ELSEVIER

network SECURITY

ISSN 1353-4858 March 2015

www.networksecuritynewsletter.com

Featured in this issue:

How secure is your building?

So-called smart buildings make use of networked technology to connect a broad range of systems to central management consoles for more efficient operation.

This use of networked technology has advantages for security as well, enabling feeds from security controls to be fed into the central management system so that anomalies in traffic flows can be seen and remedial action taken in an efficient, automated manner, as Colin Tankard of Digital Pathways explains.

Full story on page 5…

The evolution of security intelligence

Threat landscapes have drastically changed from just a few years ago, with targeted attacks now common occurrences. As a result, many of today's businesses have found themselves on the back foot.

Security intelligence offerings combining both Security Intelligence and Event Management (SIEM) solutions and 'big data for security' implementations are key tools for offsetting threats that result from both increased hacking, and vulnerabilities resulting from insider compromises, explains Sol Cates of Vormetric.

Full story on page 8…

Should the dark net be taken out?

Cybercrime in general appears to be on the rise, but despite the apparent success of the Operation Onymous sting at the end of 2014, law enforcement agencies still face problems when going after hidden websites on the dark net.

There are no international cyber-security laws, even though cybercrime tends to be global in nature. And the dark net is employed for both good and bad by criminals, journalists and political dissidents alike. So the big question in both ethical and privacy terms is would it really make sense to try and shut it down? Cath Everett finds out.

Full story on page 10…

More Snowden leaks reveal hacking by NSA and GCHQ against communications firm

Yet another batch of documents from the Edward Snowden leaks reveal that the US National Security Agency (NSA) and its UK counterpart, GCHQ, hacked Gemalto, a firm that specialises in security and communications products, including SIM cards for mobile phones.

What they were after were the private encryption keys to SIM cards, access to which would allow the agencies to eavesdrop – potentially on millions of people. Gemalto is headquartered in the Netherlands, but the attacks took place around the world.

The slides, published by The Intercept (http://bit.ly/1CZ1JLx), revealed the existence of a Mobile Handset Exploitation Team (MHET) and its operation Dapino Gamma. This targeted

Continued on page 2…

Contents

NEWS

FEATURES

REGULARS

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Tel: +44 1865 843239
Web: www.networksecuritynewsletter.com

Publishing Director: Deborah Logan

Editor: Steve Mansfield-Devine
E-mail: smd@contrarisk.com

Senior Editor: Sarah Gordon

Production Support Manager: Lin Lucas
E-mail: l.lucas@elsevier.com

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1351 for all European countries & Iran
US$1512 for all countries except Europe and Japan
¥179 300 for Japan
(Prices valid until 31 December 2015)
Subscriptions run for 12 months, from the date payment is received.
More information:
http://store.elsevier.com/product.jsp?isbn=13534858

12987

Pre-press/Printed by
Mayfield Press (Oxford) Limited

…Continued from front page

Gemalto which produces around two billion SIM cards a year for around 450 mobile network operators. One slide boasted that the agencies believed "we have their entire network". The object of the attack was the 128-bit Ki encryption key contained in every SIM card, which encrypts calls. Because the key is hard-coded there is no forward secrecy so, once it is obtained, calls recorded previously can be cracked.

"Getting compromised by a targeted GCHQ/NSA operation isn't negligent, but underestimating the implications of it is"

The 2010 document leaked by Snowden suggests that the agencies' hacking activities were very successful. In one three-month period alone (Dec 2009 to Mar 2010) the agencies obtained over 106,000 keys linked to identified SIM cards, and the document suggested stepping up operations.

Gemalto was very quick – some people think too quick – to give assurances and play down the attack. Just six days after the incident became public knowledge, the firm issued a statement saying that "an operation by NSA and GCHQ probably happened" but that, "the attacks against Gemalto only breached its office networks and could not have resulted in a massive theft of SIM encryption keys". This, of course, ran counter to the NSA's and GCHQ's own (secret) claims.

Many security specialists were surprised at Gemalto's assurances after such a short time, as such investigations usually take months and the attacks claimed by the NSA took place in a large proportion of the 85 countries in which Gemalto operates.

"Gemalto is surprisingly confident that it now knows exactly the scope of the GCHQ/NSA penetration that it didn't detect in the first place," tweeted Matt Blaze, associate professor of computer and information science at the University of Pennsylvania. "Getting compromised by a targeted GCHQ/NSA operation isn't negligent, but underestimating the implications of it is."

It's also notable that this investigation has taken place years after the infiltrations into the firm's networks occurred – and these were hacking activities by highly sophisticated attackers that might be expected to leave no trace. Some commentators suggested that Gemalto might be attempting to steady the nerves of its investors. The firm also has contracts with a number of government customers.

Although there have been some protests, the reaction has been largely muted given that these were attacks by Western nations against a private organisation going about its lawful business.

NSA also targets hard drives

Kaspersky Labs has released details of research that suggests the NSA has been planting spyware into hard disk firmware for at least the past 14 years.

More than a dozen top brands – including Seagate, Western Digital, IBM, Toshiba, Samsung and Maxtor – have been implicated. Reuters later said its sources, including ex-NSA employees, confirmed the story.

According to Kaspersky, the malware – known as nls_933w.dll – was the product of The Equation Group, operating within the NSA, which had access to the firmware source code. These activities are believed to have targeted tens of thousands of Windows computers being used by telecommunications providers, governments, militaries, utilities and mass media organisations in more than 30 countries.

There is evidence that the Equation Group cooperated with those responsible for the Stuxnet and Flame trojans. Kaspersky discovered the firmware infections because a handful of the hundreds of domain names used by the Equation Group had been allowed to lapse. Kaspersky bought the names and used them to create a sinkhole, so that infected machines started to contact the firm's servers. There is more information available here: http://bit.ly/1E2xqPr.

In brief

Freak flaw found in OpenSSL…

Yet another vulnerability has been found in SSL encryption technologies. Dubbed 'Freak', it was at first thought to affect only Apple (iOS and OS X) and Android platforms, but Microsoft later announced it is also found in all versions of Windows. An attacker with access to the same network as a victim is able to cripple the encryption used by OpenSSL and Apple's SecureTransport (which is based on OpenSSL), forcing apps to use weak encryption keys by falling back to older, less secure protocols. There's an analysis of the attack here: http://bit.ly/1EQrP2r and at freakattack.com, which has a utility to allow you to check if your system is vulnerable. At the time of writing, OpenSSL and Apple had released patches and Microsoft had offered a work-around pending a full patch, although many Android users may find it difficult to upgrade due to the fragmented nature of the platform. However, most security analysts are rating the severity of the flaw as fairly low due to the need for an attacker to share a network with the victim.

…and OpenSSL announces audit

As an open source project, OpenSSL has supposedly benefitted from the 'many eyes' approach which posits that the openness of the code helps eradicate flaws. But as the Freak and Heartbleed flaws have shown, this process isn't perfect. Consequently, the Linux Foundation's Core Infrastructure Initiative is providing $1.2m in funds to allow OpenSSL to undertake a formal security audit of its code. Organised by the Open Crypto Audit Project, the audit will start with TLS stacks, examining protocol flow, state transitions, high-profile cryptographic algorithms and memory management. The first results are expected in July. This is the first move by the Core Infrastructure Initiative, which is funded by Amazon, Google, Microsoft, Cisco and Facebook, each of which has pledged $100,000 a year for three years.

Tor ban 'not acceptable'

In spite of UK Prime Minister David Cameron's desire to see encryption facilities be denied to ordinary people, a new Parliamentary report says that banning anonymity services, such as Tor, would not be an "acceptable policy option". It cites the technical challenges of imposing such a ban, as well as the usefulness of such networks to law enforcement operations. The Parliamentary Office of Science and Technology (POST) is an independent Parliamentary group that provides technical analysis on public policy issues. Its recent POSTnote looked at issues relating to the dark net, including the use of Tor and other anonymising networks such as I2P and Freenet. It points out that such systems are often used for positive purposes – for example, child protection service Internet Watch Foundation frequently uses Tor to detect and remove indecent material. There is more information here: http://bit.ly/1BnzWlU.

Dating apps vulnerable to hacking

Research by IBM concludes that more than 60% of dating apps are vulnerable to abuse by hackers, putting (very) personal information at risk. In addition to the sort of information you'd expect such apps to store, many of them also access data on the mobile device, such as GPS location and mobile wallet billing information. In addition, they often demand access to the device's camera, microphone and storage. And in more than 50% of cases, IBM found that the same device was being used to store corporate data belonging to the owner's employer. Among the vulnerabilities found were cross-site scripting flaws, the debug flag being enabled, a weak random number generator and issues that could lead to phishing via man in the middle attacks, such as cookie hijacking. The report is available here: www.securityintelligence.com/datingapps.

Ramnit shut down

The Ramnit botnet, favoured by criminals engaging in various forms of financial fraud, has been shut down by a combined operation led by Europol's European Cybercrime Centre (EC3) and supported by the UK's National Crime Agency. Microsoft, AnubisNetworks and Symantec also cooperated in the operation to close down the botnet's command and control structure, with traffic from 300 domains previously under the control of the criminals being redirected to servers operated by the authorities. According to EC3, more than 3.2 million PCs have been infected by Ramnit, which was used for spam campaigns, phishing attacks and drive-by infections. More information is available here: http://bit.ly/1FGgMaI.

Anthem refuses audit

US health insurance firm Anthem, which recently had as many as 78.8 million customer records compromised in a data breach, has refused an audit of its systems by the Office of Personnel Management's Office of Inspector General (OIG). The Office of Personnel Management regular carries out vulnerability scans and configuration compliance tests of systems providing benefits to federal employees. It contacted Anthem to offer a "partial audit" – something it also suggested back in 2013 and which was refused then too. Anthem's only response was to turn down the offer on the basis of "corporate policy". As many as 18.8 million non-Anthem customers may also have been affected by the breach. These are Blue Shield Blue Cross (BSBC) customers whose details were kept in the compromised database. That's because Anthem is part of a network of independent BCBS plans, and people who used their insurance plans in states such as Texas or Florida, where Anthem operates, may have had their details added to the database.

