T H E E L E C T R O N

N E W S L E T T E R O F T H E I N S T I T U T I O N O F E L E C T R O N I C S

Issue 35: Autumn 2017

IP EXPO EUROPE

IP EXPO Europe opened its doors at London's ExCel exhibition centre on 4th. and 5th. October, uniquely covering the entire enterprise IT stack from cloud to cyber security and DevOps through Artificial Intelligence, Analytics and The Internet of Things (IoT).

The overall event was comprised of six sub-events under the headings of Cloud Europe; Cyber Security Europe; Networks and Infrastructure Europe; Artificial Intelligence (AI), Analytics and IoT Europe; DevOps Europe and Open Source Europe. It featured some 260 presentations and around 236 exhibitors.

First held in 2006, the event has seen attendances grow every year, reaching a total of 15, 512 attendees in 2016.

A notable addition for 2017 was the widened scope of the exhibition to include machine learning, Artificial Intelligence, cognitive and deep learning technologies.

Organisers Imago Techmedia state:

'IP EXPO Europe is Europe's number one enterprise IT event. As organisations move more of their technology to the cloud and adapt to thrive in a world of big data and growing cyber security threats IP EXPO Europe will continue to evolve and deliver the biggest and most engaged IT decision maker audience available'

Below a review of some of the major and ground-breaking themes of IP EXPO Europe 2017 is presented.

GDPR AND WHAT IT MEANS FOR BUSINESS

The European ruling on the General Data Protection Regulation (GDPR) comes into force on 25th. May 2018 and such is its importance that a complete seminar programme at IP EXPO Europe was dedicated to it.

In his paper 'GDPR: What does it mean for Businesses?' Ian Kilpatrick, EVP Cyber Security for Nuvius Group describes GDPR as "a game-changer in how organisations store, secure and manage personal data'.

With fines for data breaches amounting to four per cent of annual global turnover, or 20 million euros, whichever is greater, the consequences of any data loss is likely to be "financially devastating". [This compares with the current Information Commissioner's Office current maximum penalty of £500,000].

Mr. Kilpatrick states:

"The data in question could be usernames, location data, online identifiers like IP address or cookies, or passwords. The loss of personal or work-related information - whether that's access details, passwords or any other customer data - is endemic today; almost 1.4 billion data records were lost in 2016 alone, an increase of 86 per cent compared to the year before.

GDPR doesn't prescribe specific data protection technologies, but rather processes that organisations should undertake. However, companies should be talking to their IT providers about core data security solutions that cover things like encryption, access and identity management, two factor authentication, application control, intrusion prevention and detection, URL filtering, APT blocking and data loss protection. Also, they shouldn't neglect the network, by securing wireless access points, for example."

It is noted that the purpose of the new regulation is to shift control of personal data back to the owner of that data. When the new regulations come into force UK organisations will have just 72 hours to disclose any serious data breaches to the Information Commissioner's Office as well as the victim of the breach. Failure to notify may result in a fine of 10 million euros or two per cent of revenues.

Organisations that are based outside the EU are reminded that they still have to comply if they wish to continue using data from customers in the EU.

Restorepoint Universal Console

In order to help organisations achieve compliance, Restorepoint has launched its Universal Console, which aims to assist particularly with data protection by design and by default.

Article 25 of the GDPR states that organisations must deliver robust data protection both by design (appropriate technical and organisational measures must be deliberately taken) and by default (onus must not be on individuals to opt in to having their data protected).

Restorepoint states:

'Restorepoint Universal Console is able to both secure access to systems that control or store personal data, and leave a comprehensive audit trail, so that security can be clearly demonstrated. It acts as a single access gateway to all servers and network devices, eliminating two of the most common security risks today: privileged user access and lack of unified audit controls.

UC eliminates shared user credentials and passwords, controlling access to systems on a per-user basis, without modifying the target system. Administrators gain tight control over who has access to which information, and can alter these permissions at the touch of a button. Recording and playback features enable them to review user sessions. It is also quick and easy to suspend or revoke access automatically when employees or contractors perform prohibited actions, or when they leave the company.'

Confidentiality, Integrity, Availability and Resilience

Article 32 of the GDPR requires organisations to be able to 'ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services' and 'restore the availability and access to personal data in a timely manner in the event of a physical or technical incident'.

Restorepoint states:

'Restorepoint helps ensure that the processing systems and services underpinning the handling of personal data are highly available and resilient by centralising the backup of network configurations from over 65 network, security and storage vendors. With its simple one-click recovery process, Restorepoint can greatly speed up the restoration of services following an outage caused by hardware failure, unauthorised or incorrect configuration changes. Unlike scripting solutions that require time and expertise to set up , Restorepoint can be deployed and be protecting the network within minutes.

Restorepoint's compliance engine provides continual visibility of compliance status by automatically detecting changes in configuration, tracking against configuration policies and baselines, without intrusive network scans.

Policies are easily created and applied to multiple network devices, with compliance analysis performed automatically each time a network device is backed up. Alerts can be forwarded to SIEM products (syslog), monitoring platforms (SNMP), sent via email, or retrieved via the API.'

The Network and Information Systems Directive

This Directive, which also comes into force in May 2018, complements the GDPR and introduces fines of up to £17 million or 4 per cent of global turnover if organisations, particularly in areas such as water, energy, transport and healthcare, fail to take adequate steps to protect against hackers.

The article 'In the Line of Fire' by Brian Wall in *Computing Security*, September-October 2017, explains more, noting the NISD's role as being 'designed to create a focus on the protection of IT systems in European critical national infrastructure'.

Member states will be required to adopt a national cyber security strategy which defines objectives, policies and regulatory measures, and the Directive recognises that providers of some digital services have now become part of the critical national infrastructure. Providers, for example, of search engines and cloud services, will therefore come under the legislation.

Businesses which the Directive recognises as being 'operators of essential services' will have to 'take appropriate security measures' and 'report serious incidents to the national authority'.

The author states:

'As critical national infrastructures move towards increasingly connected large networks that allow for monitoring and remote automated control via computer networks, the potential for cyber attacks rises. The legislation will help strengthen the security standards of industries that operate critical infrastructure that people depend upon.'

CYBER CRIMINALS FOCUS ON CREDENTIAL THEFT

Criminal tactics used to access user credentials are growing in prevalence and sophistication according to WatchGuard's latest quarterly Internet Security Report. It also reveals that 47 per cent of all malware is now zero day and able to evade signature-based antivirus solutions.

