cybersecurity, innovation from research and new companies is vital, and scale is foundational to the success of any new product or concept to address today's threats. Drawing on experience of scale in the Navy, the primary issue with scale is focused on the human element. The application of cyber capability in the Navy was first tried 12 or 13 years ago. It was found that personnel in the US Navy were not competent in this area, and a career path was developed to produce sailors competent in cyber security that continues today.

The second problem with scale was found in the Department of Homeland Security (DHS) in building architecture capable of defending the US Government cyberspace. The strategy and therefore decisions we made may have been successful a year earlier, but the constantly evolving threat and technology meant the strategy could not scale into the future and would be irrelevant unless adapted.

These vignettes help to explain how I have come to view the present environment and how scale is both a blessing and curse. From a positive view scale is important as we work on new ideas to allow protection of government and large enterprise that hold valuable sensitive and personal data; enable sifting through data to identify vulnerabilities; and facilitate open information to be shared and utilised between actors to protect both the public and commerce.

New initiatives must address three priorities:

Firstly, it must address customers' problems by operationalising cybersecurity to fix the disconnect that exists between cyber-policies and operational execution. In a recent RSA survey 90% of respondents identified the lack of ability to measure, assess and mitigate cybersecurity risk as the biggest weakness organisations face in both the public and private sector. This makes it impossible to prioritise and invest in security. Cyber-hygiene needs to be brought into organisations, their supply chains, business agreements, and all contractual areas.

Secondly, the need for visibility where companies must adopt a deep and pervasive level of true visibility everywhere at scale. That means from the Endpoint to the Cloud we need pervasive and true visibility into our enterprise environments. You simply can't do security today without the visibility of both continuous full packet capture and endpoint compromise assessment visibility. Technology alone doesn't solve the visibility problem. We also face a mind-set problem where some organizations do not even want to know what's going on in their networks, and others face inertia.

The need for visibility is vital in the face of today's advanced threats. Our adversaries are not only able to disrupt access to, or deface our websites; or edit, add or delete data that is critical to our mission. Organisations are beginning to realise that not only is their data being accessed inappropriately, but it is being tampered with and new risks are being identified. As data drives decision making for people and systems, when it is knowingly manipulated those decisions could lead to catastrophic consequences.

To restate, if we don't know what's going on within our networks, sooner than we think, the day could come that we will not be able to effectively rely on the integrity of our data. Consider the potentially devastating consequences of misrepresented data on the mixing of compounds, control systems and manufacturing processes. Widespread lack of visibility could quickly become an existential threat to our IP-dependent lifestyle.

Thirdly, our expanding attack surface and the risks to the Internet of Things (IoT) means that just 5 or 10 years ago, an organization's network consisted of organically owned and operated servers and computers that largely resided on company or government property. Today, that attack surface has expanded tremendously and includes data and applications within a cloud provider's environment, company and employee owned laptops and mobile devices from phones to tablets, watches, ID badges etc. Widespread deployment of IP-enabled drones and vehicles are on the horizon and we have to recognize that innovations in robotics and artificial intelligence far outpace our ability to secure those environments.

As cyber-attack tools and services become increasingly commoditized, the cost of attacking an organization is dropping dramatically, enabling more attacks that do not have financial gain as the primary focus. Sophisticated hacktivist collectives like Anonymous have been joined by relatively unsophisticated groups, or even individual cyber vigilantes. Organizations need to realise that financial gain is no longer the only, nor even perhaps the biggest, driver of their adversaries. Security operations and risk managers should evolve their understanding not only of the threat, but also of what, why, where and how they are being targeted.

IoT device use within industrial control systems is a key vulnerability. Intrusions into systems that control operations in the chemical, electrical, water and transport sectors have increased over the last three years. The advent of connected and automated sensors aggressively exacerbates these issues. The growth in the use of cyber technology by nation-state actors, terrorists, hacktivists and others, combined with the weakness of ICS security generally, makes the critical breach of an ICS in 2016 extremely concerning and increasingly likely. We have seen this already transpire in Turkey and in the Ukraine.

In conclusion, in the US, the White House has proposed a plan that looks to address some of these threats. It is intended for the public sector, but is just as applicable across private enterprise and the constituencies we serve. In short, President Obama’s proposal calls for:

- Widespread adoption of multi-factor authentication for email and other critical applications and systems. Multifactor authentication is a vital step to delivering increased security.
- Increased funding for cybersecurity within IT budgets.
- A broad plan to modernize IT defences and focus areas.
- Creation of an empowered Federal CISO
- Adoption and acceleration of the NIST Cybersecurity framework.
- Efforts to enhance the quantity and capability of the cyber workforce.

Boiled down, that plan addresses the three critical areas to our mission success as a security industry that I’ve discussed:

- How is risk operationalized in an organization? Our customers see the need to adopt a mature enterprise risk management approach to identifying and prioritizing efforts to mitigate risk.
- How is the organization obtaining and utilizing deep and pervasive visibility? Complete, real-time, visibility into threats across an organization’s infrastructure and their supply chain to the extent possible is needed.
- How is the modern attack surface being defended? Organizations must deploy new identity assurance and access governance technologies that are built natively for the cloud and mobile era.

Each one of us here today, as members and representatives of the IT security industry has a role in this mission. It is certainly the topic of the day here – and it is a battle we can’t afford to lose.

Dr. Colin Williams, Director of Bus Dev and Strategic Partnerships D-Wave Systems Inc.

Scaling up Quantum Computing and the Potential Benefits to Cybersecurity

Dr. Williams introduced the classic story that quantum computing is seen as a threat to our existing public domain infrastructure. He argued that this is not the case in any realistic sense due to the worldwide effort now of developing post-quantum cryptosystems. These are classical cryptosystems that would be invulnerable to quantum attack, and he is optimistic that we will sooner or later develop such cryptosystems.

If these post-quantum cryptosystems make us immune to the threat of quantum computers, then it is interesting from D Wave's point of view because they can turn to considering quantum computers as having some benefit to cybersecurity.

Dr. Williams talked about quantum computing at quite a high level and why it matters. He went on to explain D Wave's current product, the D Wave 2X000 quantum processor, and talked about some of the recent performance results that have been reported in the media. He then outlined an application that will lead in the direction of benefiting cybersecurity, and finished with comments on how the technology is scaling, and can scale faster than anticipated.

D Wave sells network integrated quantum computers that may look unusual. They come as a stand-alone modular unit which can be connected to a traditional HPC centre without any elaborate power or unusual requirements. The business model is to sell stand-alone quantum cube boxes and access to quantum computers in the cloud. Premier first customers include Google, Lockheed Martin and Los Alamos National Laboratory. D Wave has a dominant position in quantum computing with over 140 issued US patents, and are ranked 4th in patent power by IEEE. There is now an eco-system for companies developing software for D Wave's platform and Google has started their own quantum hardware effort utilising the quantum linking approach. A US intelligence agency has also announced an unclassified quantum development programme.

What is quantum computing? Quantum computers are machines that make use of physical resources based on quantum mechanical principles that are impossible to access on any classical computer. The three resources were outlined.

The first is superposition; the idea that if a bit in a classical computer can be a 0 or a 1, in a quantum computer they can be 0 and 1 simultaneously.

The second is strange. In a regular computer if the bits are thought of as a memory register, performing an operation on one sub-set of those bits would not be expected to have any effect on the state of the other bits in the register that were not touched. But in a quantum computer, if those bits are quantum bits, and they are tangled, then an operation performed on one sub-set of the qubits will have a side-effect on the state of the other set of the qubits although they were not acted on directly. This gives a completely new way of thinking about how to devise algorithms that can be much more efficient than classical.

The third effect is in a process called quantum co-tunnelling. The idea that to take the computer from one state to another state, classically an energy to flip all the bits has to be provided. In the quantum computer this transition can be made in a fundamentally different way. It is possible to go from one local state to another state by tunnelling through the potential barriers in between the general states, so representing different solutions. So the D Wave machine makes use of all these phenomena, and papers have been published in physics journals establishing this.

Conceptually how the D Wave machine works is in thinking of the problem being posed as defining the energy landscape in which the different points on the landscape correspond to different possible solutions, and the best solution corresponds to the lowest points in that landscape. Navigating this energy landscape finds the bit strings that correspond to the lowest lying point. Historically, every computer, whatever algorithm it was running, could only explore the surface of these energy landscapes jumping from point to point to point. The D Wave machine is the first to have this new physical resource, quantum co-tunnelling, that allows tunnelling through barriers in the energy landscapes to find local networks a lot more efficiently than was the case classically for certain kinds of problems. This matters because if the growth in solution times in relation to problem size is plotted, for certain problems the growth rate for the quantum computer can be considerably less than the growth rate for classical computing.