Billions of Android apps at risk

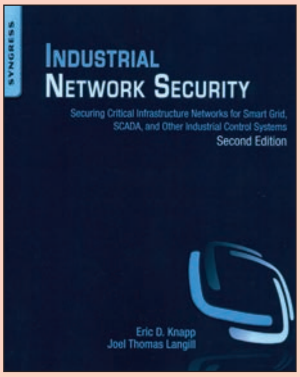
An analysis of seven million mobile apps on Android and iOS platforms by security firm FireEye has found that 31% of them contained a common vulnerability. Of those, 18% were in categories with potentially sensitive data, including finance, medical, communication, shopping, health and productivity. Additional research conducted in the second half of 2013 found a 500% increase in the number of Android apps designed to steal financial data. The report also identifies a new delivery channel for iOS malware that bypasses the Apple App Store review process. Attackers can take advantage of enterprise or ad hoc provisioning to deliver malicious apps to end users, either through USB connections or over the air. FireEye researchers found more than 1,400 iOS apps publicly available on the Internet introducing variants of security issues, signed and distributed using enterprise provisioning profiles. The report is available here: http://bit.ly/1xaShgR.

Million dollar data

Almost half of the UK population would not sell their online data for less than £1m, according to a new privacy study by Swiss datacentre firm Artmotion. However, many people are failing to take even the most basic steps to secure their information. The report was commissioned to see how attitudes have changed in the light of high-profile privacy breaches such as the Edward Snowden revelations, the regular attacks by hacktivist group Anonymous and the iCloud hack of embarrassing photos of celebrities such as Jennifer Lawrence and Kirsten Dunst. In addition to the 49% who would want at least $1m for their data, a further 10% said they would be willing to sell their personal or company data for £100,000-£1m, 10% said up to £100,000, 13% said up to £10,000, 3% said up to £1,000, 6% said up to £500, and the remaining 9% said they would give away their data for free. The study is here: http://bit.ly/199hVgW.

Reviews

BOOK REVIEW



Industrial Network Security
Eric Knapp, Joel Langill.
Published by Syngress.
ISBN: 9780124201149.
Price: €50.05, 460pgs, paperback.
E-book version also available.

The second edition of this work seems to be much-needed. Vulnerabilities in industrial control systems show no signs of abating – in fact, we're hearing about what seems an ever-increasing number of exploits and flaws.

Much of the problem seems to stem from the age of many of these solutions. Many Supervisory Control and Data Acquisition (SCADA) implementations and other industrial control systems were designed and installed before there was ever any thought of connecting them to the Internet. Those connections have been made since, but usually with little thought to security. There seems to have been a widespread belief in 'security through obscurity', with the safety of the systems dependent on people not knowing they existed, or the architectures being so arcane as to defy hacking. That hasn't worked out so well.

Smart grids are a different matter. This is modern technology that has been enabled by the Internet. And yet, once again, security considerations often seem to have taken a back seat.

The protection of critical infrastructure is finally getting the notice it deserves. Perhaps, in some ironic way, Stuxnet may have played a part in that. Although launched by what would normally be considered 'trustworthy' nation states (ie, the US and possibly Israel), rather than the kind of actors that would commonly attract the adjective 'rogue', the Stuxnet attack on Iran did at least show for certain that attacks against critical infrastructure are not just possible, but being executed now.

Indeed, one of the features of this new edition is the use of a larger number of examples of real-world attacks against control systems. It also has expanded coverage of protocols such as 61850, Ethernet/IP, CIP, ISA-99 and the move towards IEC62443, more pages devoted to smart grid security, and new coverage of signature-based detection, exploit-based versus vulnerability-based detection, and signature reverse engineering.

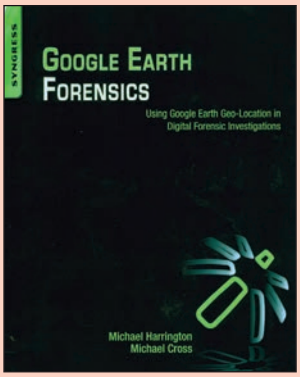
The book is littered with references to standards, and the area of industrial control systems has many of them. But as the authors point out, actually applying them to real-world systems and practices is the tricky bit. In some ways this is explained by the somewhat polarised audience that the authors had in mind when they wrote the book. On one side are engineers with a firm grip on fieldbus protocols; and on the other are network specialists most comfortable with IP protocols and Ethernet. The increasing encroachment of the latter on the former is a sign of the ubiquity of IP systems. But this doesn't give networking specialists an easy ride. They need to understand the demands of industrial control systems – most notably, the need for efficiency, which is something often sacrificed when dealing with everyday information security.

There's a lot in here, then, that deals with the intricacies of the plethora of protocols. But it is neither academic nor abstracted in tone. The book is focused on implementing, monitoring and testing security, and serves pretty well as a manual for those tasked with the job.

There's more information available here: http://bit.ly/1KVeZoW.

– *SM*-D

BOOK REVIEW



Google Earth Forensics
Michael Harrington, Michael Cross.
Published by Syngress.
ISBN: 9780128002162.
Price: €28.95, 122pgs, paperback.

In forensic investigations, knowing where a computer or device has been is becoming increasingly important. We live in an age of highly mobile computing, with powerful devices small enough to put in our pockets. Knowing the exact location of a device when it performed certain actions is a critical part of the forensic picture.

Fortunately, we also live in an age of APIs. Google Earth has worked its way into all kinds of applications, not least thanks to Google's openness with protocols and access to the data.

We've seen from a number of experiments and apps (such as Creepy) how many devices store location data as a matter of course – even, sometimes, when the user has asked it not to. In some cases, it's possible to chart a user's movements for a considerable period – just as if they had been fitted with a tracking device. This information might be stored on a phone, or embedded as metadata in other data, such as photographs.

The data by itself, however, may not mean much. It needs to be translated into a meaningful form. Yes, you could laboriously look up latitude and longitude coordinates on a map, but why bother when you could automate the process with Google Earth? Not only does this afford a rapid and easy way to understand the significance of the information, it's also an invaluable tool when presenting the evidence.

In this small but perfectly formed volume, the authors give you an insight into what Google Earth is, how it works and how to use it to best advantage. There's also a brief introduction to computer forensics and how a case is constructed. Some of this will be, perhaps, a little basic for some people who come to this book, who will be forensic practitioners looking to add another weapon to their armoury. But even here, the emphasis is on how Google Earth fits into the forensic investigation picture.

Some of the technicalities, such as XML and KML, are explained in detail, although perhaps it would have been good to see some detailed explanation of how you could automate some of the work with, for example, Python scripts. Overall, though, the authors have done a good job in showing how Google Earth can become an invaluable tool for forensic investigators.

There's more information available here: http://bit.ly/1xcs3dU.

– *SM-D*

How secure is your building?

Colin Tankard, Digital Pathways

Colin Tankard

Buildings today often incorporate the use of a building automation system, which provides automated centralised control of systems such as heating, ventilation, air conditioning and lighting. Buildings that employ such systems are often referred to as smart buildings. According to AutomatedBuildings, a smart building is defined as one that incorporates "the use of networked technology, embedded within architecture to monitor and control elements of the architecture for exchange of information between users, systems and buildings."[1]

One survey from MarketsandMarkets forecasts that the market for smart buildings will grow from more than $4bn in 2013 to reach almost $19bn in 2018, the largest share of which will be commercial buildings.[2] The development of smart buildings is part of the fast-growing vision of the Internet of Things, in which all sorts of devices will increasingly be connected over IT-based networks, many of which will come into use in commercial buildings, offering smarter and more efficient data management to drive efficiencies. Gartner predicts that 26 billion devices will be connected and online by 2020.[3]

According to Memoori, the value of the Internet of Things in terms of buildings is as much about data as devices, as collecting data from more services and equipment will provide a more granular view of overall performance.[4] For greater operational efficiency, such systems will increasingly collect, store and analyse data in the cloud.

Smart buildings and security

Commercial buildings and facilities face a range of security threats, including those from terrorist issues, disgruntled employees, workplace violence and criminal groups as well as from geopolitical actions such as riots and political unrest and natural disasters. There are also a number of other factors impacting building security that represent significant challenges. These stem from the nature of many commercial buildings, especially large complexes and high-rise buildings in dense urban environments that often are rented out to multiple companies. Security in such environments is complicated by the relative anonymity of users and occupants. This can lead to a poor security culture and result in interlopers going unnoticed and restricted movement in terms of elevators and lobby areas that can hinder guarding and emergency teams. The fact that services such as utilities tend to be grouped together into one service core, to make them easier to manage, can also make them easier to target.

> ***"The largest application group within the smart building sector is for security, which will account for 47% of revenues by 2020, with controls such as alarms, CCTVs and access control systems becoming increasingly connected"***

Because of factors such as these, monitoring systems are in widespread use in a range of facilities that include office buildings and complexes, industrial facilities and campus environments. Capabilities that they offer cover a wide range of physical scenarios, including perimeter protection, video surveillance,

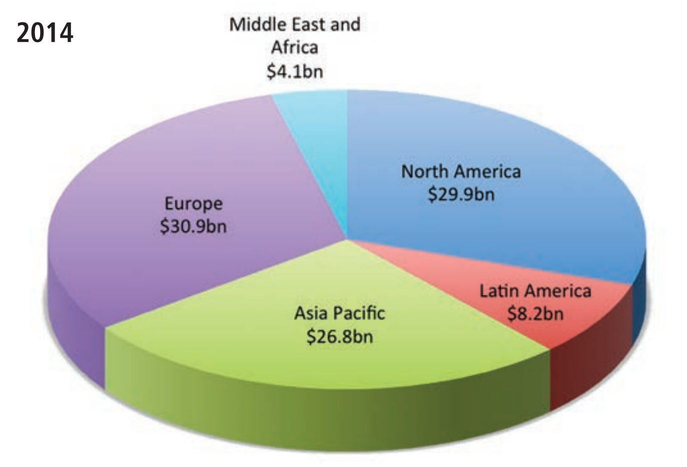


Figure 1: Market for the Internet of Things in buildings according to region, 2014. Source: Memoori.

