ELSEVIER

network SECURITY

ISSN 1353-4858 November 2017

www.networksecuritynewsletter.com

Featured in this issue:

Should jump box servers be consigned to history?

Jump boxes have been used for decades to protect and isolate critical systems. However, even though they don't store sensitive data, they raise serious security concerns.

With the growing popularity of hybrid ecosystems, where enterprises are transitioning to cloud-based infrastructure and incorporating third-party services and/or contractors, jump boxes become harder to implement effectively. A software-defined perimeter approach will not only solve jump box concerns, but will also strengthen security and compliance, explains Chris Steffen of Cyxtera.

Full story on page 5…

Putting security at the heart of app development

In the rush to get new apps to market before the competition, start-ups are cutting corners – and a failure to prioritise security is compromising customer data.

This attitude is leaving businesses open to fines and reputational damage. Any start-up wanting to create a great app with long-term value must look at the full development requirement – and that includes rigorous cyber-security. Organisations need to focus on leveraging the expertise of accredited development specialists and penetration testing teams, says Nick Thompson, DCSL Software.

Full story on page 7…

Security challenges for cloud-based email infrastructure

Commercial applications that were initially installed inside corporate server rooms are now hosted on cloud infrastructures, accessible anytime, anywhere.

However, mitigating cloud-based security risks requires that service providers and corporate users adopt a universal approach for ensuring that the right solution is in place, especially when application services used over insecure Internet connections raise new risks. Akashdeep Bhardwaj and Sam Goundar examine the kinds of threats facing cloud-based email systems and the mitigations available.

Full story on page 8…

Bad Rabbit ransomware attacks Russia and Ukraine

There has been another outbreak of ransomware, with some similarities to the NotPetya attacks – although there are also significant differences. So far, the malware seems to have mostly affected targets in Russia and Ukraine, with a handful of victims in Turkey and Germany, although it's possible it could spread further.

In Russia, the attack seems to have mainly targeted media organisations – the Interfax news agency was among the first to report problems. It has been spread via hacked media sites where the malware typically masquerades as a Flash installer.

According to Kaspersky Lab, the malware uses the same hashing algorithm

Continued on page 2…

Contents

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

Publishing Director: Bethan Keall

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

Senior Editor: Sarah Gordon

Columnists: Tim Erridge, Karen Renaud, Colin Tankard

International Editoral Advisory Board:
Dario Forte, Edward Amoroso, AT&T Bell Laboratories; Fred Cohen, Fred Cohen & Associates; Jon David, The Fortress; Bill Hancock, Exodus Communications; Ken Lindup, Consultant at Cylink; Dennis Longley, Queensland University of Technology; Tim Myers, Novell; Tom Mulhall; Padget Petterson, Martin Marietta; Eugene Schultz, Hightower; Eugene Spafford, Purdue University; Winn Schwartau, Inter.Pact

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.
Subscriptions run for 12 months, from the date payment is received.

More information: www.elsevier.com/journals/institutional/network-security/1353-4858

12987
Digitally Produced by
Mayfield Press (Oxford) Limited

…Continued from front page

as NotPetya (aka ExPetr) and is similarly capable of spreading through local networks using WMIC and local SMB shares. However, unlike NotPetya (and the earlier WannaCry), Kaspersky has seen no evidence of the use of the NSA tools leaked by the ShadowBrokers group. Neither the ExternalBlue code used in NotPetya nor the EternalRomance tool used in WannaCry have been found in Bad Rabbit. Instead, it uses brute force techniques to attempt access to shared hosts on the LAN, drawing from a hard-coded list of usernames and passwords.

Kaspersky's conclusion – that Bad Rabbit and NotPetya were written by the same people – has been supported by other security firms, including Cylance and CrowdStrike.

"BadRabbit and NotPetya DLL (Dynamic Link Library) share 67% of the same code, giving us reason to believe the same actor is likely behind both attacks," said Adam Meyers, VP of intelligence at CrowdStrike. "Bad Rabbit is likely delivered via the website argumentiru[.]com which is a current affairs, news and celebrity gossip website focusing on Russian and near-abroad topics."