The D-Wave 2X comes in a large box with three racks. One controls communication to the outside world, the second is a refrigerator and the third contains cryogens to keep the chip cold. The chip is a new kind of technology based on super-conductive electronics. To turn on the super-conducting physics, it has to be cooled to 15 millikelvin, approximately 180 times colder than inter-stellar space. Also, it is necessary to null out the magnetic field across the chip to less than a nanotesla with the whole thing then enclosed in a cage.

The chip looks like a regular chip and is made of a metal called ‘niobium’ with a regular pattern based on a repeating unit cell structure. The qubits are made out of a loop of niobium interspersed in what is called a ‘Josephson Junction’, and if the current is flowing clockwise or counter-clockwise, that gives rise to a downward or upward pointing magnetic field giving a logical 1 or 0. Because in this device the currents can flow in both directions at the same time, it gives a ‘superposition’ state; that is a 1 and 0 at the same time. Under a microscope the circular looking qubits become elongated and each qubit has 4 vertical oriented and 4 horizontal oriented qubits, using a ‘coupler’ where they cross.

There are two modes of operation in using the chip. In the first mode the problem to be solved is mapped into an objective function of a quadratic formula that shows the program parameters. When the chip is programmed it starts in an equal superposition, then slowly turn on the field that created that equal superposition and go round the loop around 10,000 times a second. To do optimisation, retain the bit string that most minimises the objective function, and if doing sampling, retain all the bit strings obtained to make the surest programmable source to draw samples from across the distribution. The latter computation is the better use of a chip because it turns out to be the core computational bottle neck in deep learning. The chip is good at giving access to physical resources that can dramatically accelerate deep learning.

In terms of performance, the most recent result was last December when Google devised an algorithm to run on chip which was intended initially to test whether it performed as quantum or as a classical computer simulation. In the course of testing, Google noticed that the chip was not only doing quantum annealing, but that it was 100 million times faster than the classical processor during simulation.

Secondly, looking at the performance of the chip as a sampler. If the problem is not to find one optimal solution to a problem, but to find a lot of solutions, this is something the chip does extremely well. In terms of looking for an application of D Wave’s current technology, the best use case is in a sampling mode.

A third way of looking at performance is in terms of a power utilisation chip. Over the last 10 years or so, power dissipation in classical processing has plateaued, and correspondingly performance has flattened. But in the D-Wave chip, power consumption is about 15.5 kw for the whole system. Of that 15.5 kw, the power being expended on the actual computation is about a tenth of a microwatt, and as the chip is made bigger, it will remain a tenth of a microwatt because it does not dissipate energy as it operates. As a result, the performance is remarkably different from quantum to classic.

In applications, machine learning is where there could be a real win for cybersecurity. Two things the chip does majorly is discrete optimisation, such as finding the optimal solution to a problem, and discrete sampling such as finding multiple solutions to a problem. Consider the case of creating a binary classified service supposing a CIO of a company has to decide whether some traffic coming in should be classified as normal traffic or a threat. Using D-Wave provides a classifier that not only fits the current trading data set, but will generalise very robustly to new data. Google applied this to the problem of developing a classifier for detecting cars in an image. Using traditional machine learning techniques, they got a classifier that was working accurately 84% of the time. With D-Wave the reliability rose to 94% accuracy.

This is the tip of the iceberg of how this technology is going to impact machine learning. Another important takeaway from this example is that if a quantum machine is used to find a classifier, that classifier can then be deployed on a conventional computer platform. So the progress in computer technology is quite remarkable. Over the last 10 years or so we have been doubling the number of qubits every year that gives an exponential rate of growth in a processor that is faster than Moore's Law and having been made from all the traditional ways of chip processing, the processor is scalable.

Raj Samani, VP CTO EMEA
Intel Security

Disrupting Adversaries - Death of the Beebone Botnet

Raj Samani highlighted that disruption of the Beebone Botnet received 2,000 pieces of press coverage then asked the question - Was the operation a success? He argued that the reality is that in these operations headlines are great, but it is only solving half the problem because the threat is still out there.

Explaining why, he asked the audience to go back and look at the way malware operators have operated. He suggested that it is fair to say the level of innovation has been significant. Going back to 2009 if looking at the way malware operates, the way that it would operate is that IP addresses in criminal infrastructure would be hard coded into malware. So if wanting to know who to disrupt it would be easy as the IP address is already there. Equally, something like Zeus would communicate every 5.3 milliseconds and then it would have a gap of 60 seconds and then communicate again. So judging by network traffic alone it was easy to know which systems were infected.

Raj then asked the audience to fast forward to 2015 where industry saw technical innovation and a basic capability that had not been seen before. He highlighted that the perpetrators were doing everything they possibly could to avoid detection. The first thing they do now is execute code at system start-up. That may not be considered a big deal, but actually it began to do other things. If an application that would potentially disrupt or terminate and kill that process, and it was self-defending as well. Equally if you tried to go to a security vendor, it would actively block you from going there. It maintains a black-list of potential websites with the potential to delete the malware. It was also sandbox aware. But the important thing is that this malware did nothing itself. What it did was act as a facilitator for the download of other malware to steal passwords or download root kits. Basically perpetrators had an open door into any infected computer across the world.

The other thing the malware did was to update itself 35 times a day. People, if they have anti-virus installed, update it once or twice a day at most. What was interesting about this malware was that it would take the serial numbers of the C drives and user name of individual infected users and create a new variant. Therefore, updates differed from each other. How do you combat something that morphs so often and keeps re-inventing itself? What it meant was that by the time AV vendors identified the malware, tracked it and communicated it to law enforcement agencies, and were ready to take it down, there were over 5 million malware samples from this one form of malware. This from something that is only believed to have infected 23,000 systems globally.

That is important as there is a lot of work done with law enforcement. Partnerships with the National Crime Agency and European Crime Centre, and a lot of the times the question that will be asked will be where the victims are because that then allows the appropriate law enforcement agency to be engaged. It was found that most of the victims were in the US and that 90% of infections were hosted in the US. That becomes important as the story moves forward. By knowing that most of the infections are in the US, law enforcement can be engaged.

Next there is a requirement to determine where the criminal infrastructure is being hosted. Again, techniques have moved on. What the perpetrators have done now is create DGAs (Domain Generation Algorithms). These are algorithms that determine what the domain will be when it communicates. In this case Intel Security identified the DGA and observed they were communicating with six top-level domains. Within two weeks of breaking the DGA, the perpetrators changed it, so the company had to reverse-engineer that code and this time round they went to three top level domains, .com, .net, .org.

Finally, the company knew the criminal infrastructure they communicated with in the past, present, and also the future. The perpetrators then changed it again, but they made an error in their pseudo code meaning all traffic went through .coms. This meant that when law enforcement went in with a Court Order, the number of domains that had to be seized or suspended was dramatically reduced. For the first time with this particular malware Intel Security knew where the criminal infrastructure was located, and more importantly where it would communicate with in the future. That allowed the company to coordinate with law enforcement, in this case the Joint Cybercrime Action Taskforce which is part of Europol, and now the group physically knew where these systems were located. A sink hole was created that allowed traffic to be re-directed from the perpetrators to Intel Security's infrastructure. For the first time full visibility of where all the victims were based was possible. For the first time ever the number of infections around the world was known. The actual highest number of victims were in Iran with the second most impacted country being Peru.

Alex van Someren, General Partner
Amadeus Capital Partners & Co-Founder – CyLon

An overview of the UK cyber investment scene

There is an environment for investment in the UK with growth and solutions in industry attracting a new generation of talent such as in CSIT. As an investor, new innovations to solve current cyber-security can come from Government Agencies to garden sheds to turn ideas into businesses.

The challenge is that merely writing cheques doesn't solve the problem; people, products and businesses need to be supported. This is a good time for entrepreneurs, businesses and investors in cyber security. Media reports about cyber security appear daily, and it is estimated that $3.6 billion is spent globally on cyber security.

Key investors are all investing in 10 – 15 companies and the challenge is to compete with these well-financed businesses. In Israel the government has a cyber security strategy. Young people do military service and then develop businesses, amounting to approximately 40 companies a year. The strategy requires high investment, but leads to viable companies. The expectation that the businesses will be taken global to US makes this a good strategy.

In the UK we have to compete with Israel and US. The UK is capable of this as there is a big market demand. £75 million is spent buying products and this is expected to increase for cyber security. That is the prize. As investors identify 'hot' areas, e.g. threat intelligence, security analytics, what can be done with data, mobile security, these present different challenges. Cloud represents remote and shared storage space presenting problems to be solved.

The UK Government is supportive, economically and through a new strategy with £860 million invested already, £2 billion in cyber security solutions, £3.2 billion spent by government to procure demand for private enterprise to get their goods to the public.

This is work in progress with a pot of money to get access to new technology. GCHQ's Cyber Invest programme is bringing start-ups together and bringing them before potential customers. This is funded by the private sector, so we are seeing support from that sector.

There are limited cyber security investors in the UK, for example Notion Capital are starting to become known capitalists in the UK. They are still competing with US and Israel, and although scaling will come, as yet there are none dedicated to cyber security.