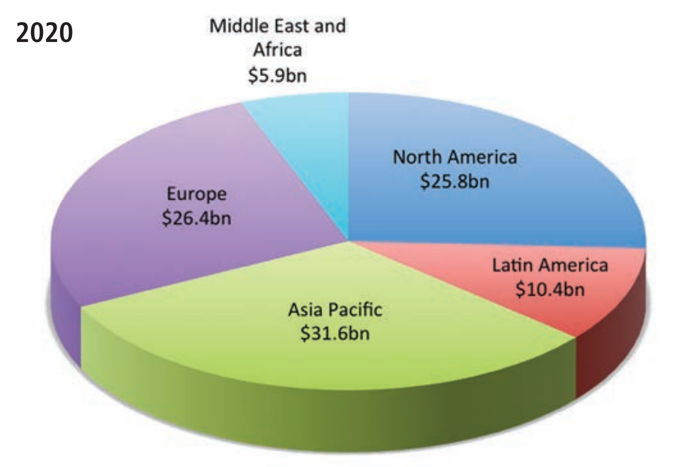


Figure 2: Market for the Internet of Things in buildings according to region, 2020. Source: Memoori.

Minimum building security

Building security measures should seek to provide:

- A consistent, compliant and auditable approach.
- Paperless environment.
- A strong secure perimeter with a limited number of access points into the building.
- Controlled access of all people and vehicles onto sites – maximising the benefits achievable from access control systems.
- Heightened security measures for areas containing particularly sensitive items and/or key operational equipment, documents, records etc.
- An intruder alarm system to support the physical security arrangements employed, supplemented, as appropriate, by CCTV cameras etc.
- Trained, knowledgeable security personnel where guarding needs to be deployed.
- Training of/communication with all building occupants and visitors to make them aware of security issues and the procedures that they are required to follow.
- Contingency plans and procedures in the event of security alerts and emergencies.
- Consistent and timely response from internal or external resources.
- Solid liaison and networking with appropriate external bodies, including police, fire service, ambulance service, local authority, utility providers and communication providers.

Source: 'Building security standards'. BBC, myRisks information. Accessed Mar 2015. www.bbc.co.uk/safety/security/buildingsecurity/buildings-security-standards.html.

employee and visitor screening and access control, and emergency response, including evacuation.

As smart building technology has advanced, such systems are increasingly being ported over from analogue to digital IP-based controls that offer expanded functionality and improved connectivity, including integration with mobile technologies. However, the expanded functionality that is offered has major implications for operational security since expanded connectivity heightens vulnerabilities to cyberattacks affecting networks.

According to Machina Research, the largest application group within the smart building sector is for security, which will account for 47% of revenues by 2020, with controls such as alarms, CCTVs and access control systems becoming increasingly connected. One of the main trends that will be seen is increased mobile connectivity.[5]

Effective controls

As buildings become more connected, one of the main challenges is managing the flow of data so that the current security environment can be understood and incidents can be responded to in an efficient manner based on gaining actionable intelligence from the data. This requires the use of a technology system that can collect, analyse and provide visibility into all information flows. This allows you to look for anomalies that could be indicative of a security risk, incident or vulnerability so that corrective action can be taken according to the incident response plan that has been developed in order to safeguard systems and applications.

For building controls, it is essential that security incident, logs and events are collected from both IT controls and physical security systems, such as logical and physical access control events, in order to give an overall picture of the environment and to provide visibility over what is happening in the network and in terms of physical monitoring measures.

For data protection purposes, all logs and events should be encrypted both in transit through the network and communications mechanisms, as well as in storage, where they should be held in a repository that is tamperproof and that is robustly protected with adequate access controls and granular, but not excessive, entitlements.

> ***"All logs and events should be encrypted both in transit through the network and communications mechanisms, as well as in storage, where they should be held in a repository that is tamperproof and that is robustly protected"***

Such a system must provide a central secure online environment that offers proactive task assignment and management for improving process flows, as well as providing a comprehensive audit and reporting facility. The audit trail is based on all events that have been tracked from multiple systems and should indicate what actions have been taken in response to every incident encountered. It also needs reporting capabilities that indicate the effectiveness of the measures that have been taken. This is also useful for governance purposes, such as alerting when security patches have not been applied in a timely manner so that remedial action can be taken.

Immediate action

So that senior executives can act on the information, reports should be provided as a dashboard, with information portrayed visually. This will allow those executives to analyse information and to pose questions to those in the organisation who can help lead to an overall improvement in security. It can also lead to more effective, granular policies being set, as well as achieving an easy to digest view of overall security, which is vital for effective governance, and for understanding the full range of threats faced and the effectiveness of incident response actions. Visualisation will also provide a spatial awareness of events, such as those surrounding the building as they unfold. Using such technology, it is possible to plot an incident on a map and apply additional information such as that available through Google Street View for a more visual description of the area. This provides a vital tool for remotely managing such an incident.

The central management system should also provide a facility for storing key documents or images relating to building protection that can aid in incident response, such as floor plans and standard operations procedures. This is also the place where best practices and procedures can be filed so that those in charge of responding to a particular incident can quickly find information that is relevant to dealing with, and recovering from, specific types of incident that could occur. And it is also where incident response plans such as fire and evacuation planning and incident management procedures and contacts should be stored. Currently, such information is typically lost in a cabinet on an inaccessible floor!

> ***"Policies are only effective if all to whom they apply are aware of their responsibilities, understand what is expected of them and are made accountable for their actions"***

The interface into the central management system should be web-based so that information is available over a browser interface and can be accessed from any Internet-enabled device, including smartphones and tablets.

By providing safe and secure interfaces to mobile devices or web browsers, remote access capabilities can be provided so that security operators can configure and control the system from wherever they are, and even out of hours. To gain full benefits, all components should be web-enabled, including the control panel, access control mechanisms and all monitoring capabilities. All endpoints that are external devices and are digitally controlled such as sensors, cameras, access control mechanisms, door and window locks should be included in the continuous monitoring process.

The central console provided by the security management system provides a policy enforcement point. Policies should be developed that cover every possible security scenario, based on detailed risk assessments that take into account the specifics of each building, its location, level of occupancy and type of business conducted on the premises. In developing risk assessments, it is important to take into account health and safety legislation compliance, which tends to vary from country to country. Policies are only effective if all to whom they apply are aware of their responsibilities, understand what is expected of them and are made accountable for their actions. Therefore, communicating with and training staff about the provisions of policies is essential.

Benefits

One of the benefits of using an IP-based security system is that a wide range of communications is supported, including call routing and mobile support, providing access to security-related information in a fast and efficient manner, making incident response quicker and more effective. Other communication methods can also be supported, including instant messaging and email for when information needs to be sent as text, such as sending floor plans to an onsite responder. These methods can also be used to send around mass notifications to all occupants or groups within a building – for example, to provide them with instructions or to send around warnings such as when a storm is approaching.

Overall, a security management system like this will improve the efficiency of building services and guarding teams by mitigating the risks that are faced and by providing for more effective and efficient remediation of incidents that occur.

Conclusions

A security management system for smart buildings will provide the underpinning for resilience in building management and critical systems, both for single or multiple buildings such as in a campus environment. For maximum effectiveness, it should cover all areas of risk that have been defined and should include mitigation strategies and automation for all security concerns identified. To suit the needs of particular buildings and facilities, the system should provide a choice of integrated applications and components to give facilities managers' maximum flexibility in terms of risk mitigation and management. This will also avoid having to invest in components that are not required in a particular situation, providing for maximum return on investment.

By choosing a system that is IP-based, it can be more flexibly deployed and

Applications and information made available through the central console

The central console of a security management system should provide:

- Incident & crisis management log records and reporting tools.
- Audit records and reports.
- Standard operating procedures.
- Contact book.
- Technical security countermeasures, including alerts and real-time change processes and workflow.
- Business continuity plans.
- Health and safety records.
- Investigations support.
- Risk assessments.
- Floor plans.
- Best practices and procedures for bomb threats and suicide bombers, hostile reconnaissance, lift entrapment, suspect packages, protest/occupation/civil unrest, lost/stolen/found property, workplace violence, active shooter, datacentre security, critical alarms, mail room procedures, CBRN (chemical, biological, radiological and nuclear warfare)/HAZMAT (hazardous materials and items) and domestic extremism.

Source: Global Aware International, www.globalaware.co.uk.

Key benefits

The main benefits of an integrated security management system include:

- Operational excellence model.
- Risk and gap analysis.
- Real-time audit and process flow.
- Paperless and prompt decision-making.
- Accountable actions.
- Real-time change management.
- Improved productivity resulting in commercial advantage.

Source: Global Aware International.

reduces the need for deploying physical communication interfaces such as cabling that are limited in their range. With an IP-based system, controls such as wireless intrusion detection units can be placed on each floor, connected via Ethernet or wireless, reducing the cost involved in implementing physical connections and improving overall security by being able to centrally control all devices.

As well as providing benefits for facility managers, a web-based security management system will improve the perception of security among occupants, making them feel safer, thus making prospective tenants more likely to be interested in taking space in the building. However, in order for this sense of security to be felt, all occupants should be made aware of the protection measures that are being taken so that they buy into the schemes and can achieve peace of mind.

About the author

Colin Tankard is managing director of data security company Digital Pathways (http://digpath.co.uk), specialists in the design, implementation and management of systems that ensure the security of all data whether at rest within the network, on a mobile device, in storage or data in transit across public or private networks.

References

1. AutomatedBuildings.com, home page. Accessed Mar 2015. www.automatedbuildings.com.
2. ‘Smart building market, worldwide forecasts and analysis (2013-2018)’. MarketsAndMarkets, Aug 2013. Accessed Mar 2015. www.marketsandmarkets.com/Market-Reports/smart-building-market-1169.html.
3. ‘Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020’. Gartner, 12 Dec 2013. Accessed Mar 2015. www.gartner.com/newsroom/id/2636073.
4. Memoori, smart building research, home page. Accessed Mar 2015. www.memoori.com.
5. ‘Growth in the intelligent buildings M2M sector will be driven by building security and demands for energy efficiency’. Machina Research, 31 Dec 2015. Accessed Mar 2015. https://machinaresearch.com/news/press-release-growth-in-the-intelligent-buildings-m2m-sector-will-be-driven-by-building-security-and-demands-for-energy-efficiency/.