Mimikatz, a popular open source tool used for credential theft, accounted for 36 per cent of the top ten malware, making it the highest.

WatchGuard state:

'Often used to steal and replace Windows credentials, this is the first time Mimikatz has appeared in the familiar group of top ten malware variants, showing that attackers are constantly adjusting tactics. The report also shows that phishing attacks are increasingly using malicious JavaScript to fool users. For several quarters attackers have leveraged JavaScript code and downloaders to deliver malware in web and email-based attacks. Attackers were seen to use JavaScript in HTML attachments to phishing emails that mimic login pages for popular legitimate sites like Google, Microsoft and others to trick users into willingly giving up their credentials.'

Another tactic has been the use of an old Linux application vulnerability to target Scandinavia and the Netherlands with attacks designed to steal password hash files, and automated tools against web servers have been used to crack user credentials:

'With the heightened prevalence of web-based attacks against authentication, brute force login attempts against web servers were present among the top ten network attacks. Web servers without protections that monitor failed logins leave automated attacks unchecked to guess thousands of passwords each second.'

A further finding was that nearly half of all malware is able to circumvent legacy AV solutions, indicating that signature-based AV is increasingly unreliable when it comes to catching new threats.

The report is based on anonymised FireFox Feed data from over 33,500 active WatchGuard UTM appliances worldwide. In total these appliances blocked more than 16 million malware variants in quarter 2, with an average of 488 samples blocked by each individual device. WatchGuard's Gateway AV solution intercepted almost 11 million malware variants (a 35 per cent increase over quarter 1), while APT Blocker caught an additional 5,484,320 malware variants (a 53 per cent spike over quarter 1). Additionally, WatchGuard's Firebox appliances stopped nearly 3 million network attacks in quarter 2, at a rate of 86 attacks blocked per device.

Corey Nachreiner, Chief Technology Officer for WatchGuard Technologies, concludes:

"From JavaScript-enabled phishing attacks and attempts to steal Linux passwords, to brute force attacks against web servers, the common theme here is that login access is a top priority for criminals. Knowing this, businesses must harden exposed servers, seriously consider multi-factor authentication, train users to identify phishing attacks and implement advanced threat prevention solutions to protect their valuable data."

WatchGuard Technologies Inc. is a global leader in network security based in Seattle, providing Unified Threat Management, Next Generation Firewall, secure WiFi and network intelligence products to more than 80,000 customers worldwide. The report may be downloaded from www.watchguard.com

ENTROPY AS A SERVICE

Random numbers underpin cryptography and are used to make cryptographic keys that lock and unlock access to data and systems. Billions of keys are made every day and almost every web connection, email, credit card transaction and IoT communication relies on them.

In *Network Computing*, Vol.26, No.5 (September/October 2017), Richard Foulds, General Manager for Whitewood Security, in his article 'Network Security Disorder' explains how the vast majority of these 'keys' are unmanaged and unprotected to the extent that as the computing resources of cyber attackers advance their ability to conduct brute force key finding attacks is more likely to succeed.

The author states:

'Currently, almost all cryptographic keys are generated by operating systems. But software is deterministic - it is preprogrammed - and if it does anything random we call it a bug. To trigger behaviour that is random, the operating system has to sample sources of randomness, more properly called entropy.'

Operating systems typically capture entropy by sampling aspects of the physical environment, from user mouse clicks to radio noise and timing jitter in the hardware, which the author says is alright for the physical world, but not for a virtual or cloud environment:

'One of the downsides of virtualisation is that it is cut off from supplies of entropy. There simply aren't enough sources of natural randomness behind the walls of a data centre.

Iot devices also suffer from entropy starvation as they tend to be low power and low-cost devices, designed for specific tasks with very limited access to randomness. How does a smart meter wake up and get a random number so it can encrypt data and securely transmit a reading?'

The answer, according to Mr. Foulds, may lie in the form of quantum-based entropy:

'Quantum entropy sources exploit random behaviour at the sub-atomic level, which is fundamentally random and unpredictable, even with unlimited computing resources. Quantum-derived entropy is the nearest you can get to perfect randomness.

As systems become more distributed across virtualised and cloud environments and the volume of Iot devices increases, it's a question of both quality and quantity. The idea of entropy as a service offers a way forward.'

In his conclusion the author points to a growing reliance on cryptography that amplifies the need for generating true random numbers:

'Complete confidence in your security systems can only come from a constant supply of true entropy across your entire application environment.'

CYBER SECURITY CHALLENGE UK

Ben Jackson, an 18-year-old student from Kings Hill in Kent, has become the latest winner of the Cyber Security Challenge Masterclass, the culmination of a year-long programme of competitions in which the best of 42 candidates from online and face-to-face rounds are invited to compete to become Britain's cyber security champion.

The 2016 Masterclass was led by PwC with the support of a consortium of organisations that included GCHQ, NCA and The Bank of England. Together they created a hyper-real cyber defence simulation in which teams had to protect a fictional global energy company called Bolt Power from a series of cyber attacks and insider threats.

Contestants played the role of PwC cyber security consultants brought in to investigate suspicious activity on the fictitious company's IT network. Teams then had to protect the company from cyber attacks launched by hacktivist groups in real-time, make quick decisions based on live intelligence updates from both clients and government agencies, prevent information leaks, and demonstrate competence in communicating technical information effectively.

The 2017 Masterclass is being held in November, led by BT. Those wishing to enter for the 2018 competition are invited to play the online games using the Cyber Challenge Play on Demand Portal and Cyphinx™, the first online virtual world designed solely to find, test and recruit cyber talent.

In introducing the second issue of *Inside Cyber*, the magazine of Cyber Security Challenge UK, the CEO of Cyber Security Challenge, Stephanie Daman, says:

"The Challenge was formed in 2010 and over the past seven years we have witnessed a phenomenal amount of talented individuals enter the cyber security industry. This is the critical aim of our work, particularly given the predicted shortfall of 1.8 million skilled cyber workers by 2022 announced recently by (ISC)2.

European Cyber Security Challenge

In addition to Cyber Security Challenge UK there is also the European Cyber Security Challenge, an annual event organised by the European Union Agency for Network and Information Security (ENISA) that aims to discover young and emerging cyber security talent across Europe.