Challenges include a lack of ambition in scale, for example selling out too quickly before fully developing a product. Investors want a short turn around; often 10 years with pressure for a return for investors. There is a need for a 10 – 15 year investment and this may come from pension funds in future.

Exports and access to working with governments is also a challenge, particularly for SMEs. This is a good time to be working in cyber security, but there is a need to scale up globally when buyers want products.

Dr William Whyte, Chief Scientist
Security Innovation

The importance of post-quantum cryptography

Security Innovation has been researching security vulnerabilities for over 15 years. Their security testing methodology has been adopted by Adobe, Microsoft, Symantec, McAfee and others. They are also security partner for Dell, Microsoft and other well-known companies, and have authored 16 books, 4 co-authored with Microsoft. The company also has 9 patents. Their main professional focus is on vehicles communicating with each other and 'Vehicle to Anything' (V2X) involving getting 300 million devices to work securely.

Challenges arise in peer to peer applications. They come from a variety of suppliers with centralised security management that may be different across applications and will operate in different jurisdictions. There will be issues in securely setting them up, privacy and the management of data, and the secure maintenance of systems after they are deployed.

Growth in this area involves more devices, a main focus being on vehicle to anything. For example, where cars are enabled to stop automatically to avoid a collision, they will need to be constantly broadcasting to maximise the chance of warning the driver directly, or through other devices. Devices and vehicles will therefore be talking to each other. Field trials have demonstrated the feasibility of 'Vehicle to Anything' and the US Government is financing this in all cars by 2022. However, boxes other people have built and cheap cars may not have a security system built in. There is also the need to ensure that the technical devices will exist for the lifetime of the vehicle, and that regulation of devices is managed across jurisdictions. With multiple vehicles and devices this represents a huge scale.

The biggest constraint on scalability is people. Where people have to make decisions there is a bottle neck. Scaling can work with decisions such as writing code and issuing updates, but there is a problem with scalability if a decision is wrong involving accountability. Decisions will be made by boxes and humans, with data sent from car A to car B involving different manufacturers, the possibility of poor software, and reliance on good faith. All of this will require 300 million devices that are authenticated, certified, securely implemented with more than 1,000 certificates per year, and finally not requiring 300 billion human decisions.

Security Innovation's V2V security management system proposes enrolment as opposed to authorisation certificates, device certification, and revocation and misbehaviour investigation. An enrolment at the start of a device's lifetime to be used only for SCMS communications, and an authorisation certificate refreshed during the devices lifetime to be used for peer to peer communications cuts decisions to 17 million per year. The problem is to ensure the Enrolment CA makes the correct decisions.

For device certification, the device must be correctly implemented with the right requirements, proper testing, and an assurance that it will stay secure. With such a guarantee, it would only be necessary to have type certification. However, different quality software will require quality assurance and testing against requirements is expensive. Bug fixes may require recertification, requirements change as attacks evolve, and different labs in different jurisdiction have different standards.

The problem for scalability is not just standard suppliers and testers, but also enforcers. This is about governance rather than technology and scalability and has an important message for any large-scale, cross jurisdictional deployment. In order to remove bad actors, cars could report suspicious messages. The disadvantage with this would be that innocent users would be tracked. Enabling misbehaviour detection without widespread tracking would involve careful data management processes. For example, if a removal decision could be legally challenged this would introduce the human decision making element that we were trying to minimise.

In conclusion, building a secure, large-scale, peer-to-peer, international, lifelong, privacy preserving connected system must pay attention to the following. Firstly, the minimisation of human decisions with device certification and clear criteria for revocation. Secondly, proper data management that would preserve privacy for general users and those innocently caught up in reports of misbehaviour, while being able to target users suspected of violations. Thirdly, a secure updating system agile enough for crypto algorithms, minimum reliance on hardware for application messages, and hardware support for post-quantum secure update.

Jim Finnegan, COO

Netronome

Network Function Virtualisation and NIC based offload acceleration

Netronome develops mega scale data centres, has developed 160 patents, and is based in Silicon Valley. Modern applications have meant a rapid sprawl of virtual machines and deployment of a large number of containers is on the horizon. Development has been haphazard and disconnected and there is a need for distributed security systems which are evolving rapidly in software and server-based networking solutions such as the open virtual switch and virtual routers. New networking features need to be rolled out on a regular basis to keep data centre infrastructure scalable.

The need for distributed zero-trust security is paramount, and in the Netronome model security policies are deployed close to the application in virtual machines and containers. This is implemented using server-based networking where network virtualisation, security, load balancing and telemetry are implemented in the server.

This presents three main challenges. Firstly, server-based networking results in 3 times higher CAPEX and power consumption. Secondly, the rate of networking innovation slows significantly when performance and server efficiency comes into play, and thirdly, current solutions cannot provide the level of security needed for network speeds above 10 Gbps.

Server-based networking implemented using COTS servers has to use software that run on the CPU cores available using a 10 or 40GbE NIC for basic transmit and receive functions and related offloads. Server-based networking implemented in the CPU cores, can consume as many as 12 of them, leaving only four for applications in VMs or Containers. Therefore, the output per server becomes restricted, reducing efficiency and severely impacting performance with only 20% of expected throughput available. This means higher CAPEX as more servers are needed to deliver services.

A fundamental tenet of server-based networking is rapid software driven innovation. The fast adoption of cloud, SDN and NFV-related technologies has created a groundswell of networking innovations. OVS software has evolved rapidly in the last few years to include technologies such as VXLAN, service chaining, and more sophisticated security policies. Another area of innovation is integration with cloud orchestration tools such as OpenStack. Future versions of OVS, called Open vSwitch for Networking or OVN will include further enhancements in the areas of stateful security in the cloud that can be easily deployed using Open Stack. The Contrail virtual router software is also evolving rapidly in a similar way. As highlighted earlier, server-based networking when implemented in software only, reduces server efficiency and performance significantly. Incorporating new server-based networking features into hardware entails waiting for new silicon that can take 24 months or more. Overall, much needed networking innovation stalls as soon as server efficiency and performance comes into question.

With the rise in recent hacks and the need for surveillance, zero-trust has come to the forefront. There is an increasing number of tenants, applications, VMs and containers, with data center customers reporting a thousand security policies per VM becoming a baseline. In the example shown, 48 VMs require 48000 security rules per server, with current server-based networking solutions falling short on the needed scale, delivering less than 1/6th the required number of policies at less than 10Gbps of performance. With thousands of container deployments per server, the challenge of scaling such distributed security implementations using server-based networking will only get worse.

A few of the mega-scale data center industry have solved the challenges. Microsoft, Amazon and Google have successfully deployed server-based networking at scale, achieving efficiencies needed in mega-scale data centers. These companies have resorted to significant R&D investments not only in the area of networking software, but also utilizing proprietary silicon, hardware and software based acceleration of server-based networking functions.

The mega-scale data center operators have shown that the server-based networking challenges can be solved. The rest of the market needs server-based network with the desired scale and efficiencies. Large data center and telco cloud service providers need an off-the-shelf, efficient and scalable server-based networking solution. There is an even larger base of enterprise data centers that are called the next 10,000 clouds. The opportunity for off-the-shelf, efficient and scalable server-based networking solutions is huge.

Operator services revenue relates to the number of VMs that can be deployed per server with required levels of performance and security. Two critical data center applications case studies illustrate this.

In implementing zero trust security using data center micro segmentation technologies, Netronome's Agilio solution delivers 4 times more virtual machines per server, while securing VMs with 8 times more security policies. This proof-of-concept is implemented using OpenStack with Netronome's partner Mirantis.

Implementing cloud-based mobility using virtual evolved packet core (vEPC) , the Agilio solution delivers 3 times more virtual machines per server while improving performance per VM by 4 times. This has implications on the number of concurrent mobile user connections that can be supported per server at high service levels. This proof-of-concept was implemented with Netronome's partner Tieto, utilizing their networking stack and vEPC software. Virtual Evolved Packet Core (vEPC) is a framework for providing voice and data on a 4G LTE network.

In conclusion, the trend towards COT server based cloud computing will continue until offload and acceleration requirements for intelligent NICs is accepted. "Software defined everything" requires a multiple instruction, multiple data NUMA architecture to scale with networking I/O and the number of rules per VM continuing to increase. Many core (00's) architecture for an intelligent NIC must be implemented in finFET technology for power and performance. Ease of programming requires an open C or P4 based run-to-completion programming model.

Dr. Ulf Lindqvist, Program Director - Computer Science Laboratory SRI International

The challenges of securing IoT at scale

IoT consists of all kinds of devices connected to the internet and has no clear definition. This is happening on an unprecedented scale and it is impossible to predict how many new devices that could last a lifetime will be around a few years from now. While smartphones have a life span of around two years with constant interaction with humans and frequent security updates, in contrast, many devices have a lifetime of up to 20 years. These include medical devices, home appliances, cars, smart meters, and building sensors. They often have little or no human interaction and are seldom if ever updated. There is the risk of IoTs that have no connectivity and no one knowing what they do any more. This lack of updates leaves these devices vulnerable.