All of the websites that were compromised in order to spread the ransomware were attacked on October 24 and Kaspersky said it had not seen evidence of any further attacks.

Wifi flaw affects nearly all devices

A vulnerability has been found in the WPA2 protocol used to secure wifi sessions. Discovered by Mathy Vanhoef of imec-DistriNet, the 'key reinstallation attack' (Krack) affects all devices using WPA2, which until now was considered the most secure protocol for wifi.

The vulnerability lies in WPA2's four-way handshake that establishes the encryption key for the session. The third message in this sequence, from the access point to the client, causes the client to install the agreed key and set a counter for a nonce (number used once) value that is used as a kind of salt along with the encryption key. By incrementing this number with each subsequent message and by starting with a number unknown to any potential attacker, it makes it impossible for attackers to reverse engineer the encryption key using 'cribs' – known or guessed bits of plain text message that can be matched to encrypted text in multiple messages.

The attack works by capturing the third message in the handshake and sending it again, multiple times, to the client. This causes the nonce to be reset to the beginning – ie, to the same value – for every message the client sends. This makes a brute force, crib-based attack possible. For example, attackers might look for standard messages they know the client will be sending out regularly, such as NTP time requests, that are in a standard format. Once the attacker has determined the encryption key, he can use this to mount man-in-the-middle attacks.

At no point is the wifi WPA2 password compromised, so changing passwords does not have any effect.

There are several variations on the attacks, depending on platform and implementations of WPA2. Both clients and access points will need to be patched. Microsoft has already rolled out a patch for Windows 10 which, in any case, was less vulnerable than most platforms. Apple's iOS platform is also thought to be slightly less vulnerable than most and has now received an update.

Android (version 6.0 upwards) and Linux are especially vulnerable because of a peculiarity of the wpa-supplicant program used for this process. When a client receives the replayed third message, not only is the nonce reset, so is the encryption key. Alas, the key is set to all zeroes, giving the attacker immediate access to the key without having to use crib-based attacks.

Another issue with Android is the fragmented support environment. Many users are dependent on equipment manufacturers or mobile service providers for patches.

The good news is that this flaw is hard to exploit. The attacker needs to be on the same wifi subnet as the target. And any communications that are encrypted – using HTTPS or SSL/TLS – remain secure. There is full information here: www.krackattacks.com.

In brief

Third of domains hit with DoS

In the past two years, a third of all Internet-connected hosts using IPv4 have been hit with denial of service (DoS) attacks, according to research by the Center for Applied Internet Data Analysis (CAIDA). "We're talking about millions of attacks," said Alberto Dainotti, a research scientist at CAIDA. The study is the result of a collaborative effort by UC San Diego, University of Twente in the Netherlands and Saarland University in Germany. The researchers used two data sources: the UCSD Network Telescope, which identifies DoS attacks employing spoofed addresses, and AmpPot distributed DoS (DDoS) honeypots, which are capable of recording reflection and amplification attacks. These techniques uncovered more than 20 million DoS attacks aimed at 2.2 million Class C addresses. There's more information here: http://bit.ly/2znJ9Rf.

Silence attacks banks

Kaspersky Labs has discovered an attack campaign, dubbed Silence, that is following the example of the highly successful Carbanak malware. The campaign is focused on banks – initially in Russia, although firms in Malaysia and Armenia have also been hit and it would be reasonable to expect attacks against banks in other countries. Like Carbanak, Silence starts with malware-loaded phishing emails being sent to bank employees and other financial institutions. Once the attackers have a foothold, they use this to spy on employees, watching for opportunities to transfer funds. The phishing emails appear to come from genuine employees of the bank and the attachments masquerade as contracts, but are actually JavaScript files with .chm (Microsoft help file) extensions. At least 10 institutions have been hit already and although their losses haven't been made public it's likely they run into the millions. There's more information here: http://bit.ly/2hLVHbv.