This provides an opportunity for the top cyber defenders from each country to meet, network, collaborate and finally compete in order to determine which country has the best cyber talents.

Challenges require contestants to solve security related tasks from domains such as web security, mobile security, crypto puzzles, reverse engineering and forensics.

Details are provided at www.europeancybersecuritychallenge.eu

INDUSTRIAL CONTROL SYSTEMS TECHNICAL SECURITY ASSURANCE

Industrial control systems are deeply embedded in many different industry sector organisations and play a vital role in organisations that make up the critical infrastructure of the country (such as energy, water, transport and healthcare).

In the past the relative isolation and specialised nature of ICS environments has meant that vulnerability to cyber attacks has been relatively low, but new research from CREST, a not-for-profit organisation that represents the technical information security industry, has revealed that this situation is now changing. An increase in the connection of ICS environments into the wider corporate network of many organisations (for example to support business process efficiencies) and greater use of conventional IT technologies (for example to lower costs associated with support and maintenance) has resulted in substantially increased cyber attack vulnerability and a number of real incidents.

In response to these developments CREST has published a Position Paper with the above title. Key major findings include the following:

*In the absence of periodic standards-based technical security testing ICS environment owners and operators have no objective way of gaining assurance that cyber risk is being adequately managed.

* ICS environments are rapidly changing (due to process optimisation, Information Technology/ Operational Technology convergence and technology evolution) and this is leading to a higher degree of exposure and a risk profile that is characteristic of conventional IT environments.

* Securing ICS environments in many organisations is technically demanding and difficult to undertake (due to obscure and often obsolete technology, limited resources and a high degree of sensitivity).

* Technical security testing specialists regard inadequate management support (such as lack of budget and poor resourcing) as the most important factor affecting the ability to secure ICS environments and undertake technical security testing activities.

* ICS security standards and guidelines are evolving but currently contain little information to directly help technical security testers, and there is no definitive standard for technical security testing in ICS environments that is mandated by regulatory bodies.

* As a result of the unique technologies, critical processes and sensitive testing requirements there is a higher demand placed on the skills, knowledge and situational awareness of technical security testers working in ICS environments as opposed to conventional IT environments.

Industrial control systems that form part of the critical national infrastructure are described as "high risk and high business impact" and therefore "require the highest level of technical testing", including Simulated Target Attack and Response (STAR) and objective focused penetration testing.

It is noted, however, that while aspects of ICS environments are unique, it is increasingly the case that with the adoption of conventional IT, ICS technical architecture is becoming less obscure and easier to understand and manage, but the paper urges "extreme caution" when conducting technical tests due to the high sensitivity of many ICS environments:

'In contrast with conventional IT environments, ICS environments typically place a higher value on "availability" than "integrity" or "confidentiality". This requires a different approach to technical security testing. Conventional technical security tests that are invasive in nature or place a burden on the network may inadvertently cause damaging loss of service events and should be avoided. For example, where a "ping sweep" might be used in a conventional IT environment to help identify hosts and nodes it might be more appropriate in an ICS environment to examine router configuration files or even to trace the physical wires for confirmation of connections.'

The convergence of IT and OT is also noted to be creating new challenges not only for solution architects, designers and implementation teams, but also for technical security testers:

'The use of network scanners in OT environments is problematic and can be disruptive or even cause devices to fail. Network security products designed to work within IT environments have not been prepared to work within an OT world that operates with more exacting communication parameters.'

The increased connectivity of IT and OT has also altered the risk profile of ICS environments:

'Previously isolated OT environments that would have been difficult to attack are now exposed to the same level of malicious activity that affects conventional IT environments. This potentially broadens the scope of any technical security testing that is required and necessitates the need for greater situational awareness and more use of threat modelling and intelligence-led testing.'

In its 'conclusions and recommendations' the paper states:

'ICS environments are more sensitive than conventional IT environments and technical security testing that could potentially be damaging should be planned and undertaken with a high degree of caution. This "deterministic" nature of the devices in ICS environments requires a different approach but not one that is so impoverished that it provides little value or assurance about the strength of measures to resist attack.'

Copies of the paper may be obtained from CREST on 0845 686 5542 or by emailing admin@crest-approved.org

AUTISM AND THE TECHNICAL SECURITY INDUSTRY

In addition to the above Position Paper CREST has also published a report entitled 'Autism and the Technical Security Industry' in conjunction with the Information Assurance Advisory Council (IAAC), Cyber Challenge UK and The National Autistic Society.

In October 2016 the IAAC ran a workshop with The National Autistic Society, members of the security industry and academia to discuss careers, skills and diversity. In particular this considered the question 'how can we support the autistic people who may have an interest in working in the cyber security industry to make sure that they have the relevant opportunities and they understand what is required of them in terms of identifying and moving towards a career in technical cyber security?'

CREST was invited to help provide some answers and six primary activities were identified:

(i) Making individuals with autism aware of the opportunities available within the cyber security industry.

(ii) Ensuring that they recognised that there was a positive view of some of the attributes that they demonstrate.

(iii) Increasing the feeling of being valued.

(iv) Supporting the application process.

(v) Supporting the interview process.

(vi) Providing support in the working environment.

The report highlights the current skills shortage within the technical security industry and calls for action from the cyber security industry in a number of areas:

'In addition to career guides the cyber security industry could easily provide more specific information packs on why the industry is interested in the positive attributes associated with autism. In addition to written documents, the industry could produce a short film on these positive attributes and how they can be applied to certain job roles within the industry. It would also help to show why individuals demonstrating these attributes are extremely valuable to organisations and to the industry as a whole.'

A call is made for more effort to make young people with autism aware of initiatives such as Cyber Security Challenge:

'We can develop individual challenges to try to raise their level of confidence before we introduce them into national competitions against a much wider audience.'

Certain roles, such as malware reverse engineering, penetration testing and intrusion analysis are identified as being 'roles where a number of autistic traits would be really beneficial in terms of the individual', and there are calls for the industry to help autistic candidates to work through the application process:

'The industry could work with existing autism institutions to provide a checklist of important considerations for completing applications and provide specific guidance. This would be designed to help somebody with autistic traits to complete what other individuals would find easy in terms of open-ended questions and to understand better what a potential employer may be looking for.

The industry could provide a showcase for autistic cyber-related activities encouraging individuals with autism to write documents, to do activities and forming an important part of their application process. Rather than having to describe the details of what they have done during a formal interview process, they showcase something they have previously completed and therefore demonstrate competence and capability.'