Managing technologies presents a challenge with a cultural and organisational gap. In the case of IoT there is no clear idea of who is responsible for a device over its lifetime, for example the vendor, whoever deployed it, cloud/communications provider, or user. For Industrial Control Systems (ICS), despite being managed by engineers who do not keep track of IT management, they have established relationships with vendors.

Security is about separation of the authorised from the unauthorised, but this is counteracted by people wanting to connect everything to everything else. What is done for IT will not work for IoT. Security for IT systems depends on frequent patching, secure configuration, and add on security products such as monitoring, filtering and secure accessibility. This will not work for the IoT that is large, distributed and autonomous.

There is an urgency to do something in the area of privacy relating to the public infrastructure and wearables and there is a disjoint in knowledge about privacy between developers and integrators. There are critical issues in relation to safety, for example in vehicles. We want improved safety and health, but counter to that the devices we are using are not secure and therefore not safe. There are issues, for example in relation to privacy regarding location and medical conditions.

These are the challenges and the solution is in focusing on assisting developers to make devices secure. SRI's vision for its strategic initiative is to provide IoT developers and integrators with effective tools and methods to build secure and maintainable systems. An IEEE cybersecurity initiative includes a document – "Avoiding the Top Ten Software Security Design Flaws" and a new conference on security for developers. There are also immediate R&D opportunities and initiatives. The US Department of Homeland Security is providing funding for start-up companies for securing the IoT, and SRI is seeking visiting researchers for its sites in California, Washington DC, and New York City.

James Chappell, CTO and Co-founder
Digital Shadows

Demystifying the dark web

Honour to be at Belfast 2016 having been through the scaling journey. What began in 2011 as an interest in digital footprints has grown to 70 people based in San Francisco and London.

What are digital shadows and what is the reality of the dark web and criminal internet?

Digital Shadows provides situational awareness for its clients. Its flagship solution is 'SearchLight' which is a scalable data analysis platform providing a view of an organisation's footprint and a profile of its attackers. SearchLight continually monitors more than 100 million data sources across the visible, deep, and dark web sifting what is relevant to clients. A portal then provides information on threats and security.

A digital footprint is generally a good thing. It is the information that is managed by organisations and intentionally left by organisations when interacting with the internet. However, some information that leaks out online can damage an organisation's security, and we started referring to this as 'digital shadows'. Digital footprints are what we mean to put on the internet, while digital shadows are unintentionally exposed. For example, if you put the word 'confidential' into a search engine, 210,000 results come up. So even information marked confidential has a digital shadow out there.

Most websites interact; Twitter, LinkedIn, but also telephone directories. The world going social can be positive, but there is more information available than ever. There is also a bigger and bigger digital shadow where there are lengthening supply chains and information is going further. Software is increasing and so is the risk to security. Cloud is like using other peoples' computers. Online storage and secure cloud services operated by Amazon, Google with terabytes of storage being cheap, but firms are storing customer data and URLs are getting shared.

Threats have digital footprints too. Attackers leave footprints and Digital Shadows can be used to report and address threats on an ongoing basis with the software we have developed. The dark web differs from the media definitions. Websites on Google, for example, are the 'surface web'. But like an iceberg, more sits beneath in the 'deep web'. Part of the deep web is called the 'dark web'. We have a developed dark web, secure overlay networks to access additional services online. This includes, for example, Tor. Tor was initially developed by the US Navy and funded by the US Government. It can protect identity, but hidden services maintain the anonymity of a user. It is now funded by the public and privacy groups etc. Headlines feature the selling of illegal drugs and firearms by criminals because the anonymity is popular with criminals, but these activities can also be carried out on VPNs. Although there is crime on Tor etc. it also exists on regular websites. The truth is that all crimes on Tor have their equivalent on the regular web.

ITP and Tor are not all bad. Privacy is a human right, but criminals use it too. Facebook is on Tor with an anonymous cat facts site. The cybercriminal economy includes tumbling, money laundering etc. Money is sitting at the top and its delivery to criminals happens through various means. There are examples in the clear web and the dark web and other market places. It is hard for criminals as they have to stay private, but in order to sell their products brand and reputation is also important. Building reputation based on user name and brand is counter to privacy, so they will ultimately fail. Only 5 – 600 fora of sites on Tor, but they are popular and you can get a lot of criminal services.

The dark web is a fraction of the size of the regular web. You have to look at the big picture and see what is on both webs, i.e. situational awareness. Be aware of what assets are out there and look at digital shadows in terms of scale and where attacks could come from.

Paul Vlissidis, Director of Domain Services and Technical Director NCC Group

A Recipe for How to Make the Internet Safer

Recipe for how to make the internet safer. This is a provocative title as user behaviour is hard to change, but propose focusing on one aspect – domain name ecosystem.

There is a change coming on the internet; a new internet. Now www and domains .com, .co, .uk etc will be transformed with domain changes and the IOT.

TLDs and brand names – no one who has bought them knows what to do with them. In total there is the potential of increasing the security debt for decades. For example, an internet of things that is there for 20 years and cannot be updated. There is an opportunity with new domain names to take more care and build in trust (.trust domain). The annual IDG survey carried out on behalf of the NCC Group found that of the 80% of users who regularly use the internet, only 20% feel comfortable doing so. For example, the use of voucher codes mean the user has to give up their privacy in order to get them. If this was a retail store and only 20% of customers felt comfortable using it they would make changes, but on the internet businesses do not tell customers about their security measures. We trust banks, but not online shopping due to assumptions we make about security and privacy.

Ways to rebuild a trust relationship:

Who are you dealing with? Looks like a bank or shop, but people are losing their life savings when emails are monitored. Criminals can buy domain names that have one letter in the domain name that is different from the bank or shop the user thinks they are dealing with. For example, a woman lost her savings when criminals monitored her emails and knew she was moving house. They bought a domain name where one letter was different from that of their solicitor. Because she trusted the solicitor she transferred money to the criminals in the belief the email with the bank details had come from her solicitor.

Apply security standards. Need for verification. Has been poor so far as no one checks who has bought a domain name and this fuels crime on the internet. There are 2,000 accredited registrations with ICANN, but do not have to register who bought them and they can be sold on. New domain companies verify the right of a buyer to a domain name, for example, .trust, .bank, or .ngo, so branded TLDs are clever where a brand name is closed and cannot be bought by others. Security in dealing with a company who is who it claims to be. Not good at knowing what is 'good' in security because of the responsibility of meeting that challenge. Better at saying what 'bad' looks like.

‘.Domain’ is building what ‘good’ looks like. If you had the chance to start the internet again, what would you want it to look like? ‘Who do you trust’ owned by ‘.Domain’ has over 200 specific technical guidelines as a benchmark to reach a security standard. Putting them in place is onerous, but achievable.

The last piece of the jigsaw is regular assurance. New TLDs required to monitor for abuse every 24 hours and then as registrant inform Register and do something, for example, take them down. This used to take 3 weeks and was too long as criminals were able to escape. Now some community DLTs are doing it in 24 hours.

Now when you put a domain online you can check for issues and this is done annually. This will make the internet safer. If something bad happens on a domain you can find the registrar who will have the contact details for the domain owner and can notify them that something is wrong in their domain network. If such a thing was available people said they would switch (50%) if they knew a domain was safer.

Lee Chen, Founder & CEO
A10 Networks

Uncover Cyber Threats and Scale SSL Traffic

SSL traffic is growing rapidly with 50% to 70% of internet traffic encrypted. Security solutions that need to decrypt SSL traffic include mail gateway, secure web gateway, next generation firewall, intrusion detection and DDOS prevention. SSL traffic has an impact on next generation firewalls with research showing an average 81% loss of performance across eight firewalls.

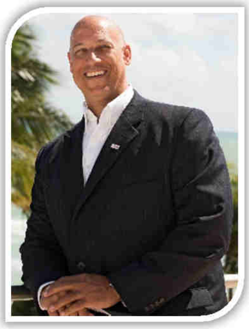
The performance of security devices is limited by SSL traffic, and most devices can do encryption and enable SSL decryption. Superior performance can be gained with SSL Insight Solution, taking decryption out of a device. Decrypting and encrypting for traffic to move on to the next device is not efficient. It is easier to manage single device. SSL Insight ‘Open Once’ insight offers reduced CapEx investing in only one device for SSL growth and no SSL decryption will boost performance in existing devices. Reduced OpEX means centralised SSL certificate management and centralised bypass policy management.