CVE lag creates zero-day risk

A delay in publishing details about software vulnerabilities is opening up opportunities for malicious actors to mount zero-day attacks, according to security firm Recorded Future. The company has previously warned of a lag between a vulnerability becoming public knowledge – at least within the security community – and it being published in the US National Vulnerability Database (NVD). Many organisations use the NVD database to manage their risk exposure. Now Recorded Future has shown that vulnerabilities are being included in China's National Vulnerability Database (CNNVD) much faster. On average, a vulnerability is published in the CNNVD within 13 days of disclosure whereas the NVD generally takes 33 days. In effect, malware authors and other criminals could use the CNNVD as a source of vulnerabilities with which to attack western organisations. The report is here: http://bit.ly/2yzWarL.

Microsoft downplayed 2013 hack

A breach of Microsoft's network in 2013 may have been far more serious than the firm admitted at the time. A number of tech companies, including Apple, Facebook and Twitter, came under attack by a skilled and well-resourced hacking group. Microsoft revealed that it had been breached but made the attack sound trivial. "We found a small number of computers, including some in our Mac business unit, that were infected by malicious software using techniques similar to those documented by other organisations," it said at the time. "We have no evidence of customer data being affected." However, according to a number of former insiders who recently spoke to Reuters, the attackers had managed to access a highly sensitive database of unfixed flaws in Microsoft's products – data that would have been highly valuable to cyber-criminals. The company carried out an assessment as to whether the flaws had been used for attacks and came to the conclusion that they had, but that the attackers could have gleaned the necessary data from other sources. Microsoft therefore decided to keep quiet about the breach. However, according to Reuters' contacts, this decision was flawed and based on insufficient information. There's more here: http://reut.rs/2Ao5SKI.

Fake WhatsApp

Google has deleted fake WhatsApp software from its Android Play Store – but not before over a million people had already downloaded it. The fake app's page on the Play Store looks exactly like that of the genuine app. Even the name of the company appears to be WhatsApp Inc, but actually contains two invisible Unicode characters at the end, presumably to evade automated checking for duplicate names by Google. When the app is installed it downloads the real app and embeds it inside advertisements. Google's systems failed to spot the fakery and became aware of it only when alerted by Reddit users. It's assumed that the developer created the app to make money from advertising impressions, but there was also the possibility that the ads could lead people to malicious sites.

Code-signing certs cost more than guns

There is now a lucrative trade in code-signing certificates on underground forums and they typically fetch up to $1,200. This means they sell for more than counterfeit US passports, stolen payment cards and even guns, according to an investigation by security firm Venafi. The certificates allow cyber-criminals to create malware that will run on more secure platforms – for example, in many instances software won't execute on Windows 10 or Apple's iOS and macOS unless it is properly signed. The report, conducted by the Cyber Security Research Institute (CSRI) for Venafi, found that such certificates are relatively easy to find in hacker forums.

DNC hackers identified

US investigators have identified at least six people – all Russian – that they believe are responsible for cyber-attacks against the Democratic National Committee (DNC) and the leak of emails that had a significant effect on the 2016 presidential election. According to a report in the *Wall Street Journal*, the Justice Department has gathered enough evidence to bring a case early next year. Research carried out by security firm Mandiant credited the attacks to the Fancy Bear hacking group (aka APT28), which is thought by many to be a branch of Russian Military Intelligence (GRU). However, even if indictments are brought, this is unlikely to lead to extradition and trial. The Kremlin has always denied involvement. There's more information here: http://on.wsj.com/2AlzyIF.

Reaper botnet

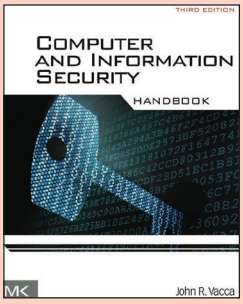
Another botnet based on compromised Internet of Things (IoT) devices has been identified. Security firm Check Point said that the botnet – dubbed Reaper and originally spotted by Qihoo 360 Netlab in September – had infected "an estimated million organisations", raising fears of another Mirai-like attack. However, Arbor Networks subsequently calculated the botnet size at around 10,000-20,000, with the numbers constantly fluctuating. The firm found another two million hosts that could become potential Reaper nodes but which, for some reason, have not become infected – possibly because of flaws in Reaper itself. The malware is commandeering wireless IP-based cameras, routers, storage boxes and wifi access points made by vendors including D-Link, TP-Link, Avtech, Netgear, MikroTik, Linksys and Synology. Arbor believes the botnet may be meant for use as a DDoS-for-hire tool. The firm has more information here: http://bit.ly/2zlUcu4.