Among the initiatives currently being promoted by CREST is the concept of virtual work placements to help overcome geographical restrictions and financial difficulties associated with identifying work placement opportunities:

'These virtual work placements could provide the opportunity for individuals to comment or contribute to research activities which they then get recognised in terms of their contribution to a final publication. This remote but focused working may be very suitable for individuals with autism.

Virtual work placements could be a good way of providing the showcase and the opportunities for people with autism to demonstrate that they can work as a team, even if that team is remote, and provide a positive contribution.'

TELECOMS INDUSTRY AND DNS ATTACKS: ATTACKED THE MOST AND SLOWEST TO FIX

EfficientIP, a leading provider of DDI (DNS, DHCP and IPAM) solutions, has published a report on cyber security in the global telecoms industry that shows that telecoms companies suffer the most DNS-based attacks and that each attack on average costs around £460,000 to fix.

Key findings were that:

* DNS-based attacks cost organisations globally £1.7 million on average every year across several industries.

* 76 per cent of all organisations were subjected to a DNS attack over the last year and 28 per cent experienced data theft.

* 42 per cent of all respondents in the UK spent an entire business day (six hours) to restore their systems.

* The top five security threats for telecoms organisations were DDoS (42 per cent), Malware (36 per cent), DNS Tunnelling (31 per cent), Cache Poisoning (28 per cent), and Zero-day Exploits (20 per cent).

* Telecoms organisations suffered more attacks than any other surveyed (an average of four a year).

* 5 per cent of telecoms organisations surveyed admitted an attack cost them more than £3.75 million.

* A quarter of telecoms organisations lost sensitive customer information following a DNS attack.

* For 42 per cent of telecoms companies surveyed attacks resulted in in-house application downtime causing poor customer experience online.

* Recent cyber attacks have revealed the criticality of patching to avoid easy exploits, but telecoms companies have only applied an average of four patches out of the eleven critical ones recommended by the ISC in 2016.

* 40 per cent of telecoms companies took six hours to mitigate a DNS attack compared with just one hour for over 50 per cent of retailers.

In response to the findings EfficientIP's CEO David Williamson stated:

"Telecoms organisations need to adapt to the new surge of cyber attacks and cannot use yesterday's security technology for today's problems otherwise short and long-term costs could strike a severe blow to company revenues. To face recent industry challenges and customers' high performance expectations, the communications sector needs to change its approach to network management and incorporate automation as quickly as possible."

The 2017 Global DNS Threat Survey Report involved interviews with 1,000 respondents in three global regions (APAC, Europe and North America) which included CISOs, CIOs, CTOs, IT Managers, Security Managers and Network Managers. Telecoms organisations accounted for 10 per cent of the survey base with 10 per cent of the 1,000 organisations having UK headquarters.

Copies may be obtained from www.efficientip.com.

Protecting Data and ensuring DNS Services Continuity

At IP EXPO Martin Wellsted, General Manager, Northern Territory for EfficientIP, gave a presentation entitled 'Protect your Data from Data Exfiltration' in the Cloud Security Theatre.

Delegates were introduced to the world's first DNS security solution enabling complete DNS transactions inspection and advanced analytics for real-time behavioural threat detection, known as DNS Guardian. EfficientIP state:

'Patented smart countermeasures provide unique adaptive security to protect data and confidentiality and guarantee unmatched continuity of DNS services, even under the most insidious attacks.

DNS Guardian benefits from an architectural innovation that separates the DNS cache from the recursive function to dramatically strengthen and enhance the security of the overall service. When under attack, each function is protected separately regarding its own properties, avoiding side effects and ensuring service availability. DNS Guardian's patented countermeasures can be adapted to each function's specific needs and detected attack.'

DNS Guardian is noted to be particularly effective against DNS tunneling:

'Analysing non-cached DNS queries and size allows for efficient tunneling detection and prevention, far more so than a pattern-based detection based on a known, potentially outdated reference database.'

The advanced analytics provide 'an unprecedented understanding' of DNS threats that offers the opportunity to activate the right countermeasures at the right time according to each specific attack type:

'The Quarantine Mode isolates IP addresses with malicious behaviours so that they have unrestricted access to cache data only, while their recursive requests are blocked. This protects the server from the attack and reduces the risk of blocking legitimate clients.

However, under extreme conditions when a source attack is not identifiable (typically in the case of a slow-drip or highly distributed attack) DNS Guardian detects the risk of exhaustion of server capacity and activates the patented Rescue Mode. This exclusive countermeasure ensures that the cached DNS answers remain 100 per cent available to the clients, even if a data validity update is not possible, ensuring 100 per cent accessibility to most critical business applications and services.'

Provision is also made for upstream DNS server failure:

'When the global DNS system fails or becomes unreachable because of an internet backbone failure, a recursive DNS engine may not be able to serve a client's recursive DNS queries. As a result, clients end up disconnected from every service, while in fact they may still be accessible, up and running. DNS Guardian intelligence prevents such a situation occurring. When a request is received for a domain present in the cache but expired, DNS Guardian ignores the failure coming from the local recursive engine and responds to the client using the answer stored in the cache with a low TTL value (30 seconds). The benefit is an increased continuity of service during a short external failure, much like Rescue Mode.'

DNS Blast

Complementary to DNS Guardian is DNS Blast, said to be the world's fastest and most advanced DNS cache security solution. It is described by EfficientIP as 'a game-changing technology offering a revolutionary approach to DNS cache and recursive security.'

In addition to DNS Guardian, it also includes a hybrid DNS engine:

'The SOLIDserver ™ Blast appliance incorporates two DNS cache engines (BIND and Unbound), managed transparently as a single unit. It provides SmartArchitecture™ templates - a unique solution to easily design, deploy and centrally manage hybrid DNS architectures mixing servers that are running on different technologies. Hybrid DNS Engine ensures the highest level of security to instantaneously mitigate zero-day vulnerabilities and maintain full control of upgrade processes.'

It also simplifies DNS architectures to decrease TCO and obtain quick return on investment:

'DNS Blast is a purpose-built DNS security appliance that allows for the drastic simplification of a DNS infrastructure by eliminating dozens of DNS clusters, numerous load balancers and useless firewalls. The DNS server ensures its own security with performance and security focused on a single point, without the need for complex configurations or the irritating setup of approximative filtering rules.'