Privacy is a big concern. SSL Insight Solution requires a rich bypass policy, addressing privacy concerns, bypassing certain categories of websites. Opt out domains and users allows bypassing of certain users and static domains. SSL certification and certificate management is vital. Certificate validation requires validation of external certificates before they are presented to the user, also providing similar, or more levels of validation as a browser. In addition, revocation checks are carried out for incoming certificates.

For SSL Insight Solution high throughput and CPS is important as business internet traffic will grow at 20% CAGR until 2019. PFS ciphers are disproportionately heavy on CPU, and PFS is growing. It is now supported on 91% of top one million sites compare to 61% in 2014.

There are more choices available to deploy SSL. Basically just have traffic proxy vendors with more flexible deployment that can look at all data. It offers not only performance management that is only deployed once, places importance on security and offers a preferred centralised consolidated solution to do SSL decryptions. This requirement is growing rapidly and SSL as a processor is also growing rapidly. A consolidated single device offering a better security solution.

Harold Moss, VP Security Strategy
Akamai



A Millennial Strategy: How enterprises are changing for the better and how you can help?

At a conference in Boston, Invest NI asked the panel "What scares you most?" Harold's answer was millennials. Millennials are seen as a transformation in the workplace. Aged between 18-33 years of age millennials represent a changing workforce. In a survey of millennials in the workplace conducted by Forbes, 53% said they would rather give up their sense of smell than their technology, 60% will leave their company within three years, 68% demand an integrated, seamless experience regardless of channel, and 56% refuse to work for companies that ban social media.

In the past employees did what their company told them with security policies. This is no longer the case. Millennials expect accessibility for all their devices when working from home, and a faster experience. They are not interested in security policies, but expect the company they are working for to have them in place.

The notion of ergonomics has been around for some time with the idea that things are self-healing. This relies on trust, and fortunately the millennial generation trust everything. But if looked at organisations ten years ago, no one actually came up with an ergonomic solution because they were afraid of shutting down the network or service by accident, so you have to be careful how you implement those things.

The enterprise mesh is really about mobility. Mobile first strategy is a radical concept, but no one can ever tell you what it is. A mobile device is the new attack method. It is a computer connected all the time to the internet where most attacks come from. Mobile security is emerging and we are going to see a different model. The view of a bank recently was to secure their own application by suiting it to the posture of the device, assume it is secure, and not waste any more time on it. This is forward thinking and actually a creative approach. The internet of everything means information is accessed from a range of devices.

In the social digital world where a lot of people talk about privacy, young people don't really care about privacy or security any more, and have a different attitude to the sharing of information. To free up space, young employees move data to third party cloud providers without their company knowing. Young employees are no longer going to work under the constraints of controls such as verification and access.

Future challenges include the difficulty for organisations in hiring and retaining staff and this is driving how investment is made. There is a need to think differently. Technology is moving to the cloud where costs can be consolidated. Mobility will be core, and bolt-on security will not work. Employees expect it to be built-in, easy to use, and adaptable. Therefore, security needs to evolve and react faster, given the speed of the internet. The low cost of technology an attacker can acquire is making attackers more efficient.

Gordon Muehl, Vice President Industrie 4.0/Industrial Internet
Infosys

Open Source Security

Infosys 1 is a really successful product running 1 billion bank accounts through open source. There is no money in software any more. People use open source. Open SSL; the good news is we now pay developers to fix vulnerabilities in open source code. This is better. The bad news; no one is identifying how many issues are in there except Linux who say there are now only 250,000 defects. So there is someone there fixing vulnerabilities in only a few systems like Linux. Most are not, so many people do not depend on open source, but if you think you aren't going to depend on open source the only alternative is to go back to using paper. Why is it not working?

Most companies do the security requirements for the software they write, but not for what they use on open source, so therefore it is not being maintained. Most people do not understand the code as they did not write it so no one fixes or scans code for vulnerabilities, and fixing it is not very exciting anyway. So no one does it and in two years they may fix one thing, and really no one cares as it is maintenance work no one wants to do.

Who does it? The whole idea of people fixing open source is untrue and you only need to find one or two vulnerabilities to be able to break into it. So it is good for the bad guys, but not the good guys.

The conclusion is to adopt OSS package. Why not share what Microsoft has scanned and use this component. If one or two companies adopt the component, even with limited application, OSS is becoming more pervasive and consequently more vital.

There are real challenges. For example, a paper mill runs for 100 years and the software that takes 7 years to build costs $2mill. These machines run for years and only shut down for one or two days a year. Other systems also run for years, for example planes and cars are only fully maintained annually, whereas software is updated hourly. Where this happens there is not a fit. Lufthansa has started giving pilots an iPad for flight information instead of paper. However, iPads have OSS and security issues even if not connected, plus it now has to cope with IOT. The lifecycles do not fit. We need to address the principles of what we do and do it better, for example authentication and encryption etc. NSA, banks, stealing data and selling it on is not the issue. There are easier ways to damage a company. IT and OT, where there are physical parts in IT systems, for example in a refinery are 60% to 80% accurate. This is alright if there are physical things to see, but if this is no longer the case then there is a reliance on integrity, and this is now what is feared. If someone destroys data you cannot just go and find it, as it will not be known where the back-ups are or when it happened. When everything is virtual you cannot go into a warehouse to look.

Integrity and reliance are the solution. If transactions are built on chain systems, you could ask the clients what parts they know about. If you get the chain correct, other principles are extremely relevant i.e. language, protocols, integrity. Challenge redundancy. Open source community and how people interact with each other also applies to software and points will fail. Research and governments need to adopt a security highway that companies could invest in.

Pete Lockhart, CTO
Roke Manor Research Ltd

Autonomy and Security or the Road to Sucess (sic)

Roke are a technical research and development company specialising in active and defensive cyber solutions, data science, and electronics and software engineering. Clients include Government agencies and departments, defence primes, and industry partners. Roke have around 300 engineers and have recently started a cyber academy at Southampton University, a complimentary organisation to CSIT.

Roke has managed to cross the barrier between the commercial world and the world of defence. This has been managed successfully through commercial technology such as 3G and 4G and defence technology such as phased array radar.

In relation to what IoT is all about, why we need smart grids, and whether it is going to achieve the level of safety we require, we use the framework of machine situational awareness. There is a physical world and that has certain properties. We create transducers which we convert into signals. Signals are then converted by a process of detection estimation into data. We then go through a process of object recognition, for example is it a person, or a tank, or a car? Once we have identifiable objects we can start talking about information and thinking about relationships between objects, using conceptual mapping to create knowledge and cognition that can equal insight and decision making capabilities.

When we talk about autonomy we want to close the loop completely and have a system that has strategies and goals. When complicated algorithms are put into a visualisation system, data collected by a camera can be used for behavioural analysis. This involves spotting people, velocity, and identifying social groups moving in the same trajectory. Recording normal behaviour allows unexpected behaviour to be picked up from, for example gaze pattern. We then go from video detection to behavioural analysis.

In dealing with scale, Roke's STARTLE is an architecture for machine situational awareness. Machine situation awareness uses autonomous threat detection, assessment and sensor cueing. It emulates "conditioned fear response" based on how the amygdala in the human brain detects threats and cues a response. It uses features to drive a threat detector that triggers a rule. This state of the art technology has been demonstrated in autonomous navigation sea trials to create a risk model and Sensor Fusion; sensor in motion has been tested by the UK Bike team.

Machine detection is a world model problem to address market need. For example, car manufacturers are attempting to cater to an aging population addressing accessibility needs, while also providing vehicle connectivity demanded by the younger population. Connected autonomous vehicles enabling people to drive and to be connected while driving even includes media hype where Google are proposing self-driving cars without pedals or steering wheels. Currently the race is on between the US and the UK to produce the first autonomous vehicles.

Autonomous vehicles create dangerous spaces in safety and security. For example, in a dangerous situation a vehicle may hand back control to a driver who is not used to handling the vehicle. Self-driving cars could be a target for hackers with people trapped in their vehicle until a ransom is paid.

People talk about data created by vehicles, rather than the security of the data itself in the car. This represents a security issue. Can updates be applied to the in-car technology? Who will be responsible for these? Currently the end user has the responsibility for updates and security. In order to create an economic incentive for the security population to address this issue, users need to demand a security rating for vehicles. A security model for machine situational awareness would require limit checking and end point user verification. This would include sensing capability and an understanding of security and connectivity assurance and insurance.

Guy Wakeley, CEO
Equiniti

Building Scale and Resilience: a journey from private equity to plc

Macro environment changes – should we be worried?

The rate of change shows that GDP and life expectancy are growing. Medical care is more effective, and an aging population is an enormous issue. Improvements in medical care mean the system will be overburdened, with life expectancy following retirement having risen from 6 years to 26 years.

Computing power has also grown in last 20 years and kids are fluent in the language of technology. In 2050 it is possible there won't be any disability due to genome technology and more computer scientists than ever driving change. However, growth and development and events create challenges. For example, climate change, rising sea levels, hurricanes and flooding.