Tor overhauled

The Tor network, which allows people to use the Internet anonymously and is widely employed by journalists and activists, is going through its biggest refresh in a decade. The Tor browser has been updated after it was found to contain a flaw that could leak a user's IP address under some circumstances. The system is also upgrading its crypto to SHA3 and there are several new features planned. There's more information here: http://bit.ly/2j6DGIp.

Reviews

BOOK REVIEW



Computer and Information Security Handbook
John R Vacca (ed).
Third edition published by Morgan Kaufmann. ISBN: 978-0-12-803843-7.
Price: $130, 1280pgs, hardback.
E-book edition also available.

Like so many technical domains, information security has rapidly become extremely complex and diverse. At one time, any self-respecting 'hacker' (of whatever colour hat) could reasonably expect to have a strong grasp of every aspect of security. Now, it's far more common to see people specialising in some particular niche – malware reverse engineering, say, or mobile device exploitation.

That kind of specialism is increasingly reflected in publishing, with information security books becoming more narrowly focused. But not this book, now in its third edition. The editor, John Vacca, has pulled together contributions from a large number of experts into a massive tome that touches on pretty much every angle of security and privacy – no fewer than 91 chapters in 15 sections.

The book tackles these issues at every level, from theoretical concepts (most notably in cryptography) through the quotidian implementation and management of security-related systems to higher-level issues of risk assessment. So while one would normally discuss what audience a book is aimed at, here it's hard to think of anyone with any interest in infosecurity who wouldn't get something out of it.

Indeed, the real value in this book might be in the way it covers aspects of security that you don't think are immediately pertinent to your work or interests. After all, this is not a book you're going to read from cover to cover. But imagine your day job consists of ensuring the security of your organisation's network and, suddenly, because of a new project, you find yourself needing to get up to speed with cellular network security. Or perhaps you need to make a presentation that touches on risk management.

In a sense, you could view this work as a large collection of primers that allows you to fill in the blanks in your knowledge. That's not to suggest that the chapters are in any way lightweight or superficial – far from it. There's plenty of practical, technical detail to get your teeth into here. However, if you really need to master one of these topics and become fully proficient in it, you'll almost certainly want to invest in more detailed publications. The ground covered here is so vast that not even nearly 1,300 pages is enough to treat everything exhaustively.

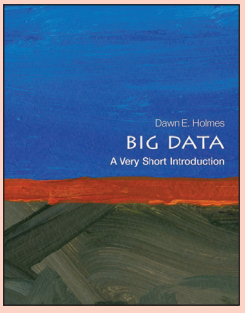
The quality of the content from the 30-plus authors is very high, although sometimes quite partial. For example, a chapter on Internet of Things (IoT) security concentrates on the ITU-T reference model – an important subject, to be sure, but one that doesn't really give a feel for the broad scope of IoT security issues. And I mention IoT to highlight the fact that, even though this book is in its third edition, developments in the field will quickly leave it behind. No book on security can remain up to date.

So why buy it? This is the reference work you want on your bookshelf when you need to quickly get a grounding in some new aspect of security. All the chapters come with extensive references, pointing you in the right direction if you need to explore more. But whatever it is you need to know about security, this will get you started.

There's more information here: http://bit.ly/2zjYjao.

– SM-D

BOOK REVIEW



Big Data: A very short introduction
Dawn E Holmes. Published by Oxford University Press. ISBN: 9780198779575.
Price: £7.99, 152pgs, paperback.

There are many fashionable terms in IT that people like to throw around to show that they are on top of the trends. Big data is definitely one of those, but how many people truly understand what it means and what the implications are is debatable.