Also featured is improved resiliency and user experience with decentralised DNS architecture:

'DNS Blast's purpose-built high performance DNS security appliance enables new architecture designs by deploying servers as close as possible to users through distributed DNS infrastructure, just like CDNs do with their content appliances.'

INCREASED HACKING RISK FOR BLUETOOTH DEVICES

A set of previously unknown security vulnerabilities in Bluetooth technology has apparently left billions of devices, including phones, laptops and televisions, vulnerable to hacking. Experts from Armis, a security firm, have found flaws that could potentially put up to 5.3 billion devices with Bluetooth capabilities at risk from a particularly infectious type of attack.

Based on a proof of concept, the security gaps, named BlueBorne, can potentially be used by hackers to spread malware and intercept data. This could occur without any user interaction or clicks and the flaws impacted all devices on Android, Windows, Linux and Apple iOS versions earlier than iOS10.

Unlike traditional cyber attacks the Bluetooth method does not require a victim to fall for a malware-ridden link or download a booby-trapped document. Instead it can take advantage of four critical zero-day bugs and spread 'over the air'.

These vulnerabilities are described by Armis as "the most serious Bluetooth vulnerabilities identified to date" and "can enable a complete takeover of the target device". If Bluetooth is enabled a hacker could connect to the device and force surrounding web-connected technology to become a carrier of the virus.

Yevgeny Dibrov, Chief Executive of Armis, stated on 12th. September 2017:

"These silent attacks are invisible to traditional security controls and procedures. Companies don't monitor these types of device-to-device connections in their environment so they can't see these attacks or stop them. Previously identified flaws in Bluetooth were primarily at the protocol level. These new vulnerabilities are at the implementation level, by-passing the various authentication mechanisms and enabling a complete takeover of the target device. The automatic connectivity of Bluetooth, combined with the fact that nearly all devices have Bluetooth enabled by default, makes these vulnerabilities all the more serious and pervasive."

The time taken to exploit a device is noted to be no more than ten seconds and the exploitation would work even if a device was already paired with another.

Mark James, an expert with cyber security firm ESET, an exhibitor at IP EXPO, commented as follows:

"In theory, to be safe on these devices, Bluetooth needs to be disabled until a patch is applied. If no patch is on the horizon then you should seriously consider replacing that device with one that is being patched or actively maintained. When exploits like these are found on technology that is integrated into almost every device we use it is a real concern."

Further information may be obtained from Mark James, IT Security Specialist, ESET UK, Sovereign House, 242 Charminster Road, Bournemouth, Dorset BH8 9RP. Telephone: 0845 838 0832. Email: Mark.james@eset.co.uk

ENHANCING THE SECURITY OF FIRMWARE

Hackers are continually seeking to find new ways of infiltrating critical infrastructure and increasingly this involves hacking the lowest level of a platform, the firmware, where threats are most difficult to detect.

In order to address this Intel has developed the Intel® Data Center Block for Business - PFR Server Block. This features Intel® Platform Firmware Resilience and enables platform security starting in the factory all the way through power-on, system boot, OS load and beyond. It aims to prevent firmware from being intercepted, detect firmware corruption, and automatically restore a system if malware is detected. This is described as 'an ideal solution for security-sensitive industries':

'The PFR Server Block is designed with security-sensitive customers in mind, featuring a 2U rack optimised system configuration that is loaded with security features for critical infrastructure, government and financial customers. To make server management easier this product includes utilities to simplify the provisioning of security features and securely update firmware components remotely across an entire rack. The system also includes a dedicated management port to enable secure, anywhere-access from any device.

The PFR Server Block supports three Intel Xeon processor E5-2600 family SKUs that have been enhanced to support the latest Intel Platform Firmware Resilience technology. These CPU SKUs anchor the root of trust at the lowest levels of the platform. Together with a security-specific ASIC and authentication code modules, Intel PFR guards the platform through a CPU directed secure boot mechanism to authenticate firmware and, if necessary, restore firmware images.'

More details may be obtained from ark.intel.com

NEXT GENERATION ENDPOINT PROTECTION

For about the last two decades hackers have been continually targeting the endpoint, and companies have been deploying large amounts of software to secure it, in the form of antivirus, anti-malware, desktop firewalls, intrusion detection, vulnerability management, web-filtering and anti-spam. Unfortunately, however, traditional security is not working with hackers increasingly using masking techniques to bypass the security software.

According to endpoint security specialists SentinelOne it is "very easy" to do this, requiring only basic coding skills, and in their report *'Next Generation Endpoint Protection'* a diagram is used to illustrate how attack masking techniques can be used in conjunction with each other to take a known binary and cause it to appear completely new, unknown and benign on the surface.

It is also explained how, along with masking techniques, hackers are also using different vectors or paths to deliver malicious code:

'Attacks can be single-vector or part of a multi-vector, more sophisticated attack.'

The report is particularly critical of antivirus software, noting that despite it having existed for a quarter of a century it still has not innovated to protect against attacks that use unknown threat techniques:

'It continues to look for a known hash, and small changes to the hash can bypass the system. Antivirus also overlooks the fact that attacks can be file-less, infecting the memory and writing directly to RAM rather than file systems. In addition, antivirus is not known to be user friendly, hogging bandwidth with updates and spiking CPU with resource intensive scans.'

Sandboxing, by contrast, began about five years ago, but this too has been found to be flawed:

'They, in essence, "emulate" the execution of unknown files inside a virtual machine residing on the network and monitor file behaviour throughout its execution inside the "protected" environment. While these solutions have been able to increase detection rates of new threats, they are far from being 100 per cent effective.

Attackers quickly realised while their current packing techniques could not be used to bypass the sandbox environment, they just needed to detect the environment, which could easily be done by noticing limited emulation time, lack of user interaction, and only a specific image of the OS. Once the environment is identified, they ensure their malicious code will not run in the emulated environment, will be flagged as benign, and will continue its route to the end device and only run there (where the endpoint antivirus can do little to stop it).'

With this backdrop SentinelOne argue that a completely new model with an entirely different approach is needed:

'Instead of looking for something known or its variant, like signature-based detection, next generation endpoint security is analysing file characteristics (to uncover known and unknown file-based malware) as well as the entire endpoint system behaviour to identify suspicious activity on execution. Endpoint detection and response (EDR) monitors for activity and enables administrators to take actions on incidents to prevent them from spreading throughout the organisation. Next-Generation Endpoint Protection (NGEP) goes a step further and takes automated actions to prevent and remediate attacks.'