Systems are inter-connected. Banking systems and the speed of cash movement means that when things go wrong they do so very quickly. No one predicted the banking crash. Markets change and organisations can be eradicated through the actions of one person. Global epidemics and the speed of their movement, businesses and cybercrime, the amount of data that is held. With any resource there can be a disaster, as with data theft, hacking, and data manipulation.

There are concerns about the new world order and cyberattacks. Scientists and computer security experts have to fight threats, organisations are moving significant amounts of money, including government money, and the security of financial information and data is crucial. Having recently floated a small equity company on FTSE creates a realisation of increased threat from cyberattack due to increased public exposure.

Companies need to talk about cyberattacks; their depth and severity and the recovery of reputations. There is a need to leverage the resources of academia, and businesses need to talk more openly about cyberattacks and share intelligence even when it will involve market sensitive discourse.

Stewart Garrick, Special Projects Manager
The Shadowserver Foundation

Public/Private Partnerships and Botnets (what they don't teach you at Hendon)

With a background in law enforcement the last 4 years have been spent investigating cybercrime and managing support to law enforcement agencies globally. Shadow Server is a not for profit organisation that does not sell information, but gives it away free to victims. It gets donations, financial and in hardware. It has a global reach, scans the internet daily, carries out collection and analysis, sink holing and botnet takedowns. Through agreement it can take control of middle section and can see addresses of botnet users. Can register networks and get reports form scans. Therefore, with this unique information it can help with law enforcement.

Botnets and law enforcement:

The problem with crime is scale; hundreds of thousands of victims and banks etc. had to rethink investigation strategies. Operation Clean Slate looks at four things in investigation strategy. If only one area is looked at, criminals learn, change strategy, then come back and re-infect.

Crime is trans-jurisdictional and can take three months to investigate which is too long. Information sharing and trust models are difficult for law enforcement to learn to work with. Shadow Server Foundation is a not for profit organisation, so it is easier for law enforcement to trust and work with.

What did game Over Zeus teach us? It took 4 years to take down and was a successful botnet. A clean slate methodology involved combining a partnership of private companies feeding in information to bring it down. This provided a good result. Zeus was malware that moved money from accounts. At the top there was the malware coder who was employed. The aim was to get the malware onto the computers of victims, and it is traffic sellers who provide the victims. Volume is what counts for mass banking Trojans. A haul of people write exploit loaders and cryptographers run multiple copies of anti-viruses (AVs).

A botnet represents a cottage industry with cryptographers and counter AVs working together. In the wild malware has 5-10 days before it is detected by AVs, then the criminals change it and re-distribute it. All these factors have to be in place for the crime to take place with drop handlers having a key role as they have contacts in various countries.

A current growing threat is ransomware. This requires the criminals to provide a support service. Instructions on how to use the system, encryption key etc. have to be given to users who fall prey to an attack, otherwise victims will not be able to retrieve their data and will not pay the ransom. Providing such support services and being in contact with victims aids law enforcers in identifying botnets.

Stuart Murdoch, CEO and Founder
Surevine

Challenges in scaling Surevine

Surevine does secure, scalable information sharing and collaborative intelligence analysis. It was formed as the CISP platform that brings together academia, law enforcement and businesses to share cybersecurity information, and includes social networking.

Surevine was established in 2008 to help those who have sensitive information to share, but found it hard to collaborate. Surevine is in the unusual position of having a product spun from R&D with a customer before spin-out. This put the company on a different trajectory where it was not compelled to raise funding to market its product. Therefore, there was steady growth without the points where businesses usually stall or plateau.

When the business started the co-founders communicated with the team every day, so there was a common culture and knowledge and communication effort was not necessary. It is recognised that this communication model starts to break down at a team size of 7+ or minus 2. It went from collaboration systems using own technology and working with each other and customers, to starting to need a structure, and then to the size of the business now which is quite different. The problems that are encountered are also different.

The three critical stages from entrepreneur to CEO after the second plateau became obvious. What needs to happen when the business gets to 24 people? There is a need to break things down into different structures involving different skills. There is a change in what the CEO spends their time doing. Progress has meant not being involved in the day to day running of the business and stepping back from the day to day operational side.

This is hard for an entrepreneur to do and making the change has required different skills. A different dynamic has been built with the Board. There was a need for strategic thinking rather than involvement in operations. Strategic growth has involved 3 people on the Board from outside the business in order to keep the focus on the strategy. A layer of middle-management has also been brought in for the day to day decision making.

It has been difficult to take such a step back and to no longer know all of the workforce personally. Information and communication is now mediated by others, but this has allowed the CEO to focus on the scale of the business. Where the business was self-managed before, in order to get the job done, each team now needs to operate independently to address problems, but also still feel part of the Surevine culture.

What's next? Growth means growth into new markets. Growth overseas brings new challenges. How does a business without venture capital go out into the global market? A main asset is a good technical skill base and having loyal employees. In Silicon Valley the average time an employee stays with a company is 6 months, and they can also earn a high salary. In the UK, if we want businesses to scale and grow, we have to keep skills based in the UK and not have firms swallowed up by US firms. If an employee is only staying in a firm for 6 months, they will have less loyalty and be less efficient. For example, why would they care about who might have to fix bugs in the system next year if they are planning to have moved on? It is therefore vital that we keep a reliable, long-term skills base in the UK.

Ryan O'Leary, Senior Director, US Threat Detection Centre WhiteHat Security

Security at Scale: The Impossible Challenge

Business is driven by websites. There is an ever-increasing online presence with an increasing number of criminals using more sophisticated methods. So there is an ever-growing attack landscape being defended by small security teams. This is due to a lack of talent and good security automation.

WhiteHat was founded on the problem of scale. The reasons scaling is difficult are simple. There is huge demand, and a shortage of talent that is also expensive to hire. WhiteHat realised there was a long gap in the ability to test sites, with time wasted sifting through false positives and negatives. The model does not work, so the solution was to bring automation and customer together where WhiteHat vets security vulnerability.

Is it impossible for companies to assess vulnerabilities and securities? Probably since there are many attacks and possibly only 10 people to do the job. There are never enough people to address security. Businesses are moving to the Cloud and a growing number of stores are going online. Therefore there will be more attacks. The bad guys will find ways to bypass blocked vulnerabilities, the shortage of security talent will be worst in small and medium companies, and there are not a lot of good security tools with having to check false negatives costing money. Supply and demand for talent and security is human driven. For example, a bank can transfer money to another person's account, but it can also carry out a negative transfer due to sloppy coding allowing it to happen.

Security has moved from the basement to the boardroom, but it is still under-resourced. In 2011 Sony PlayStation was breached and brought down with a huge loss of revenue. The clean-up cost for Sony was $171 million. Target and Ashley Madison were also breached when the only data they had to protect was their users'. Anthem also lost sensitive medical data. All of these data breaches snowballed into the need to accelerate security teams.

There is a demand, but people do not scale. So why is there a shortage in the market? People are coming out of universities without having been taught security coding or vulnerability training, even in the heart of Silicon Valley. This is a systemic problem with universities, and firms do not want to have to train these people themselves.

Problems with scaling: -

First approach is to hire people, but good people will get bored testing a couple of sites and will move on when the firm has become dependent on them.

Outsource to SaaS platform with the skill set to provide continuous testing 24/7, but then there is no in-house talent development.

Take out cyber insurance. This is cheap at present, but everything else is a con. Currently, for $10,000 it is cheaper to take out insurance. However, the company will get insurance money in the event of a breach, but will lose brand reputation. Cyber insurance is cool at the moment; premiums are low and cover is high. They have no way of measuring what to charge in premiums and companies self-certify that they have all their security measures in place. When insurance companies start having to pay out, premiums will go through the roof.

Solutions: -

These are not simple. There is a need for more people to get into security. Secure coding will mean less avenues for attack, so courses in coding are needed at all universities. Developers being trained at university level need to think about security and more money needs to be available for security. Changes in mind sets need to move away from firewalls and AV.

There is a need for better testing – better tools – better people. Money spent on security is not seen to be working. There is a saying that there are two types of companies – those who have been breached, and those who don’t know they have been breached. More money needs to be invested in security.

BREAKOUT STREAM 1: SCALE-UPS

Moderators: Stephen Wray (CSIT), Sandy McKinnon (Pentech Ventures)

This stream was inspired by the Sherry Coutu "Scale –up Report on UK Economic Growth" published at the end of 2014. In this report Coutu outlines that while the UK was a great place to start a business it still lags other leading economies in high growth Scale-ups (fast growing companies that contribute substantial growth to the economy). According to the report, the most effective intervention government leaders, businesses and academics could do to drive the economy is to actively work toward closing the scale-up gap.

During the first session Alex van Someren (General Partner, Amadeus Capital Partners) provided an opening address speaking from experience of building successful cyber scale-up companies. The expert panel, who are currently leading, building and supporting scale-up businesses, discussed and advised on what they felt was essential to scale – up.