One of the concerns about big data is that because it has achieved 'trend' status, many people assume that it is an inherently good thing. This has led to organisations harvesting data from the people who use their services or buy their products with little thought as to how to properly and ethically exploit that information.

Some businesses, of course, are entirely built on data collection – Google and Facebook spring to mind. Others have built their businesses around providing the means to collect and manage massive data trawls: for example, big data supports Amazon's retail operations but the firm's infrastructure services, such as AWS, have proven a highly lucrative sideline and are arguably more significant in the development of e-commerce and the modern app culture.

You can't fully understand today's Internet-enabled business models without understanding how big data is collected, structured and analysed. In many cases, some of the leading organisations are big data businesses: Google is not a search company, nor is Facebook a social network. Both are in the business of exploiting massive datasets, mainly for the purposes of advertising.

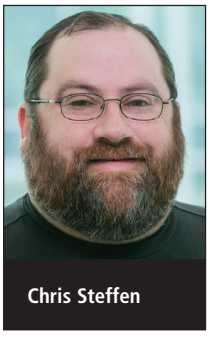
This book is, as it says, a short introduction to the topic – a high-level view, if you like. It is for anyone who has bandied about the term 'big data' but with a nagging sensation that they don't really understand what that means. It's something you could usefully give to that annoying senior executive who insists on using 'big data' the way equally clueless people used to use 'synergy' with similar incomprehension.

And it's good to see that, even in such a slim volume, security is not forgotten. Because the problem with valuable data is that it can be valuable to others, too – such as cyber-criminals. If you have data, then you have the care of data and so it's prudent to ask yourself whether you really need it at all. If you're not working that data for all it's worth, then the answer is 'no'. And not collecting data can reduce your risk exposure. Much of that is beyond the scope of this book, but as a primer in the subject it works well.

There's more information here: http://bit.ly/2yDshGZ.

– SM-D

Should jump box servers be consigned to history?


Chris Steffen

Chris Steffen, Cyxtera

Jump boxes have been utilised for decades to protect and isolate critical systems. The main purpose of the jump box is to act as a security guard at the entrance to the infrastructure. It checks the credentials of users approaching the gate, ensuring that only authorised users can log into the network environment and from there can safely get access to any of the other servers or boxes.

All traffic and actions by the jump box are logged and recorded via audit controls and, to further shield the connection, one could use multi-factor authentication when logging in. When it comes to protecting a system that's critical, jump boxes can make it harder for attackers to leverage stolen credentials.

However, even though jump servers don't store any sensitive data and can be a practical tool for enterprises with outsourced datacentres, they raise serious security concerns that simply can't be ignored.

Indeed, with the growing popularity of hybrid ecosystems, where enterprises are transitioning to cloud-based infrastructure and incorporating third-party services and/or contractors, jump boxes start to become harder to implement and significantly less effective.

Network separation

Looking for ways to create separation between networks with different security considerations, jump boxes offered an ideal solution. A system or device that acts as a bridge between two different networks, a jump box provides a method of controlled access from one common network to another, which usually contains highly protected, significant resources. Typically, they are highly regulated, more often than not by a security operations centre (SOC) or similar technical controls, requiring elevated approval or classified status to gain access.

Traditionally, jump servers are secured in much the same way as a normal desktop computer – ie, a username and password – with the user authenticating to a specific network. For example, a user requests permission for access to a jump server and, after access is granted, the secure connection is opened (via launching the jump server itself or opening a port on a firewall), with the user now having access to both networks (such as a user network and a protected production network). The jump server may have additional tools or restrictions as to the data or tools that can be used, but typically the user will now have complete access to the production network for as long as he or she is connected to the jump server.

As you'd expect, jump servers are heavily defended – they are not usually connected to the Internet and they are fully patched and automatically updated, which should make the network environment more secure. However, this is not always the case.

Three problems

While jump boxes may have ticked the check box for a regulatory audit to address separation of duties requirements, today they present three main problems.