The case is made for replacing antivirus with next generation endpoint security:

'To completely replace the protection capabilities of existing legacy, static-based endpoint protection technologies, NGEP needs to be able to stand on its own to secure endpoints against both legacy and advanced threats throughout various stages of the threat lifecycle - pre-execution, on-execution and post-execution.'

The solution uses the four core pillars of advanced malware detection, mitigation, remediation and forensics:

'During execution malware often creates, modifies or deletes system file and registry settings and changes configuration settings. These changes, or remnants that are left behind, can cause system malfunction or instability. NGEP must be able to restore an endpoint to its pre-malware, trusted state, while logging what changed and what was successfully remediated.

Since no security technology claims to be 100 per cent effective, the ability to provide real-time endpoint forensics and visibility is a must. Clear and timely visibility into malicious activity throughout an organisation allows you to quickly assess the scope of an attack and take appropriate responses. This requires a clear, real-time audit trail of what happened on an endpoint during an attack and the ability to search for indicators of compromise.

The SentinelOne Endpoint Protection Platform (EPP) offers organisations real-time unified endpoint protection that unifies prevention, detection, and response in one platform managed via a single console. SentinelOne EPP leverages advanced machine learning and intelligent automation to protect Windows, OSX, and Linux-based endpoint devices from threats across all major vectors: advanced malware (file and memory based), exploits and stealthy script-based attacks. It closely monitors every process and thread on the system, down to the kernel level.

A view of system-wide operations - system calls, network functions, I/O registry and more - as well as historical information, provides a full context view that distinguishes benign from malicious behaviour. Once a malicious pattern is identified and scored, it triggers an immediate set of responses ending the attack before it begins.'

Deep Visibility

The SentinelOne Endpoint Protection Platform is augmented with SentinelOne Deep Visibility to provide full visibility of endpoint data. This uses patented kernel-based monitoring to allow a near real-time search across endpoints for all indicators of compromise:

'Deep Visibility monitors traffic at the end of the tunnel, which allows an unprecedented tap into all traffic without the need to decrypt or interfere with the data transport layer. This allows the engine to stay hidden from attacker evasions while also minimising user experience impact.

Deep Visibility allows for full indicator of compromise search on all endpoint and network activities, and provides a rich environment for threat hunting that includes powerful filters as well as the ability to take containment actions.'

ADVANCES IN NETWORK TRAFFIC MANAGEMENT

BT and Dell EMC are collaborating on research dedicated to validating a new way of managing network traffic.

Their proof-of-concept, which is taking place at BT Labs in Adastal Park, near Ipswich, will explore how disaggregated switching can create flexible networks that are more responsive to customer needs.

In his article 'BT and Dell EMC to develop flexible SDNs of the Future' in the September 2017 issue of *Networking*, Rahiel Nadir states:

'Unlike traditional integrated network switches currently used by data centres, operators and enterprises around the world, disaggregated switching utilises merchant silicon-based systems combined with either commercially available or open source system software. According to the two partners this represents a "significant shift architecturally", applying server-like principles to the delivery of dynamic network services over fixed-line and wireless networks.'

Disaggregated switches are noted to have the advantage of being able to be managed flexibly using Netconf protocol and YANG models.

The article states:

'BT is evaluating the performance of Dell EMC's disaggregated switches against traditional integrated switching hardware to test the performance, economics and programmability of this new virtualised approach. The company says the trial will enable it to make informed decisions about the role this kind of solution will play in the dynamic network services of the future.

The two companies will evaluate a number of potential use cases as part of the trial. These include the instant activation of Ethernet circuits from a third party (such as an enterprise), and the ability of the system to deliver real-time network operational data.

The platform also offers the potential to deliver other programmable use cases such as bandwidth calendaring - flexing the bandwidth of an Ethernet circuit according to customer need via a predetermined calendar - and delivering network telemetry data to third parties automatically.'

DEW POINT COOLING SYSTEM FOR COMPUTING AND DATA CENTRES

The traditional vapour compression cooling systems used in computing and data centres is recognised as being neither energy efficient nor environmentally friendly. Other alternative cooling systems, such as adsorption, ejector and evaporative do offer some energy saving potential, but have inherent problems that have restricted their widespread application.

Now, an international team of researchers led by the University of Hull and supported by the DCA Data Centre Trade Association is working on a joint EU Horizon 2020 research and innovation programme to develop a design theory, computerised tool and technology prototypes utilising the dew point cooling principle that is widely used in other industrial fields.

In his article 'An energy efficient Dew Point Cooling System for Computing and Data Centres', Professor Xudong Zhao, Director of Research for the School of Engineering and Computer Science at Hull University, in *Digitalisation World* (September 2017) presents a diagram illustrating how the new system could function to deliver a 60 to 90 per cent energy saving.

The author states:

'During operation, a mixture of the return and fresh air will be pre-treated within the sorption bed (part of the sorption/desorption cycle), which will create a lower and stabilised humidity ratio in the air, thus increasing its cooling potential. This part of air will be delivered into the dew point air cooler. Within the cooler, part of the air will be cooled to a temperature approaching the dew point of its inlet state and delivered to the computing and data centre (CDC) spaces for indoor cooling. Meanwhile, the remainder air will receive the heat from the product air and absorb the evaporated moisture from the wet channel surfaces, thus becoming hot and saturated and being discharged to the atmosphere.

As the adsorbent regeneration process requires significant amounts of heat while the CDC data processing (or computing) equipment generates heat constantly, a micro-channels-loop-heat pipe (MCLHP) based CDC heat recovery system will be implemented. Within the system, the evaporation part of the MCLHP will be stuck to the enclosure of the data processing (or computing) equipment to absorb the heat dissipated from the equipment, while the absorbed heat will be released to a dedicated heat storage/exchanger via the condenser of the MCLHP.

The regeneration air will be directed through the heat storage/exchanger, taking away the heat and transferring the heat to the desorption bed for adsorbent regeneration, while the paraffin/expanded-graphite within the storage/exchanger will act as the heat balance element that stores or releases heat intermittently to match the heat required by the regeneration air.

The heat collected from the CDC equipment and (or) from solar radiation will be jointly or independently applied to the adsorbent regeneration, while the system operation will be managed by an internet-based intelligent monitoring and control system.