The evolution of security intelligence

Sol Cates, Vormetric

Sol Cates

Threat landscapes have drastically changed from just a few years ago with targeted attacks now common occurrences. Hackers are actively seeking to steal credit card data, personally identifiable information (PII), critical intellectual property (IP), and other legally protected information to retail to the highest bidder. As a result, many of today’s businesses have found themselves on the back foot.

Furthermore, nation state-motivated attacks on both business and government entities are escalating, with critical intellectual property in the form of plans, formulas, production methods and the reputation of national institutions the primary target.

Expanding the periphery

At the same time, organisations are expanding their periphery beyond the traditional enterprise WAN and firewall – SaaS applications now account for over 50% of IT application spending, according to Gartner, and spending increases by both government and commercial enterprises of all cloud resources is forecast to nearly double by 2018. Mobile usage of enterprise data is also expanding, and a key concern for many organisations. Not to mention the avalanche of data starting to flow form the Internet of things (IoT) as new devices like cameras, refrigerators, home security systems, automobile sensors, power grid data and extended location information connect up to the Internet.

This expansion in the use of new technologies, combined with the increased threat environment as ‘dark’ sites expand to support a new international criminal class, is driving the need for tools that can sift through data to intelligently and proactively identify threats in process before they compromise organisations.

Representative of what is turning into a multi-billion dollar industry, organised criminal gangs are putting much more time, energy and resources into identifying or buying new methods of attack that can't be detected by traditional security solutions – so-called zero-day exploits. Indeed, once social engineering and spear-phishing campaigns penetrate an organisation, criminals then leverage these zero-day exploits to establish a beachhead, and begin mining private data and critical IP.

"The data produced by unauthorised access attempts can be monitored and used to investigate possible threats. In doing so, enterprises can 'watch the watcher' and make sure that security and administrative accounts are not compromised"

We only need to look to stories like those contained in the Mandiant report on 'APT18', a hacking group affiliated to the Chinese government, and 'APT28', a group engaged in espionage against political and military targets in Eastern Europe, to know that hackers can keep their data mining operations working undetected for a long time. APT18, for one, is charged with being responsible for a campaign targeting the data of Community Health Systems, a Tennessee-based hospital chain, for at least five years. In August 2014, the hospital announced that 4.5 million patient records had been affected during that period. The days of relying on a firewall and IDS/IPS or making sure that appropriate anti-virus was in place are long gone.

Security intelligence tools including both Security Intelligence and Event Management (SIEM) solutions and 'big data for security' implementations are key tools for offsetting threats that result from both increased hacking, and threats resulting from insider compromises. These tools allow the flow of data to be exploited to detect patterns of usage and access that would not otherwise be available. SIEM solutions monitor both real-time events and a mountain of long-term data to find anomalous patterns of usage, qualify possible threats to reduce false positives, and alert organisations when needed. However, a SIEM solution can be blind to possible threats to your protected data.

Current role

Pairing a SIEM solution with a data-centric security solution that delivers data access enforcement is essential to protecting data to the highest degree. While enforcing encryption rules and data access controls in all these environments, data security agents typically collect and log information on file access by users and processes, as well as details on the use of the infrastructure that protects them. This detailed information, in the form of RFC5424 or CEF logs, represents essential data that can be analysed using a SIEM solution's security intelligence capabilities to identify usage patterns that may represent a threat.

Patterns of abnormal activity indicating that a user or process has been compromised can be found much faster with this approach. Take, for example, an administrative account that suddenly begins accessing volumes of data; this may be indicative of a compromised user. Equally, these same activity pattern recognition tools that will identify a compromised user could also indicate an insider with a grudge, or who has decided to profit from their position.

In the context of the data breaches we are seeing, the overarching benefit of this approach is that unusual or improper data access is tracked and reported on, accelerating the detection of insider and outsider threats that have bypassed perimeter security. Furthermore, beyond abnormal activity recognition, such audit capabilities provide visibility into the types of files accessed by any given user at any given time. And the data produced by unauthorised access attempts can be monitored and used to investigate possible threats. In doing so, enterprises can 'watch the watcher' and make sure that security and administrative accounts are not compromised. This unprecedented insight into file activities can in turn be invaluable in aiding the investigation of someone who is under suspicion.

Security intelligence and big data

We know that deployments based on 'big data' collection and manipulation are now becoming a reality, which is increasing both the potential attack surface and adding another tool for analysing and protecting sensitive data. Conventional big data implementations are used by organisations like retailers to profile customer behaviour, power companies to analyse usage patterns, mobile application developers to capture consumer behaviour and so on. But there is a second important use case – and that is for analysis of security related data.

"It's quite likely that we'll see movement toward service providers – both cloud service providers and managed security service providers – becoming the preferred alternative for security intelligence"

In a 'big data for security' implementation, information about physical employee access patterns, online access locations, data access information, network traffic and many other factors are combined to identify risky behaviour that may indicate a compromise or threat. For example, a critical database normally accessed by an account only from within the organisation on a weekday, is suddenly found to be accessed from an IP address in Ukraine on a weekend, and to be downloading large amounts of data. This then immediately raises an alert to lock or flag the account as potentially compromised. Big data's advantage for this is the massive amount of data that can be analysed and correlated (well beyond the capability of most SIEM systems), leading to identification of threats that would not otherwise be found.

This expansion in both the commercial and security related use of big data, has also resulted in high demand levels for skilled security and data analysis professionals – the supply of which is struggling to meet demand. This is putting pressure on vendors to pre-package security intelligence capabilities into big data platforms as a way to enable customers to better secure their projects. It's also quite likely that we'll see movement toward service providers – both cloud service providers and managed security service providers – becoming the preferred alternative for security intelligence.

As has happened with other complex IT and security technologies, enterprises will come to a point where they ask themselves whether security intelligence is core to their business or whether it's something that is easier, faster and less costly to implement and maintain if managed by outside experts. Security intelligence based on SIEM and big data implementations has the potential to be outsourced to service providers with the requisite experience, skills and implementation capabilities. Note that, for organisations with the most sensitive needs (many financial institutions, government agencies, etc), outsourcing to a service provider simply isn't a viable option. For these organisations, in-house implementations will continue to be the standard.

Explosion of devices

The Internet of Things trend will also change matters. Devices that collect all kinds of data are exploding in popularity, and it is only a matter of time before they start to become useful for security intelligence purposes. Indeed, power meters, cable modems, phones, medical devices, wireless access points, traffic density scanners and more will increasingly feed data into big data implementations. Interestingly, security-related big data implementations will result in new data sets that can be used for context aware pattern recognition and profiling. This information can then in turn be used to enhance current threat recognition, or to provide a logical check to prevent false positives based on less complete security profiles.

> ***"Businesses of all sizes need adequate security intelligence mechanisms in place to monitor all activity across their networks, so that they can spot any suspicious activity and stop hackers in their tracks"***

Data is becoming an increasingly valuable currency, and hackers are becoming more cunning in their attempts to steal it. For businesses, this has greatly increased the risk of reputational damage and called for a step change in current data security policies, particularly as consumers are rapidly losing patience with those who cannot safeguard their private information. As such, businesses of all sizes need adequate security intelligence mechanisms in place to monitor all activity across their networks, so that they can spot any suspicious activity and stop hackers in their tracks. However, as operational infrastructures become increasingly complex, security practises will need to evolve in tandem.

There remains the issue of how to fund the implementations and tools required to protect systems. Today's organisations are faced with the fundamental need to reprioritise their IT security spending to support these new tools. It's a hard decision for many who have spent decades keeping intruders at bay with the latest firewalls, network segmentation tools and endpoint defences – and these are now becoming less effective. It isn't that they should be eliminated, but they should no longer be the core focus of an organisation's security stance. A shift in spending priorities is needed.

About the author

Sol Cates is chief security officer for Vormetric and is tasked with ensuring the company's internal security profile remains robust, while maintaining a strong pulse on the technical and business decision- making process in today's IT/IS organisations. Cates partners with teams throughout the company and the industry to engage with both customers and partners. He is sought after to speak publicly to elevate industry understanding of data security best practices in today's complex cyber threat landscape. The technical depth and understanding of the information security space Cates has developed over the last 17 years is rooted in the intelligence community, financial services industry and other large enterprise organisations. He originally joined Vormetric in 2003, as a security engineer, and later became the senior director of field engineering and solutions architecture. Cates' career also includes technical sales, engineering and support leadership roles at Tripwire, Symantec, SignaCert and Spectra Physics, as well as consulting for many Fortune 500 companies and government agencies on cyber-security.

Should the dark net be taken out?

Cath Everett, freelance journalist

Cath Everett

Although the dark net is not necessarily something that many people outside the tight world of information security are hugely familiar with, its profile has been rising steadily over recent months. For example, it hit headlines around the world towards the end of last year, following the high-profile Operation Onymous, which was conducted by a mixture of US and EU international law enforcement agencies.[1]

Onymous targeted so-called 'dark markets', or online marketplaces operating on the dark net that sell illicit goods such as drugs, stolen credit card numbers and weapons. The aim was to raid and close down these illicit shopping sites, the most famous of which was Silk Road 2.0, which was only accessible via the Tor network – the original and most famous means of accessing the dark net.[2]

Tor, formerly known as The Onion Router, is a peer-to-peer network and browser employed by interested parties from the early 2000s to surf the Internet anonymously. It was originally developed by the US Navy in the mid-1990s in order to communicate with agents in the field without divulging their whereabouts, so as not to put them in danger.

But Tor, alongside other newer darknet file-sharing variants, such as JonDo, are now used by criminals, whistle-blowers and dissidents alike to enable them to communicate anonymously with trusted peers and avoid government snooping.[3]

"No-one really knows how big the dark net in its entirety is either because its services are by their very nature hidden"

As to how large the dark market black economy actually is in reality, though, no accurate statistics are currently available as no-one actually knows. In fact, no-one really knows how big the dark net in its entirety is either because its services are by their very nature hidden – although it is believed to be much smaller than the open Internet.