In this session the overriding theme was that of **customer validation** and knowing and building a relationship with that first customer. Patience in this area is essential!

- Know your customer and understand what they really want and where they really are – then go there!
- Continual customer discovery is essential. Start-ups can get enamoured with their own technology and must maintain a healthy scepticism about their product's ability to solve the problem
- Having the patience to nurture the relationship with the customer particularly when securing and gaining validation for the product for the first time
- It is not always possible to identify those businesses with high growth potential in order to provide bespoke or specialist assistance that can encourage scale
- Team formation is key to take the start-up to the next level – a motivated A-Team can change the world!

The second session on the scale-up theme looked at leadership and team formation. In this session Sandy McKinnon (Pentech Ventures) set the scene, speaking to what Pentech and other VC's look for in an investible team and commonalities in team dynamics from their most successful fast growth companies.

Once again a key theme emerged relating to **cultural fit** within the organisation. Good A-Teams can change the world!

- Core people involved at the early stages of start-up must lead NOT manage
- Just like making the first sale is hardest moving from 1 to 2 to 3 people is most difficult
- What should be sought in a co-founder – Courage, Camaraderie, Competence and Commitment
- Co-founders with complimentary skills should be sought
- Teams that adapt and collaborate with each other are successful
- Networks are essential in sourcing the right team members and co-founders
- Always follow –up! This is expected especially in the U.S.
- An idea will always be an idea without a champion

BREAKOUT STREAM 2: SECURE UBIQUITOUS NETWORKS

Session 1

NIMBUS: Cyber threats, malware and the cyber threat intelligence sharing ecosystem

Instant sharing of threat intelligence is the cornerstone of cyber defence, enabling effective response to threats. Who is sharing what and for what purpose?

Facilitator: Professor Sakir Sezer

Research Director: Secure Ubiquitous Networks, CSIT

Professor Sezer's research interests include cloud, SDN/VNF and mobile security, traffic forensics, malware analysis and high-performance networks and content processing. He has successfully managed numerous EPSRC and EU research projects comprising consortia of academic and industrial partners. His patented research has led to major advances in the field of high-performance content and security processing and is being commercialised by Titan IC Systems. He has published 146 research papers, has given many plenary and keynote talks at major international (e.g. IEEE, IET) conferences.

Co-Facilitator: Ryan O'Leary

Senior Director, US Threat Detection Centre, WhiteHat Security

Session 2

Secure Ubiquitous Communications Networks

Emerging Internet of Things (IoT) technologies and the security of underpinning ubiquitous networks: - A system is only as secure as its weakest link – what are the security challenges of ubiquitous networking for IoT? Discussions topics:

- automotive/vehicle cybersecurity,
- ICS/smart grid security,
- Connected health security.

Facilitator: Professor Sakir Sezer

Research Director: Secure Ubiquitous Networks, CSIT

Co-Facilitator: Ulf Lindqvist

Programme Director, SRI International

BREAKOUT STREAM 3: DEVICE AUTHENTICATION

Session 1

Lightweight Authentication for IoT devices

Co-facilitators – Dr Liz O'Sullivan (CSIT), Dr Neil Hanley (Sirona Technologies Ltd)

Cisco estimates that by 2020 there will be over 50 billion connected devices, changing how we interact with the world as they communicate with each other in the background. Autonomous cars, homes that know when to turn the heating on, real-time health monitoring will all become a reality. This increased connectivity opens up a range of new attack vectors, allowing hackers to disrupt cyber-physical systems on a new scale. This is already an issue as has been seen by the numerous hacks appearing constantly in the news, most notably the infamous "Jeep hack" featured in Wired magazine, as well as a recent power outage in the Ukraine that was attributed to a cyber-attack.

Securing these connected devices is far from a trivial problem, not least due to the wide range of computational capability in the IoT devices, from high end dedicated ASICs to low cost, throwaway RFID tags. The objective of this session was to discuss the challenges of this new paradigm, and to explore new lightweight ways to authenticate devices, for example using physical unclonable functions, and how to ensure compatibility with existing products and protocols.

Dr Elizabeth O'Sullivan introduced the session, explaining the background to the topic area and setting out the objectives of the session.

Dr Neil Hanley, CSIT Research Fellow, and Co-founder and CTO of Sirona Technologies kicked off the session with a short background presentation covering the following areas:

- Some examples of IoT implementation scenarios including connected homes, industrial control systems, medical implants and devices and connected cars.
- Some examples of recent newsworthy attacks including cars being forced to crash, electronic door locks being compromised in hotels and the recent Ukraine power plant attack.
- The range of devices to be secured, from high-powered servers, through laptops and tablets, to low-cost RFID tags.
- A summary of the many protocols (e.g. Thread, Alljoyn, Zigbee) and algorithms (e.g. AES, Simon & Speck, ECC) which are already in play and provide challenges in evaluation and interoperability.
- An introduction to Physical unclonable Functions (PUFs) and the ongoing work at CSIT in this area.

Dr O'Sullivan then opened the discussion to the group, offering delegates the opportunity to explain their own perspective on IoT device authentication and the specific challenges faced by their own organisations. Some of the challenges observed and discussed included:

- ***Ad hoc networks*** – if establishing, or participating in, any kind of ad-hoc network, there needs to be some way to quickly establish an appropriate level of identity, authentication and trust.
- ***Information integrity*** – in addition to the identification of devices as the source of information, there needs to be some way to guarantee the integrity of the information provided, especially important in scenarios where safety is a concern, such as vehicle telematics.
- ***Authorisation*** – beyond authentication, there also needs to be an appropriate model of authorisation and fraud detection capability

- ***Long term security*** – in applications such as space communications or building sensors, where devices may be out of reach, there needs to be some method of ensuring their long-term security.

- ***Code signing and software/firmware updates*** – where devices are inaccessible, there needs to be an appropriate method of authenticating code updates and patches.

- ***Managing the human element*** – even within an IoT environment, there is still often the need for human interaction. As the weakest link in the security chain, are there authentication approaches which could effectively remove/replace the human? This led to an interesting discussion on biometrics and the challenges of convenience, privacy and the potential use of inferred identity.

Dr O'Sullivan closed the session by thanking all the delegates for their insights and drawing the following summary conclusions:

- There are many varying perspectives on IoT and a similar variety in the challenges.

- The use cases and challenges discussed align well with the assumptions and problem statements which underpin the work at CSIT.

- The PUF technology being developed at CSIT has the potential to address many of the challenges of authentication in a machine-to-machine environment.

- Other research programmes at CSIT align well with additional challenges in the areas of encryption and biometrics.

Session 2

Device Authentication in a Post Quantum World

Co-facilitators - Dr Liz O'Sullivan (CSIT), William Whyte (Security Innovations)

In February 2016, NIST released a Draft Report on Post-Quantum Cryptography announcing preliminary plans for the transition to quantum-safe cryptographic algorithms in NSA Suite B. This will mean increased key sizes for symmetric algorithms (AES) and secure hash algorithms (SHA) for encryption and message authentication, and a complete replacement of public key algorithms such as RSA, ECC and DSA for digital signatures and key establishment/exchange used in TLS/SSL, IPSec, X.509, SSH etc. The result is that the cryptographic algorithms and protocols that support authentication will change dramatically in the coming decades. Organisations that build systems and infrastructures that require long-term security and have long life spans are urged to consider this transition in architectural designs now. Efforts are in place within NIST, ETSI, IETF, and in EU Horizon2020 Projects such as SAFEcrypto, for which CSIT is the lead partner, to examine potential replacements for current public key cryptographic algorithms.

The objective of this session was to explore the effects that quantum computing may have on both existing applications and emerging technologies. In particular the session was seeking insights from industry to feed in to ongoing research programmes and standardisation efforts.

Dr Elizabeth O'Sullivan introduced the session, explaining the background to the topic area and presenting some background material, including:

- An introduction to post quantum cryptography, and the challenges presented if a scalable quantum factoring device emerges.

- An overview of the leading approaches to quantum safe cryptography.

- An introduction to the SAFEcrypto Horizon 2020 project, covering consortium partners, use cases and the main project activities:
    - Vulnerability and risk assessment for use cases
    - Derivation of lattice-based constructs (signatures, authentication, IBE, ABE)
    - Hardware and software architectures for selected primitives
    - Physical attach-resistant design methods
    - Management, distribution and storage of keys
    - Proof of concept demonstrator
- An introduction to the questions being studied by the ETSI Quantum Safe Crypto group:
    - Do we need drop-in replacements for current technologies or new advanced approaches?
    - What are the most common specific use case scenarios?
    - What is the balance between strong theory and practical efficiency?
    - Should solutions be in hardware, software or both?
    - What are the interoperability challenges?
    - What should a migration plan look like?

William Whyte then outlined some very specific challenges he was observing in the world of Vehicle-to-Vehicle (V2V) communications, including the challenge of the overhead required for passing authentication and signature parameters when there is already a high volume of communication in a short time period.