First, they are very inconvenient. Though arguably they were supposed to be inconvenient, waiting for approvals and authorisations has always been cumbersome.

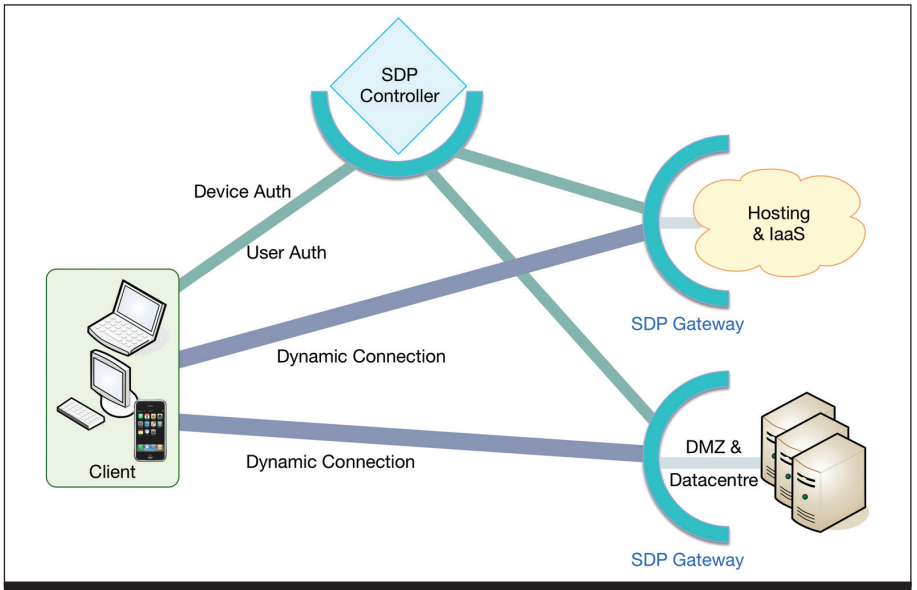
Next is lateral movement. Once the jump box is open, the user has free rein to access pretty much any and everything on the protected network.

Finally, there are the implications of a cumbersome and manual process. As already mentioned, jump boxes often have to be manually opened by a person – usually a member of the network operations centre or security operations centre team, requiring an email authorisation chain or trouble ticket to be approved before the connection is allowed. However, in today's hybrid environment where users are looking for efficiency and flexibility, the resultant delay causes frustration, with many looking to circumvent these controls.

Insecure security

Even though sensitive data is not saved on the server's disk, users' credentials are saved in the memory of the jump servers. This makes a jump box an attractive target for cyber-criminals. In recent years we have seen an increase in targeted assaults utilising privileged account exploitation with many citing this as the primary attack vector. If a malicious actor were to gain access to a jump server, he would then have the ability to connect to any or all resources that are available on the networks to which the jump server provides access (referred to as lateral movement), without the need for re-authentication. In most cases, the jump server will have access to a less-protected user network, but this in turn will still have sight of the protected production network with the applications and data that these protected systems generally access.

While jump boxes were originally introduced as gatekeepers to protect the infrastructure from outside threats, the reality is that, if compromised, these serve more as an enabler for attackers to access everything inside a network. For a malicious user, gaining access to a jump server is akin to giving the nefarious individual the keys to the entire



The software-defined perimeter security model.

kingdom and then turning a blind eye to their subsequent antics.

From the jump server, attackers can move from resource to resource, determining where the high-value data and processes reside, until they find anything and everything that they are looking for. If the organisation does not have a clear view of the actions being performed in real time, there is a very real risk of an attacker making away with an organisation's intellectual property, sensitive or personal data or even installing additional back doors for later exploit before disappearing through this concealed gateway.

Slamming the gate shut

To avoid those issues and ensure full security of their networks, organisations should consider implementing a different discipline that creates one-to-one network connections between users and the data they access. By taking a software-defined perimeter (SDP) approach, the main problems that are often found with jump boxes can be avoided.