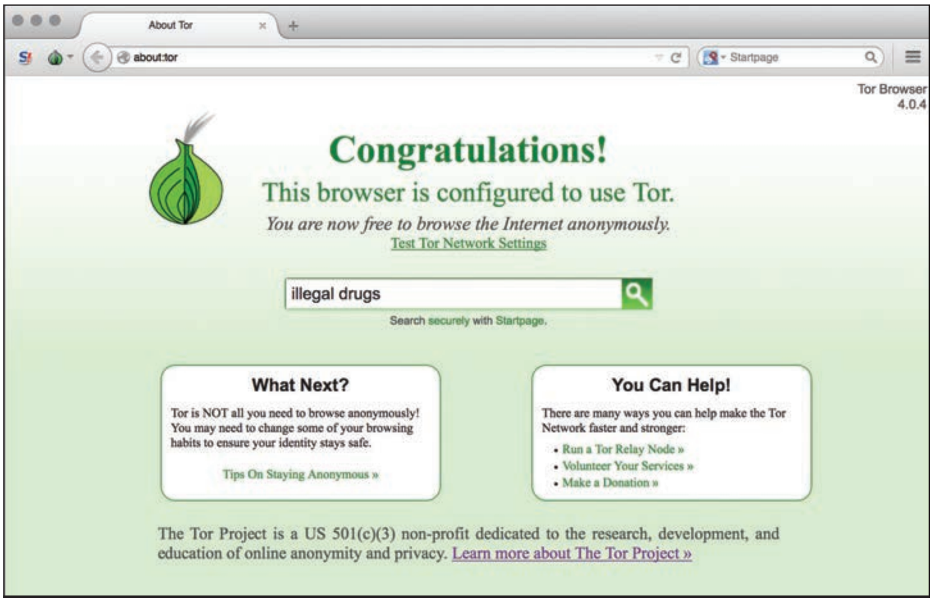
Hidden services

However, to give some inkling, members of the Tor project estimate that, on their network alone, there are between 1,000 and 1,200 hidden services and approximately three million users.

Operation Onymous, by way of contrast, led to the much-touted shutting down of around two-dozen hidden services and the arrest of some 17 marketplace vendors and administrators. Around $1m-worth of bitcoins, the standard currency for dark market transactions, as well as €180,000 in cash, drugs, gold and silver were also seized.

But it is worth noting that criminal activity in the dark net tends to be quite specific in nature, says Neil Hare-Brown, chief executive of information security consultancy Storm Guidance. For instance, most fraud and denial-of-service style attacks tend to be undertaken on the open Internet. "I don't know any denial of service attacks that have occurred through the dark web – it's so slow, it's like going back to the mid-1990s so it's just not performant enough," he explains.

On the other hand, Hare-Brown indicates that hackers undertaking targeted attacks would probably opt for the anonymity of the dark net. Criminals and terrorists also popularly employ it as a communications tool in order to help them plan activities. In addition, illegal shopping sites such as Evolution and Agora have now resulted in a situation where "most drugs are being bought and sold via the dark web – so many, in fact, it's amazing", he adds.



Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Settings

illegal drugs

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- Run a Tor Relay Node »
- Volunteer Your Services »
- Make a Donation »

The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

The Tor Browser Bundle allows anyone to use the web anonymously and easily.

Another recent moment in the spotlight for the dark web, meanwhile, was its name-checking by UK Prime Minister David Cameron last December when he unveiled the creation of a new government unit to target individuals using it to share child sex abuse images. The unit, which will be jointly run by British intelligence agency GCHQ and the National Crime Agency, which fights serious and organised crime in the UK, has yet to be assigned a name. But a key goal is to develop new high-tech ways of analysing vast quantities of child-related pornographic material on the dark net in order to better identify and arrest offenders.

Global network

Such activity would appear vital when, according to Tim Watson, director of the Cyber Security Centre at Warwick University, a huge 80% of all visits to dark net websites are to those hosting abusive images of children. As a result, focusing on paedophile activity as a starting point appears to make sense when trying to tackle dark net crime, with or without the inevitable elements of political expediency.

"A key goal is to develop new high-tech ways of analysing vast quantities of child-related pornographic material on the dark net in order to better identify and arrest offenders"

"If you look at high-tech crime units across the UK, traditionally about 70% of their activity is spent on paedophile stuff," Watson says. "There's lots of crime, but if it's a choice of going after people stealing credit card details or a gang abusing children who continue to be at risk, I think the public would probably support them in what they're doing."

In a move that should help such efforts further, some 30 countries around the world, including the US and UK, have likewise agreed to either set up their own national databases of child sex abuse content or provide links to Interpol's International Child Sexual Exploitation

Neil Hare-Brown, Storm Guidance: "Most drugs are being bought and sold via the dark web."

Database (ICSE DB).[4] ICSE makes it easier to share and remove these images once they emerge from the dark onto the open Internet, but the main objective in creating a global network is to make it easier to detect criminals and identify victims across international borders.

International cooperation

Nonetheless, the ongoing dearth of international legislation or even global harmonisation of national laws means that tackling crime on either the open Internet or the dark net remains a huge challenge.

Guillaume Lovet, threat intelligence lead at network security company Fortinet's FortiGuard Labs in Europe, the Middle East and Africa, explains that being able to arrest criminals, whether paedophiles or not, is only possible if they happen to be located in the same countries as their victims, which is rarely the case.

While the perpetrators are often based in Eastern Europe, South America or China, their victims are generally found in the West. "So Western Europe and the US can have all of the laws they want, but if the aim is to arrest someone in the East, they need cooperation there," he says.

The big question, though, is why countries elsewhere would bother to cooperate at all. As Lovet points out: "The victims are elsewhere and crime profits the local economy as the money generated in the West is taken back to the East, creating a chain of wealth creation."

As a result, most countries have no incentive to take action and, even if laws are passed to please the international community, they tend to be enforced only infrequently and under pressure. To make matters worse, the lack of bilateral agreements between individual countries outside of the European Union makes the bureaucracy involved in investigating international crime vast, which in turn makes such activity very expensive.

Storm Guidance's Hare-Brown explains: "This team from the UK will need to visit here and there and meet their dignitaries, officials, experts and the like. But it causes practical, logistical problems, which means you're very limited in the number of investigations that can be performed each year."

Nonetheless, he puts the relative success of Operation Onymous – despite widespread criticism in the information security community for overstating outcomes that later had to be revised – more down to "good, old-fashioned, standard police work" than any mind-blowing technical capabilities.

"Western Europe and the US can have all of the laws they want, but if the aim is to arrest someone in the East, they need cooperation there"

"Really it was about good investigation work, which involved following up leads and putting people under surveillance," Hare-Brown says. "I'd love to say it was about great high-tech skills and tools, but it was much more about the quality of the investigation."

National level

Even at the national level, however, the situation is far from straightforward. According to a recent UK Home Office report on cybercrime, not only is as little as 2-3% of such activity reported, but there is also no consistency between police forces on how they undertake investigations.

To compound the issue, law enforcement teams tend to be under-resourced, which means, in the words of Mike Gillespie, founder and managing director of information security consultancy Advent IM, it becomes "like chasing a spectre".

Tim Watson, Warwick University: "It's sometimes difficult for those parts of the police focusing on cybercrime to get the resources they need."

"It's like Del Boy in [the TV show] 'Only Fools and Horses' with his pop-up stalls. He sets them up, sells stuff from them for a while and then they pop up somewhere else – and it's the same with beta and mirror sites on the dark net," he says.

Shut down?

Despite the UK Government's rhetoric about its keenness to tackle the issue, it appears that at least some of the foot-dragging may have a political element.

"It's sometimes difficult for those parts of the police focusing on cybercrime to get the resources they need," explains Warwick University's Watson. "The government is waking up to the fact that we have a big hidden crime problem, but the question is does it really want to show crime figures shooting up, especially if there's not enough money to properly resource things?"

This ongoing situation has led to there being a significant skills gap within law enforcement agencies resulting in a lack of trained specialists – and even general awareness.

As John Walker, chief technology officer at Cytelligence, which offers organisations cyber-protection services, points out: "If you walked into the aver-

Mike Gillespie, Advent IM: Prosecuting cases is "like chasing a spectre".

age police station and said you'd been attacked by criminals in the dark net, they'd just stare at you."

All these difficulties notwithstanding, there appears to be little appetite to try and shut down the dark net completely – even if it were technically possible. Watson explains: "It's the equivalent of asking should we close down illegal activity in a city. You could shut the city, but the problem is that there's a lot of valid activity goes on there and where would everyone live?"

"If you walked into the average police station and said you'd been attacked by criminals in the dark net, they'd just stare at you"

For example, he pointed out, valid dark net activity is carried out by journalists, whistle blowers and dissidents fighting against totalitarian regimes. "So there's an argument to say that the benefits of having it in place outweigh the disadvantages, and I think a number of people would have difficulties if you said it was going to be completely closed down," Watson adds.

Advent IM's Gillespie agrees: "Just because you have nefarious elements doesn't make the technology evil. But the NSA has been quite vocal lately that if people use elements of the dark net, they will consider you a potential target."

A growing problem

The justification appears to be that, if someone choses to use Tor – "the whipping boy for the dark net" – they must have something to hide rather than simply preferring to have a bit of privacy. "But it's that kind of attitude that makes people wary of the whole security thing," Gillespie says.

"There's a fine line between national and international security and the protection of individuals and the masses," he continues. "We obviously want criminals to be caught, but you have to be careful. There's been a continual erosion of civil liberties in the UK over recent years and every time they've been handed over, we've been told it's in the interests of national security."

The proposed banning of encryption technology to enable UK intelligence services to access all digital communications is the latest case in point.

"The technology evolved to protect data in transit and at rest from criminals," says Gillespie. "So the danger is that we lose our protection against criminals so that the government can catch criminals. It doesn't make sense."

Nonetheless, there is concern that cybercrime on both the dark and open Internet is continuing to grow apace and is becoming ever more dangerous. For instance, one worrying trend is how progressively porous the boundaries between different types of cybercrime have become over the past 12 months.