This super high performance has been validated by simulation and the prototype experiment carried out in Hull and other partners' laboratories. The coefficient of performance of the proposed dew point cooling system reaches as high as 37.4 in ideal weather conditions, while the average coefficient of performance of traditional cooling systems is around 3.0.'

ENGINEERING SIMULATION FOR THE DIGITAL AGE

This was the theme for a special event dubbed 'DC Day', hosted by Future Facilities at The Churchill War Rooms in London on the evening of 4th. October.

"The war on data centre cooling is hard, expensive and often an intuitive one", according to Future Facilities, whose objective is to ensure that software moves forward and meets the requirements of the data centre industry.

The audience was provided with a tour of the data centre lifecycle through the virtual facility, which sought to demonstrate how engineering simulation can enable an understanding of the consequences of change in a way that is both cheaper and faster than traditional prototyping.

Presenters Louise Hewitt, Business Development Manager , and Dave King, Product Development Manager, said:

"We can prototype generators and chillers, but it is hard to move them around. We can with simulation. The virtual facility presents something to your client that will really work. Building construction can be justified with simulation."

Future Facilities are therefore pioneering the use of simulation for this task and in the panel discussion that followed the data centre industry was likened to the aviation industry of the 1970s when redundancy was found not to solve technical problems. "Do what the airline industry did with flight simulation, simulating failures through software", the audience was advised.

Human error was noted to be rife in the data centre industry, with a mistake being made on average every four minutes, and questions from the floor included the issue of simulating control in order to avoid it. In particular it was recommended that rather than focusing on reducing errors to zero it is more important to look at preventing catastrophe.

There was a focus on building models "from the ground up" using the Future Facilities library as a starting point. "More assumptions mean more deviations from reality", the audience was told, and advice given to consider aspects such as cable routes that are often neglected.

Complementary to DC Day is the article 'Virtual Reality - are we on the Edge of a Data Centre Revolution?' by Future Facilities Product Manager Mark Fenton in *Digitalisation World* (September 2017), which introduces 'The Rift Experience', which uses a virtual reality headset to present a fully immersive data centre simulation.

According to Mr. Fenton there has been "a healthy level of scepticism and even trepidation towards the technology", but this "melts away" upon transportation to a rooftop chiller plant or back in time to an IBM mainframe facility. He says:

"This fully flexible experience may be the foundation of almost unlimited opportunities for our data centre ecosystem: designers walking clients around their concepts, colocation providers selling a proposed cage layout, upper management touring their investment, facility engineers troubleshooting their own sites. It is clear that virtual reality will not only change the way we visualise our data centres but, more excitingly, it will change the way we work with them as well.

For operational sites VR will naturally progress to AR (augmented reality) where performance data can be overlaid onto the real world. Imagine walking through your data centre, putting on your AR glasses and superimposing live DCIM data or simulation results directly onto your view. With human error causing the large percentage of data centre outages, AR could be invaluable in training and assisting site staff to ensure fewer mistakes are made.

When looking at cooling performance, site staff could visualise the airflow around overheating devices to fully understand the thermal environment - and then interactively make improvements. In addition, IT and Facilities could use this technology to proactively visualise their next deployments, a maintenance schedule or even a worst-case failure. VR offers a fully-immersed testbed, where you can experience first-hand the engineering impact of any data centre change you're planning to make."

Further information may be obtained from Future Facilities Limited, 1 Salamanca Street, London SE1 7HX. Telephone: 020 7840 9540. Email: info@futurefacilities.com

HELITECH AND MRO EUROPE 2017

These twin exhibitions ran in parallel with IP EXPO Europe and to conclude this issue of *The Electron* an overview of some of the recent electronics developments in the aviation sector is presented.

Next Generation Simulators for Helicopter Training

The article 'Next-Gen Sims' in *Vertical* (August/September 2017) by Howard Slutsken introduces Augmented Reality, Virtual Reality and Mixed Reality as "the shiny new toys appearing in many sectors" and suggests that they may soon become important tools for helicopter training also.

The article quotes Nacho Navacerrada, Business Manager for the Spanish simulator manufacturer Entrol as follows:

"We are considering AR goggles in the future as well as AR/VR systems together with current simulation. There are still many hurdles to solve, but we are confident this technology could be integrated with current simulation. AR technology is improving very quickly and it will be a game-changer that will open a lot of new possibilities for helicopter training.

We have seen significant improvements in image generators and databases. They are reaching the level of the gaming industry, there is plenty of satellite imagery and environments are more realistic than ever."

Airbus simulates future Air Traffic Management Systems

In *Air Transport World* (October 2017) the article 'Airspace Vision' by Graham Warwick explains how Airbus' Silicon Valley outpost A3 has launched a project to help fundamentally redefine air traffic management (ATM) to allow many different types of vehicles, including delivery drones and air taxis, to share airspace and enable new missions.

The project, called Altiscope, is a simulator for evaluating ATM policy options and operational models at a level that allows regulators, policymakers, operators, city planners and other interested parties to test different approaches and view the impacts.

The article states:

'In the future that Altiscope is being built to simulate there could be several hundred vehicles ranging from low-altitude delivery drones and urban air taxis to high-altitude remote sensing and communications relay aircraft flying in airspace above major cities.

Decisions such as how close vehicles can fly to buildings in urban environments can have unexpected effects on airspace capacity and mission capability, and Altiscope is designed to enable planners to evaluate the impacts and evolve the rules.'

First 4G LTE-based air-to-ground Network

SmartSky Networks have begun the process of deploying the first airborne 4G LTE-based air-to-ground network in the US. Using 60MHz of spectrum and patented beamforming technology, the network will provide over ten times the typical speed and capacity of the current industry standard ATG network and at a lower cost per bit.

The company's estimate for completing coverage to support the network's nationwide service launch has been updated to mid-2018, reflecting additional time being required for STC-related software optimisation and production of base station rules.

Data Analytics for Predictive Maintenance

Mario Pierobon in *MRO Management* (Vol. 19, Issue 3), September 2017, p.34-40, explains how the use of big data has matured to the point where analytical services are able to be offered for predictive maintenance.

Whilst the use of data analytics to predict and avoid unscheduled maintenance events and to improve the performance and design of aircraft is not new, the level of sophistication of the tools is. The result is that it is now possible to work on a near to or actual real-time basis.