The discussion was then opened to the delegates, and a lively discussion followed, including the following main topics:

- ***Constrained devices*** – where devices are low power, or have only a small amount of memory, there is a real challenge presented concerning updates. If software or firmware updates are required, then there needs to be space on the device for at least two versions of the software/firmware, plus updating algorithm.
- ***Constrained communications*** – some delegates mentioned uses cases where only very low bandwidth communications are available, introducing additional overhead challenges.
- ***Consistency*** – in an IoT environment, where many devices are involved, keeping all those devices synchronised can be challenging, especially when devices may not be always-on. How would delayed updates be handled? What happens to the device during the update cycle?
- ***Identity Based Encryption (IBE)*** – the Estonian government model was discussed, where protection is implemented using identity based encryption so that only certain sub-sets of data can be accessed by a device or person based on their identity credentials.
- ***The ethereal nature of quantum computing*** – as quantum computing is a future technology, it can be hard to convince people, especially in industry, that this problem needs to be addressed now. Why not just wait until quantum computing is realised?

Dr O'Sullivan thanked the delegates for their views and participation, and confirmed that some of the topics discussed would be fed back into the SAFEcrypto project and the ETSI standardisation efforts.

BREAKOUT STREAM 4: SECURITY ANALYTICS & AUTONOMOUS SENSOR SECURITY

Session 1

Data-driven intelligent autonomous systems for real-time situation awareness

Co-facilitators - Prof Weiru Liu (CSIT), Pete Lockhart (Roke Manor Research Ltd)

CSIT's theoretical research focuses on uncertain information fusion; multi-criteria decision making, online planning under uncertainty, and multi-agent systems, in addition to real-time data analytics. This research has led to:

1. Design and development of a multi-agent based event reasoning framework for correlating dispersed events detected (data analytics) from heterogeneous sources in a distributed complex environment for achieving situation awareness (decision making, planning, and actions). Applications include intelligent surveillance in cyber-physical systems, smart homes, and intelligent energy and transport management in smart cities.

2. Design and development of intelligent autonomous systems using multi-agent techniques for complex control problems (e.g., SCADA) and for designing collaborative (software) agents, or mixed teams of multi-robots and human for working together in complex environment. Applications include search and rescue services, complex industrial control problems, and games for entertainment or education.

Through sensor information fusion from large sensor networks, we can detect anomalous behaviour and malfunctions in sensors for security or other purpose of interests. Real-time surveillance information is used for achieving situation awareness for decision making, dynamic online planning and actions. Furthermore, game-theoretic approaches have been developed to allocate (security) resources based on real-time surveillance information (through data analytics and information fusion).

Prof Liu provided a demonstration of event reasoning tools demonstrated as part of CSIT's PACES project followed by Pete Lockhart introducing some of Roke's state of the art autonomous vehicle developments followed by a security model for machine situational awareness before asking how businesses might put a regulatory framework around it. A group discussion then followed with challenges articulated including:

- Vehicles put an unreasonable amount of trust on GPS systems. There is a need to analysis what you is being assumed and what levels of trust is put in them.
- Balance checking, is this consistent with what we expect?
- Spoofing tyre pressure sensors could be an issue with VIP vehicles for example if wanting to stop
- There is a need to secure the connectivity layers.
- In the IoT world a lot of this is driven by cost, which is a huge concern.
- The transport sector walking blind into security issues.
- Analogies in electrical safety world – redundancy, time to failure, level of assurance
- What are the economic drivers for security in theses spaces?
- Does safety take priority over security – is there a security economics issue?
- Economics of security, rules haven't been written.

- Are market verticals actually broken – can you really expect a 80 year old to download a patch onto their car to keep it secure?
- Autonomous systems still have human element at the top as ultimate arbitrator
- We assume data is correct. Someone could be feeding false data. How can we trust the data provider? How do we trust that it isn't being spoofed?
- How do you spot data incest, data recycling?
- Credit card industry have been in this for 30 years – its called fraud detection. Security community needs to learn from fraud detection algorithms in the credit card industry.
- Trusting your data is a wider problem than cyber security, need redundancy, duplication, where one sensor is faulty you trust a second one
- Biology – many parts of body are duplicated – two ears, eyes, lungs, etc
- Subsumption architecture in vision, human body walking downstairs. Lower level overrides higher level thinking – safety
- Do you create a sense of self that is the systems compass that is the default state that should be returned to?
- Turn the processing model on its head, process exceptions rather than everything
- Can you mine a provenance graph from communications up and down the stack?

Applications where we could apply this stack of technologies included:

- Wayfinding, autonomous energy management, military domain
- Last mile delivery robots
- Autonomous cars should operate in certain ways – if knowledge is changed – what?
- What happens if humans forget how to drive cars, then what? Is it like learning to ride a bike?
- Five step framework from assisted autonomy to full autonomy

Session 2

Security Analytics: Big and Deep, Just How We like It

Co-facilitators – Dr Paul Millar (CSIT), Dr Ben Greene (Analytics Engines), Will Semple (PWC)

As with many other application domains, the Big Data analytics revolution is starting to change the intelligent security landscape. Next generation Security Information and Event management systems will be run on platforms such as Hadoop using programming tools such as MapReduce, PIG and Storm. These tools have the potential to provide a considerable advance in actionable security intelligence by reducing the time for correlating and contextualizing heterogeneous security event information, and also for correlating longer-term log data for forensic purposes. However, there are several challenges that need to be overcome before its potential can be fully realised. These include data provenance, privacy, security and availability. In particular the lack of available big data benchmarks in the information security domain is a serious impediment to future research. At this year's NIPS conference, arguably the world's premier machine learning conference, there were 400 papers presented, but not a single one on security analytics. To help illustrate these issues we will describe current work ongoing in CSIT which is looking at streaming deep graph mining for network intrusion detection.

Following a presentation by Dr Paul Millar on the big data, processing, SIEM's, Graph mining and deep learning the panel led a discussion during which the following research challenges and opportunities where articulated:

Confidentiality is an issue. Agreement needs to be explicitly made with customers when their data is shared on first contact and subsequently for each individual new evolution of the research. Industry has huge PR challenges around researching on individuals data.

Is there a double edged sword however? In Bio/Pharma patients provide data, if the researcher finds anomalies it is beholden on researchers to feedback to patients. Code of ethics guidance lessons need to be learned.

Researchers are coming up against private companies and private data. To counter this, researchers need to flag up the benchmark that data sets would allow them reach. More compelling arguments needed. Knowing more tomorrow than we do today is not enough.

Could Government cyber security strategy incorporate recommendations around providing data sets? Possibly. Is the provision of data sets almost a research question in its own right? There are Privacy, security, identifiability, commercial interests.

Could industry help researchers calibrate synthetic data? This might lead to concerns around fidelity – how real?

Perhaps the idea is that the data never gets out, companies offer a service where new algorithms can be tested against?

SIEMs

Industry currently tunes and prunes SIEM settings to limit output. Extensive research is required on new tools and techniques for finding unknown unknowns. The best place to start is what question does the human analyst ask? This question comes down to visibility. Forensic responders are likely to dig deeper into the host so security analytics should initially mimic this and be used to gain visibility.

Data sets

The group discussed what the right data set looks like to carry out the research on so that different tools and techniques can be benchmarked. A baseline level was discussed, where that should be set and even what makes up a universal baseline. What is the data wishlist?

Data controllers and processors are rightly reluctant to share. Notwithstanding, some data can be shared. For example malware samples could be (given the appropriate legal authority to store and process) but not companies IP or customer data.

There are no tools which can verifiably export cleansed data, free from sensitive information. This represents a research and development opportunity.

The group debated whether this could be done with local public sector or open data for example. It doesn't have to be the MOD or similar.

Securing big data stores

Securing big data stores is a problem. There are currently perimeter based offerings for Hadoop such as Cloudera's solutions. Embedding security directly into data stores might be a solution. An alternative approach might be to identify the data people wish to take and why. Perimeter security may now be largely irrelevant.

If we solve this where do our adversaries go next? It is easier for adversaries to buy compute power than many organisations. As a result they will develop their own adversarial tools using machine learning.

Final thoughts

Google are offering up free/cheap services with the intention of gaining datasets that they can analyse specifically to differentiate their own enterprise offerings in terms of security.

Human Computer Interaction – what are the best ways to visualise incidents so non-PhD's in SOCs can analyse, interact and experience the data?

The technologies are there, the limitation is the imagination of developers.

THE QUEEN'S ANNIVERSARY PRIZES

FOR HIGHER AND FURTHER EDUCATION

2015

CSIT was honoured by Her Majesty the Queen in 2015 for its work in "strengthening global cyber security"

CSIT CENTRE FOR SECURE INFORMATION TECHNOLOGIES

A Global Innovation Hub for Cyber Security

www.csit.qub.ac.uk