In the past, crimes tended to be motivated by money, involved targeted attacks by state-sponsored hackers or were undertaken for ethical reasons by hactivists, or for fun. But the three are now starting to morph into each other, warns Fortinet's Lovet. For instance, in January last year, there were a series of targeted attacks on Target shops, followed by more in December on Home Depot. "So it seems that criminals motivated by money were starting to use the tactics of state-sponsored hackers and the like," he says.

Another concern is the progressive amount of consumer and corporate goods and services that come with IP addresses and network cards in order to connect them to the Internet.

John Walker, Cytelligence: "It's the equivalent of asking should we close down illegal activity in a city."

"Increasingly, everything is harmonising under one IP Internet-enabled system, which means that people can go wherever they want," Storm Guidance's Hare-Brown says. "Everything is becoming connected from smart fridges to corporate networks so hackers are now able to act with growing levels of impunity."

About the author

Cath Everett has been an editor and journalist for more than 20 years, specialising in information security, employment, skills and all things HR. She has worked in the online world since 1996, but also has extensive experience of print, having worked for publications ranging from The Guardian *to* The Manager. *She returned to the UK from South Africa at the end of 2014 where she wrote a lifestyle blog for International Business Times.*

References

1. 'Operation Onymous'. Wikipedia. Accessed Mar 2015. http://en.wikipedia.org/wiki/Operation_Onymous.
2. The Tor Project. Home page. Accessed Mar 2015. https://www.torproject.org.
3. 'JonDo – the IP changer'. Home page. Accessed Mar 2015. https://anonymous-proxy-servers.net/en/jondo.html.
4. 'Victim identification'. Interpol. Accessed Mar 2015. www.interpol.int/Crime-areas/Crimes-against-children/Victim-identification.

Threats to satellite navigation systems

Guy Buesnel

Guy Buesnel, Spirent Communications

Global Navigation Satellite System (GNSS) solutions are everywhere now. The capabilities of what many people loosely term GPS can be found not just in cars and aircraft, but are increasingly being integrated into many portable devices and are a key function in the Internet of Things (IoT). But not enough attention has been paid to weaknesses in the systems – notably, their vulnerability to jamming and spoofing.

Jamming the signal

Large-scale GNSS jamming poses a major threat but, hopefully, a distant one. More immediate is the risk of accidental disruption of systems relying on GPS, where a little bit of hardening could provide a lot of comfort.

In January 2007 GPS reception across downtown San Diego was disrupted. This was later reported as causing chaos: air traffic control was compromised, emergency pagers stopped working, cell phones lost signal and ATMs packed up. It took the best part of three days for the authorities to discover the cause: two US Navy ships in San Diego harbour had been conducting a training exercise when a GPS interference source was accidentally activated. It turned out that, contrary to initially claims, the event actually passed almost unnoticed, and yet all those terrible consequences *could* have happened.

Most people have had some experience of a gap in GPS performance – you are briefly informed by your GPS receiver that you are in some unlikely location, before it jumps back to a more credible scenario. But overall the system works so well that people take it for granted. What is not so well known is that the very reliability of the system means that it has become the foundation of a whole lot of other location-critical or time-critical systems. If that Navy vessel's jammer slightly distorted GPS readings, it would be a passing irritation to the taxi driver – but, for a very large ship with a pilot navigating in inland water, a few meters wrong could result in significant damage and pollution.

Useful services

Location services are a useful tool for any car driver, and more important for delivery people or taxi drivers where time is money. They are helpful for hill or forest walkers, all the more so in the wilderness where getting lost could risk lives. Of course they are vital for ships at sea and aircraft – but in such critical cases there will also be back-up location services in case of emergency. But how many people know that some railway systems rely on precise location at a station to determine when the doors should open?

And how many people know about another role played by GPS – namely providing ultra-precise clocking for time-critical systems such as ATM cash machines, cellphone networks, power supply grids and other utilities and certain financial trading systems? This is what lay behind the exaggerated stories of chaos in San Diego – they were all things that might have happened if the local GPS coverage had been significantly jammed.

A GPS jammer designed to plug into car cigarette lighter capable of jamming signals for up to 500m.

> ***"Even the cheapest jammers available online can cause complete outages of the receiver signal"***

Of course the risk from Navy vessels only applies near the coast, but there is a far wider threat from pocket-sized GPS jammers on sale today – as you see if you Google 'GPS jammers'. According to a *Guardian* newspaper article, these pocket-sized devices are used by thousands of people in the UK. "It creates a bubble around the vehicle for about 500 metres that jams any GPS receiver or transmitter," Prof Charles Curry of Chronos Technology told the newspaper. "It stops any tracking system the owner might have put on the car. Usually they will block GSM [mobile phone] signals too that might also be used to send back a location. It means that for anyone trying to track the vehicle, it just vanishes off the map – it's as though it were in an underground car park."[1]

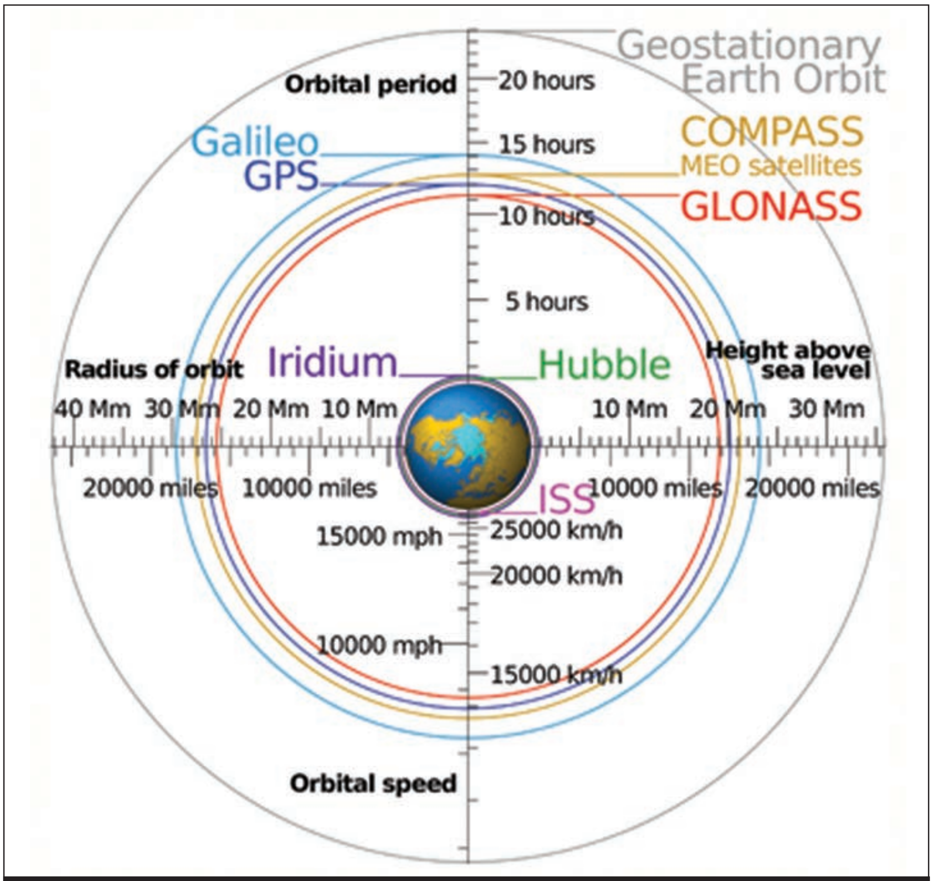
Why would anyone want to do that, other than for a prank? There are several reasons: a car thief not wanting to be caught in case the vehicle is fitted with a tracker; someone trying to avoid an automatic tolling or distance-based insurance system; or an adulterous spouse covering tracks when ostensibly 'calling in at the office'. More realistically there are delivery vans fitted with trackers to monitor driver behaviour – not driving for too long or at prohibited times or entering forbidden areas. Some van drivers have used these jammers to cover moonlighting activities, and taxi drivers have been known to pocket the fares rather than share them with the cab company. "Even the cheapest ones [jammers] available online can cause complete outages of the receiver signal," Dr Chaz Dixon, Stavog project manager, told reporters.[2]

> ***"Anyone responsible for building, or installing, GPS-enabled systems should consider testing them for vulnerabilities and, if necessary, finding ways to harden the system against jamming"***

A 500m bubble may not pose a major threat under most circumstances – but what if thousands of people are using them? Or what if some systems are extra sensitive? Last year a truck driver was fined $3,000 because his little jammer was affecting air traffic signals at Newark Airport and in June 2014 the Federal Communications Commission (FCC) fined a Chinese manufacturer of portable GPS Jamming devices, a record $35m.[3] Other types of unregulated electronic devices can also cause problems – for example, harmonics from illegal porno TV transmitters in Europe have been known to affect GPS receivers.

The real problem

So what is the real problem here? It breaks down into two contrasting scenarios. In one case there is a possibility that someone might get hold of a military grade device capable of disrupting all GPS systems across a wide area. Think of all the things that might have happened in San Diego: train doors not opening causing delays that disrupt timetables, ATM machines not working so bills don't get paid; taxis and deliveries going haywire and no-one being able to use their cellphones to get out of the mess; emergency services not arriving on time – a myriad little crises like throwing sand into a machine and ultimately causing the entire city to grind to a halt. As a terrorist act it could do more damage than a bomb. As a crime it might seem pretty pointless – unless used to lock down the region's police forces to provide cover for a major robbery.



A comparison of GPS, Glonass, Galileo and Compass (now BeiDou) satellite navigation system orbits with the International Space Station, Hubble Space Telescope and other orbits. Source: Wikipedia, http://en.wikipedia.org/wiki/Satellite_navigation.

The second scenario is far more immediate: the spread of pocket jammers or interference from unlicensed sources could increase the risk of important functions relying on GPS being compromised in a totally unexpected manner. Anyone responsible for building, or installing, such GPS-enabled systems should consider testing them for such vulnerability and, if necessary, finding ways to harden the system against jamming.

GNSS test systems are available now that will recreate any number of jamming attacks under realistic and extreme operating conditions and these can be used to assess the vulnerability. Once this is known, the operator is better placed to assess the risk and plan emergency measures. If your train doors will not open without GPS, then consider the options for manual override. Better still, it might be possible to harden your systems enough to reduce the risk to a manageable scale. Even simply knowing the extent of vulnerability is better than facing the unknown.