Predictive Failure Analysis is one area where recent data analytics developments have had a particularly profound impact, and the article highlights, notably, SkyWise, a new system that collects data from across the systems in Airbus A320 family aircraft and, using the Rockwell Collins Flight Operations and Maintenance Exchanger (FOMAX) program, transmits the data to Airbus.

Jaime Baringo, Head of Digital Business Development at Airbus, is quoted as follows:

"Current Airbus predictive solutions in SkyWise provide high dependability on the prediction enough in advance, providing the airline with the ability to take timely and informed decisions. Also, when connected with other systems in the airline, they provide actionable items so that benefits can be scaled and made systematic after every flight. Legacy systems were looking at a reduced number of parameters and therefore had limited coverage across aircraft systems. Also, they were unable to systematically provide guidance without generating significant amounts of No Fault Found.

The power of the analytics contained in FOMAX-SkyWise allows airlines to identify predictive models which, combined with the OEM's expertise, can quickly make new models available and hence grow prediction coverage exponentially.

In Airbus we have also seen the value of combining this data with operations information so that we can improve and create new models that work faster and are more effective; this is now possible with SkyWise. With the expertise from our design office we are now able to propose predictive models that bring significant efficiencies with the aircraft as it is. On top of that, we are introducing FOMAX, that natively connects to our SkyWise platform, providing 20 times more data from sensors and systems that are not accessible otherwise. FOMAX is a minimal addition to the aircraft as it integrates seamlessly with existing avionics.

It has really taken off over the past year and we are adding new operators every month, now that they have heard from the proven field experience from the pioneering airlines. The users do not have to manipulate the data as it automatically flows to SkyWise where it is ingested and pre-processed. They simply log into SkyWise and get alerts on predicted failures for their fleet.

The experience from the field is amazing, with direct short-term results and proven savings as a result of the avoidance of operational interrupts, reduction of spares and overall decrease of maintenance cost. SkyWise also allows the airline to benefit from the collaborative intelligence and experience across the various operators in the platform while preserving their competitiveness."

Use of Drones to maintain Industrial Assets

Many major industrial companies are now moving towards robotic inspection services, combining their knowledge of infrastructure maintenance with drones, robots and artificial intelligence for automating the collection and analysis of data.

In *Inside MRO*, October 2017, official publication of MRO Europe, Graham Warwick (p.18) explains some of the recent developments in this area, beginning with Honeywell's new commercial inspection service that uses Intel's Falcon 8+ industrial drone. This is targeted at the utility, energy, infrastructure and oil and gas industries and the InView package includes the drone, pilot app and a web portal to help customers to create standardised routines and crisis-response inspections as well as providing data analytics.

The author then moves on to discuss Avitas Systems, launched by General Electric in June, which replaces time-based manual inspections of assets such as transmission towers and flare stacks with automated checks based on assessing the risk of defects developing.

The article states:

'Avitas Systems is offering inspection services to the oil and gas, energy and transportation industries. It uses drones, crawler robots and autonomous undersea vehicles to automate inspections.

Avitas Systems is using Nvidia's DGX computing systems to run the artificial intelligence (AI) algorithms it is developing for use in planning the inspection paths, processing the images collected, and for the data analytics involved in automatically detecting defects such as corrosion, hot or cold spots or microfractures.

Nvidia's DGX-1 supercomputing workstation is being used centrally for coding and training deep learning algorithms, such as convolutional neural networks for image classification and general adversarial neural networks for labelling captured images.

Additionally, Avitas Systems plans to deploy Nvidia's compact DGX Station supercomputing system locally with the robots to help recognise defects automatically at inspection sites.

Avitas Systems is using AI to plan flightpaths for drones that optimise the collection of data at points of interest on assets such as pipelines and refineries. AI is then used to layer the images collected on a 3D model of the asset and to perform automatic defect recognition.'

Israel leads the way in ISR Technologies

Israel's top technology companies are working with the Israeli Defence Ministry on a new class of intelligence, surveillance and reconnaissance (ISR) technologies. This includes, notably, the SkEye drone payload from Elbit Systems and Fast-scattered sensors.

David Eshel, in his article 'Fresh Eyes' in *Aviation Week* (October 2-15 2017), explains:

'Traditionally, UAVs for ISR missions carried payloads that were designed to display maximum details of the target. Therefore, coverage was restricted to a narrow field of view - an image taken through a "soda-straw" at specific targets of interest.

SkEye simultaneously captures and stores aerial views of a large area, generating a time-stamped, all-seeing gigapixel sized image. Analysts can view the area as live video or review past streams showing the same locations to explore variations, trends and patterns of life, or track back from locations of known events in a forensic study seeking to identify linked events, locations and perpetrators.

The Fast-scattered sensors system uses up to 1,000 miniature sensors that are dropped from the air, and as they hit the ground form a network that covers a designated area.'

Further developments include advanced technologies to perform surveillance in urban areas, where suspects avoid detection by immersing themselves in crowds. Advanced facial recognition algorithms capable of tracking subjects and recognising those attempting to avoid detection by wearing a hat or disguise are being developed.

Another development is that of a stabilised weapon for drones from Duke Robotics:

'The Tikad system won a US Defense Department innovation award in 2016 and is now open to crowd-funding investment. It uses a lightweight, stabilised weapon platform that moves accurately in six degrees of freedom and absorbs much of the firing recoil to enable precise shots. The system can mount assault rifles, hand guns, grenade launchers or light machine guns.'

Open Cosmos

In 'Space Oddity' (*Elite Business*, July 2017) Eric Johansson explains how nanosatellites with a payload of up to 20kg can now be launched at a fraction of the cost and time of conventional options:

'While it could traditionally take up to around four years and cost roughly £5 million to get a small satellite into orbit, Open Cosmos offers a one-stop solution that slashes both the time and the price. The cost for a three-unit nanosatellite mission starts at £500,000 and the timescale from planning to launch is less than a year.

The company is able to achieve this by doing everything from mission simulations to spacecraft designs in-house. By owning all the technology, and standardising interfaces, it is able to simplify the mission, removing handcrafted and costly elements.'

Mr. Johansson quotes CEO and Founder of Open Cosmos, Rafael Jorda Siquier, as follows:

"We are entering a new age of space heralded by the miniaturisation and commercialisation of electronics. Formerly, testing in orbit meant bespoke, bulky and costly satellite platforms. That's no longer the case and the UK is leading the way in unlocking space for the masses."