SDP is a security architecture developed by members of the Cloud Security Alliance (CSA).[1] A relatively new network security discipline, it is devised around the user and designed for hybrid environments. The concept is to create one-to-one encrypted network connections between users and the data they access. This approach ensures that all endpoints attempting to access a given infrastructure are authenticated and authorised prior to being able to access any resources on the network. SDP takes an 'authenticate first, connect second' stance that ensures that only authorised users can connect to network resources. In tandem, unauthorised network resources are made invisible and therefore inaccessible. Thus, the attack surface area is reduced by hiding network resources from unauthorised users.

These session-based connections should be temporal – ie, they are provisioned when needed and then torn down afterwards, which prevents unauthorised access. There are SDP solutions available that can be configured to automate the approval process and through integration with 'trouble ticketing' systems, can grant access to specific resources and only these resources, escalating requests that don't meet the set requirements. Once access is revoked or closed, the user will no longer have access to these resources – a process that should be actioned immediately but is often overlooked.

Another benefit of an SDP approach is that, if an authorised endpoint device should become infected and a threat moves laterally to a server which the user is authorised to access, it will not be able to continue on discovering additional workloads to infect other resources, such as ports and protocols, as these are invisible. This containment to a single segment prevents the ability of such threats to communicate with a remote command and control (C&C) server – locking them down and keeping hackers out.

The final advantage that SDP delivers is the ability to encompass future architecture. As more devices are introduced to the environment – such as IoT – and working practices continue to evolve, the fact that it secures traffic between workloads will allow it to also morph and embrace these practices.

A leap of faith

There was certainly a time and place for jump boxes as part of an enterprise network. However, advances in technology have made them cumbersome and changes in working practices have rendered them obsolete. In tandem, the propensity of attackers to identify and then exploit privileged and shared credentials means that organisations need to be able to not just isolate, but also conceal, the important elements of the infrastructure and sensitive data.

Updating the security and network infrastructure to use a Software-Defined Perimeter approach will not only solve jump box concerns, but will also strengthen other security practices and compliance considerations that organisations face today.

About the author

Chris Steffen is the AppGate SDP technical director at Cyxtera. He helps to define AppGate's technical abilities as it relates to network access management and cloud computing solutions. Before joining the team at Cyxtera, Steffen served as chief evangelist, cloud security for Hewlett Packard Enterprise (HPE). He has also served in executive roles as director of information technology at Magpul Industries (a plastics manufacturing company) and as principal technical architect for Kroll Factual Data (a credit service provider). Steffen has presented at numerous conferences and holds several technical certifications, including CISSP and CISA.

Reference

1. 'Software Defined Perimeter Working Group'. Cloud Security Alliance. Accessed Oct 2017. https://cloudsecurityalliance.org/group/software-defined-perimeter/#_overview.

Putting security at the heart of app development

Nick Thompson, DCSL Software

Nick Thompson

In the rush to get new apps to market before the competition, start-ups are cutting corners. Yet in an era of escalating cyber-security threats and punitive data protection regulations, a failure to prioritise security is compromising customer data, leaving the business at risk of both fines and reputational damage. Any start-up looking to create a great app with long-term value must look at the full development requirement – and that includes rigorous cyber-security.

Whether based at Silicon Roundabout or a barn conversion in Worcestershire, the drive to create a popular app continues to inspire innovative start-ups. As app opportunities expand beyond traditional tablets and smartphones to include connected cars and virtual reality devices, funding for start-ups shows no sign of slowing.

But there is so much more to long-term success than a great idea. While there are any number of people out there who can code an app, what about the underpinning infrastructure? Where is the data going to be hosted? How is customer support going to be delivered and – in an era of escalating concerns regarding the safety of personal data – what is the security strategy?

Just consider a recently developed app designed to improve the life of people living with a terminal illness: for example, there may be sensitive information that must be safeguarded – imagine the outcry from their loved ones should information be compromised in some way.