There is not much that the system installer can do against the first scenario: defending against a military scale attack is better left to the military. But even then it can help to have your systems tested so that emergency measures can be devised and assessed.

The more widespread problem is uncertainty: small devices may only compromise signals over a short distance, but GNSS signals at the Earth's surface are of such low power that even the weakest jamming signal could cause unpredictable results. So it is best to measure that vulnerability, weigh up the possible risks, and decide how best to reduce or bypass them.

Spoofing the signal

The other major concern is spoofing. There is growing concern that faked

What is GNSS?

Although most people refer to satellite navigation systems as 'GPS' (Global Positioning System), strictly speaking that describes just one of the systems in use today – the US Navstar network of satellites, originally intended for use by that nation's military. It first became operational in 1978 and was opened up for global availability in 1994.

Global'naya Navigatsionnaya Sputnikovaya Sistema (Glonass) is the Russian equivalent, developed during the Soviet era and which went through a period of post-Soviet decay before being restored to global coverage in 2011.

China has a regional system, BeiDou (formerly known as Compass) which is aims to expend to global coverage by 2020.

The European Union and European Space Agency are developing the Galileo system, with some satellites operational now but with the full system offering global coverage not expected to be ready before 2020 at the earliest.

France is also developing a regional system, Doris (Doppler Orbitography and Radio-positioning Integrated by Satellite), and India and Japan have undertaken similar projects.

signals, apparently from a GNSS, could be used for criminal purposes. Recently, a group from the University of Texas demonstrated how a false GPS signal generator could override a luxury yacht's navigation computers as it travelled from Monaco to Rhodes in the Mediterranean. First an alarm reported that the ship had wandered off course and the computers re-plotted the supposedly 'correct' course based on false signals. There was no secondary warning to suggest that the new course was incorrect.

Professor Todd Humphreys who lead the spoofing team said: "I didn't know, until we performed this experiment, just how possible it is to spoof a marine vessel and how difficult it is to detect this attack … With 90% of the world's freight moving across the seas and a great deal of the world's human transportation going across the skies, we have to gain a better understanding of the broader implications of GPS spoofing."

Those broader implications could include the critical role of GPS in providing highly accurate time data, as we've already seen.

Why are GPS systems vulnerable?

GPS navigation devices have become so common – in cars, built into smartphones and in handy gadgets for rugged outdoor activities – that it is perhaps surprising to learn that they rely on very delicate measurement of extremely weak signals.

"The signals reaching your GPS device are actually weaker than the background electronic, or thermal 'noise'"

Even with around 30 satellites in orbit at about 20,000km above the globe, the distance between any satellite and a GPS receiver is far greater than the distance to the nearest cell tower, while the satellite has to rely on solar power to generate its signals. The signal power can be thought of as being equivalent to a 40-watt light bulb, and the signals reaching your GPS device are actually weaker than the background electronic, or thermal 'noise'. So how can the system possibly manage?

Part of the answer is that the GPS signals are, by digital data standards, lengthy pieces of code, and the receiver is specifically listening for those codes – just as you might recognise someone calling your name even across a crowded, noisy room. To achieve this, the receiver takes its time – again by digital data standards – while it searches for and acquires those faint satellite signals. This is why, when you switch on your satnav, you typically have to wait a few seconds for it to come to life.

Having taken time to identify the signals, the actual calculation of position relies on extremely accurate timing. Each satellite contains its own atomic clock keeping near-perfect time that forms part of the signal transmitted – so the receiver gets a time signal that was 'exact' when transmitted but is 'slow' when received because of the time it takes for the signal to travel from satellite to receiver. The discrepancy between time signal and time of arrival provides a measure of the receiver's distance from the satellite.

It is actually even more difficult than that. First, the speed of light, and so of transmission, is slower as the atmosphere gets thicker towards the surface of the earth, making the calculation a lot more complicated. Second, the receiver does not have its own atomic clock on board, so cannot be totally accurate about the signal delay. To get round this problem, the system has to use the satellite time signals to reset its own internal clock at the same time as measuring those signals – effectively becoming the satellite's 'slave clock'. What makes this possible is an element of redundancy: if you had perfect time in the receiver you could fix your location in 3D space with only three satellite signals; instead the system looks for four (or more) satellite signals to not only provide verification through redundancy but also allow for iterative time verification.

The miracle is not so much the miracle of human inventiveness, as the miracle that it actually works – in a relatively cheap handheld or wrist-worn gadget.

Cracking the system

Given such weak signals and such a complex calculation, the easiest way to disrupt GPS, as we've seen, is to jam the signals. However, this is a pretty blunt instrument, in the sense that the impact of the jamming cannot be controlled or targeted. Approaching the jammer, the receiver will stop tracking satellites and most individuals will realise that something is amiss and stop using it. Out comes that dog-eared street map you last saw somewhere in the car boot – and in something as critical as an aeroplane there are always alternative navigation systems just to be on the safe side.

What could be even more threatening is 'spoofing' – that is, creating fake GNSS signals with all the complexity of real signals while specifically designed to generate false but convincing position data. However, you can guess from what has been said about the nature and subtlety of these signals, it is clearly not such a trivial task as simply jamming.

The real threat of spoofing is that the victim does not know what is happening and so carries on using false information. A spoofing box like the one created by the students could be concealed aboard a ship or plane and at some time be switched on, replicate the real signals and be accepted and then increase signal strength until it dominates the real signals, and then begin to bend reality by taking the vessel off course and into forbidden territory – or onto rocks.

Cleverly done

This would need to be done cleverly – not even the most trusting navigator would accept that the ship was cruising down Kensington High Street – so what defence measures are there apart from common sense? There is visual confirmation – if the supposed location looks way off course suspicions will be aroused – and there are alternative positioning systems such as those based on dead-reckoning using accelerometers, vision sensors, or an alternative fixing technology such as eLORAN. Augmenting your GNSS with one of these technologies could provide an indication that something is wrong.

"The damage could be less obvious than a plane or ship going off course – such is the extreme accuracy of the GPS atomic clocks that they are widely used as a source of accurate timing"

Then there is the alternative provided by another good GNSS. Although the US military might regret no longer having a monopoly with GPS, the fact that there are other systems operational or coming online will provide extra resilience, and the European Galileo constellation is deliberately designed to complement GPS for additional accuracy and resiliency. So a truly diabolical spoofing attack would also need to foil all these back-up alternatives, and that could include not only the complexity of creating realistic GPS signals but also spoofing every other likely GNSS signal in the vicinity just in case.

Would it be worth the effort? We can see the potential for disruption that might tempt an enemy nation to launch a spoofing attack. And the damage could be less obvious than a plane or ship going off course – such is the extreme accuracy of the GPS atomic clocks that they are widely used as a source of accurate timing. Every cell tower, for example, has its own GPS receiver, not because it might forget where it is, but to provide a super-accurate time signal for its own transmission purposes.

Some financial high-speed trading systems are so incredibly time-critical that they rely on GPS time data to determine precisely when trades were made. You can imagine criminal – or military – ingenuity might develop ways to generate all sorts of mayhem out of a cleverly targeted spoofing attack.

Do not forget also the human factor: these systems have served us so well already that it is increasingly tempting to put blind faith in them. The recent MAIB report on the collision between Seagate and Timor Stream identified several human errors, including an oversight that one of the ship's AIS devices was broadcasting a heading 160 degrees out.

We are entering a whole new territory – with little more than a spoofed GNSS to guide us. Maybe.

Analysing and minimising the risk

It is perhaps comforting to know that a spoofing attack will demand rather sophisticated technology to generate realistic signals and not be immediately recognised as a fraud. But it remains cold comfort unless there is some way to assess how your GNSS receiver responds to spoof signals and use that information to devise a counter-strategy that increases resilience to interference.

Test beds have been created to provide such test and measurement – the EU's Joint Research Centre has developed one for its Galileo project, for example. But now we are seeing the introduction of commercially available systems to test GNSS under laboratory conditions.

These new solutions provide a laboratory test bed, incorporating simulators, monitors and computers with software designed expressly for GNSS testing, and that includes testing against possible spoofing attacks. Basically, the system creates those subtle GNSS signals in a truly realistic manner – taking account of all the factors that can distort their timing and the sort of background noise they struggle against – and transmits them down a cable to the receiving device, rather than through the air. This allows very sensitive monitoring and measurement of the receiver's behaviour under truly realistic GNSS operating conditions, as well as when various spoofing, jamming or other likely attacks are thrown at it.

"Eventually there will be a set of standard tests which will allow GNSS users to select the best equipment for their application based on the level of protection against jamming and spoofing"

In practice this could allow a large GNSS user or receiver manufacturer to test devices to see how well they perform, how reliably and how vulnerable they are to attack. It also means that device manufacturers now have a means to develop standardised tests against set criteria to improve the performance and reduce vulnerability of their products. Eventually there will be a set of standard tests which will allow GNSS users to select the best equipment for their application based on the level of protection against jamming and spoofing it offers.

This has important implications for the whole GNSS market, as users can begin to demand equipment that has passed certain tests on an industry standard test bed, and these tests could include a measure of spoofing vulnerability.

About the author

Guy Buesnel is product manager, GNSS vulnerabilities for Spirent Communications. He has more than 16 years' experience of protecting GNSS receivers from emerging threats , having started his career as a systems engineer involved in developing GPS adaptive antenna systems for military users at Raytheon Systems in the UK. He then became involved in GPS and GNSS receiver system design with the aim of designing a new generation of rugged GNSS receivers for use by military and commercial aviation users. In 2007, Buesnel became the European GNSS product line manager at Rockwell Collins UK where he was responsible for UK and European GNSS development activities. In 2013, he accepted a position at the Satellite Applications Catapult in Harwell where, as a principal satellite navigation systems architect, he was responsible for helping UK businesses to understand GNSS vulnerabilities and use this understanding to grow their businesses within the UK. Buesnel is a Chartered Physicist, a Member of the Institute of Physics and an Associate Fellow of the Royal Institute of Navigation.

References

1. Arthur, Charles. 'Thousands using GPS jammers on UK roads pose risks, say experts'. The Guardian, 13 Feb 2013. Accessed Mar 2015. www.theguardian.com/technology/2013/feb/13/gps-jammers-uk-roads-risks.
2. 'Moonlighting truck drivers source of GPS jamming in the UK'. LiveViewGPS, 18 Jun 2013. Accessed Mar 2015. www.liveview-gps.com/blog/moonlighting-truck-drivers-source- gps-jamming-uk/.
3. Brewin, Bob. 'FCC hits Chinese jammer vendor with record $34.9 million fine'. Nextgov, 19 Jun 2014. Accessed Mar 2015. www.nextgov.comdefense/2014/06/fcc-hits-chinese-gps-jammer-vendor-record-349-million-fine/86818/.

Delivering the Internet of Things

Gary Newe, F5 Networks

Gary Newe

The Internet of Things – objects and appliances with embedded sensors and chips capable of communicating online – will result in 50 billion devices being connected to the Internet by 2020, according to Gartner.[1] From fridges and bathroom scales, to fitness bands and home thermostats, the number of 'things' connected to the Internet is really taking off and it's a very exciting time for everyone. However, for many enterprises and consumers, the excitement of this new realm of connectivity is clouding the fact that, with more devices connected to the network, there comes a new array of security implications.

Support expected

For the enterprise, workers will use more devices to get their work done and they will expect the business to support these devices. Except that this isn't a vision of 2020 – it's an issue businesses are facing right now and is something that a surprising number of organisations are still shying away from. Businesses have to support more devices and more applications, whether they are hosted on premise or in the cloud, and ensuring that the right security is in place is a central part of this discussion.

Recently, we have seen concerns from the chairman of the US Federal Trade Commission (FTC), Editith Ramirez, at the Consumer Electronics Show (CES) who discussed the security of the Internet of Things and said that connected devices pose huge risks to privacy and security, and could allow businesses to paint a "deeply personal" picture of every consumer.

All we have to do is look at the recent massive Target breach, which was caused by a heating, ventilation and air conditioning company.[2] Stealing personal data and corporate data is bad enough, but the prospect of hacking into life support systems and even embedded medical devices is life-threatening.

If we look at what developments have been made for home products, and the hacking activities associated with them, it was proven recently that it only takes 15 seconds to hack Nest smart thermostats. Addressing the trend of fitness trackers, FitBits have been hacked and other fitness trackers are equally as vulnerable.[4] Also taking a look at the new wave of smart and connected televisions, there have been countless claims that these have vulnerabilities and, worryingly, hackers can take over the built-in microphones and cameras to take a look into consumer's lives.[5]

Collapsed perimeters

Network perimeters are collapsing, and IT now has to contend with a huge number of devices and applications that may well be beyond the traditional network perimeter. As more people, devices and applications get connected, businesses will need to be able to scale their architecture to meet the growing demand. All of this has to happen without spending any more money, as companies are always looking to reduce total cost of ownership of their networking infrastructure. The ability to dynamically allocate resources quickly, safely and reliably is not easy to achieve, but is essential in such a fast-changing environment.

> ***"Cost is often still a deciding factor in why organisations aren't prioritising investing in security solutions"***

What's needed from businesses is a change in attitude and the need to prioritise. Cost is often still a deciding factor in why organisations aren't prioritising investing in security solutions but it's important to note that the market has moved on from the days where investing in security solutions always required a large upfront cost.

For example, a distributed denial of service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Solutions to prevent DDoS attacks can be expensive and this often causes enterprises to put off implementation.

But, this doesn't have to be the case as organisations can look at implementing a DDoS-as-a-Service solution which will still provide the protection the organisation needs, but in a more cost-friendly way.

These highly adaptable solutions combine on-premises DDoS protection capabilities with a high-capacity cloud service and can take advantage of programmable technologies and APIs for a customised performance.

Other protections

But it's not just the security from DDoS attacks that organisations need to be thinking about. They also need to be protecting themselves in other ways too. Encrypting data and understanding who is accessing data from what device, and what authority they have to access the data, are all equally important. There are a variety of attack vectors out there and it's sensible to ensure that all bases are covered.

Over the next decade, we are only going to see more devices work their way into businesses, so it's worth being forward-thinking and prepared for any security implications that this brings. The cost – financially and in reputation – is far greater if an organisation suffers cyber-attacks and as a result has downtime or corporate or sensitive data is stolen, so it's worth looking at priorities over upfront cost.

Once cost is addressed and organisations understand that this doesn't require a complete overhaul of the IT infrastructure, the discussion should look at the sheer number of new devices that will be entering the workplace to evaluate the security implications they could bring.

> ***"No matter what devices are connecting to the network, if you protect data at the application level you should be in good stead"***

Fitness trackers are something that we're definitely seeing more of in the workplace. Tracking steps, distance travelled and calories burned is a phenomenon that has taken off a lot over the past year. This is great to see, but as this means that even more data is travelling across the networks in the workspace as a result of these devices, there is a chance that this could give hackers the opportunity to strike.

This greater willingness to embrace the Internet of Things puts most businesses in a position where they need to prepare themselves adequately for the changing ways in which employees will use technology in years to come. You can take specific steps to dealing with an influx of new connected devices making their way into your organisation. Here are a few thoughts on how to prepare.

Protecting the network

Make sure that your applications are protected. No matter what devices are connecting to the network, if you protect data at the application level you should be in good stead. This can be done using encryption. When you encrypt information at the application level, you can protect sensitive data and control access in a more fine-grained way than is possible with almost any other form of encryption. It is also worth remembering that application-level encryption can be policy-based and geared to specific data protection mandates such as PCI DSS (Payment Card Industry Data Security Standard), making it very suitable for enterprises.

Plan for an influx of devices and the impact it will have on capacity and bandwidth. This can be done by looking at an estimate of how many connected devices will be coming into the workplace over the next year. It could be as many as double if we look at how fast wearable tech, for example, is growing. Once this is established, think about how much extra bandwidth this will require. If there are double the amounts of connected devices, then you will probably need even more than double the amount of bandwidth.

Continued on page 20...

...Continued from page 19

If staff will be using wearables for business purposes, prepare guidance on the applications and acceptable use. This can be done easily, with a few sessions being held with employees to explain company regulations with connected devices and by offering advice from a security standpoint. If you tell your staff that corporate-sensitive data could be at risk, as well as their own personal data, if regulations aren't followed, then they are more likely to follow the guidelines.

"It's crucial that your company maintains control over who has access to its network and data"

It's crucial that your company maintains control over who has access to its network and data. Understanding who is accessing, where from and on what device will allow this level of control. Once this has been established, it is easier to put necessary measures in place to protect against any anomalies in accessing data, which could be a sign of hackers at work.

People factor

Technology and processes can support businesses through the changing flow of data brought about by wearable technology, but businesses must also remember the people factor and should keep employees updated on new processes and company regulations. This will help make sure that employees and processes are aligned and that business data is accessed within company policy, regardless of the shift in end-user technology.

With a whole new array of devices available and with our networks becoming busier with data every day, it's important to stress that businesses need to prepare for the age of the Internet of Things that is already upon us. Security measures need to be put in place and large and small company's alike need to think about their business and employees when planning to protect against vicious attacks. The security measures are out there and careful planning can go a long way, don't worry about cost and set out your priorities early. The key? Don't get overwhelmed and don't put it off – get prepared for the Internet of Things now!

About the author

Gary Newe is director, field systems engineering, UK, Ireland and Africa for F5 Networks, which he joined in 2007. His role includes working with channel and SI partners as well as working with larger customers on a range of F5 specific solutions. Newe is a Certified Information Systems Security Professional (CISSP) and also holds CCSE, CCNA and NSA certification. He is an active blogger on security challenges and application delivery. Previously, Newe worked at Siemens and Entropy, and has over a decade of experience in the network industry.

References

1. 'Gartner says personal worlds and the Internet of Everything are colliding to create new markets'. Gartner, 11 Nov 2013. Accessed Mar 2015. www.gartner.com/newsroom/id/2621015.
2. Vijayan, Jaikumar. 'Target breach happened because of a basic network segmentation error'. CIO/Computerworld, 6 Feb 2014. Accessed Mar 2015. www.cio.com/article/2378946/data-breach/target-breach-happened-because-of-a-basic-network-segmentation-error.html.
3. Sawyer, John. 'Tech Insight: Hacking the Nest thermostat'. Dark Reading, 14 Aug 2014. Accessed Mar 2015. www.darkreading.com/vulnerabilities – -threats/insider-threats/tech-insight-hacking-the-nest-thermostat/d/d-id/1298036.
4. Kumparak, Greg. 'Awesome Netflix/Fitbit hack detects when you've fallen asleep, auto-pauses your movie'. TechCrunch, 27 Feb 2014. Accessed Mar 2015. http://techcrunch.com/2014/02/27/netflix-fitbit-hack/.
5. O'Callaghan, Jonathan. 'Could your smart TV be HACKED? 'Red button' feature could be used to hijack web accounts'. Daily Mail, 9 Jun 2014. Accessed Mar 2015.

EVENTS CALENDAR

20–24 April 2015
RSA Conference 2015
San Francisco, US
www.rsaconference.com

21–22 April 2015
The Payment Security Summit
London, UK
www.pay-sec.com

27 April 2015
Data Risk Management in Financial Services
London, UK
www.drmfsummit.com

19–22 May 2015
OWASP AppSecEU
Amsterdam, Netherlands
https://2015.appsec.eu/

26–29 May 2015
Hack in the Box
Amsterdam, Netherlands
http://conference.hitb.org

26–28 May 2015
IFIP SEC 2015
Hamburg, Germany
https://ifipsec.org/2015/

2–4 June 2015
Infosecurity Europe
Olympia, London, UK
www.infosecurityeurope.com

2–3 June 2015
Infosecurity Intelligent Defence
Olympia, London, UK
www.infosecurityeurope.com/intelligentdefence

26–30 July 2015
AHFE – Human Factors in Cyber-security
Las Vegas, NV, US
www.ahfe2015.org/board.html#hfc