When the vulnerability of weak and out-of-date security processes is revealed by another data breach virtually every week, no business can afford to overlook security requirements. Organisations' reputations are being damaged and with the forthcoming General Data Protection Regulation (GDPR) promising fines up to €20m or 4% of turnover – whichever is the greater – few organisations will be able to afford a lackadaisical approach to security. So while it is tempting to try to rush a new app to market without looking at the full picture, overlooking the security requirements could result in business failure before the great idea has even got off the ground.

Leverage expertise

Yet for the vast majority of start-up organisations, security remains an incredibly low priority – if it is even considered. As a result, many organisations are simply assuming that an app developer will have the skills to add on the required security solution. This is simply not the case. Can you really expect a coding expert to have the knowledge to successfully implement data encryption? Ensure firewalls are correctly deployed and updated? Or manage intrusion detection?

Robust app development requires a team with diverse skills, ranging from business analyst to technical architect; front end developers, security experts and, critically, testers. With the recommended ratio of one tester to every two developers, a successful team will require a minimum of five people. And that is where a bespoke software development company that has spent years building up the right skills can ensure that every aspect of the app development model – especially security – is addressed.

Furthermore, bespoke development specialists will follow a robust security methodology and have proven credentials by achieving security standards, such as ISO 27001 accreditation and Cyber Essentials Plus, the government-backed scheme to improve the resilience of UK business. Under GDPR, these organisations will also bear responsibility for the safety of data – it is both the data controller (owner) and processor (such as a third-party software provider) that will face the wrath of the regulator should a breach occur – and will have put in place robust processes to encrypt and manage data as a result.

Company issue

Cyber-security shouldn't just be considered for the data being stored within the apps under development, it's also something that needs to be considered by the development company itself. It is crucial that any agency commissioned to create software has its own internal-, as well as external-facing, cyber-security. This internal security is vital for protecting organisations from a variety of threats, such as past employees – who may have left to work for competitors – logging into their old employee account and pilfering confidential or innovative information.

Similarly sometimes the security risk lies at the heart of the application, within the code it's been written in. Developers want to write secure code but many aren't armed with the knowledge and tools needed to address any advanced problems. The IT skills gap in the UK has been widely commented upon and due to the lack of experts available to provide training, this knowledge gap is surprisingly common. When starting to develop their apps, organisations need to ensure they are entrusting the right developers, with the right levels of expertise and ability to create the complex and secure code they need.

Security often isn't at the forefront of the design process: it takes a back seat to functionality and feel, and while this may be understandable, it's unforgivable. To avoid pitfalls later, organisations need to communicate clearly with their development team so that they can find a way to instil the look and performance they like, without compromising on security.

Testing the boundaries

Although an app will go through rigorous testing, the best way to ascertain its level

of security is to engage with an ethical hacker. Penetration testing will expose any vulnerabilities in the system and really show the risks of what could happen should those vulnerabilities be exploited. It can also highlight any potential network availability issues and help to reduce the likelihood of unexpected downtime, or loss of accessibility. Awareness of these issues ahead of launch will help organisations maintain the trust of their users, as bad management of a cyber assault or data breach could mean stakeholders might withdraw their interaction with the app, or even the brand entirely.

Penetration testing isn't just beneficial, it's often mandatory. Many industry and legal compliance requirements dictate certain levels of testing. A well chosen penetration testing company will not only help companies adhere to these, but also provide extra accreditations.

Finding the right host

On-premise was historically thought of as a secure host: however, the evolution of cloud has now pushed it into being an outdated, time-consuming and expensive option. Even if companies can accept these disadvantages, they may not be able to come to terms with the security risk on-premise poses. Aside from the opportunities it offers to hackers and thieves, the risk of employees losing or breaking the machines on which vital data or coding is stored is enough to make on-premise a significantly less secure option.

Yet despite the increase in the use of cloud hosting, there are still some security fears around public cloud-based hosting. The word 'public' is partially to blame here as it implies that everyone and anyone can gain access. In actual fact, although a public cloud will store servers together in the racking of a datacentre, each company's information is segregated in a very secure way.

Public clouds are more secure than most organisations realise, as due to the extreme security requirements, providers will only employ the best security experts available to protect their service and reputation. Public clouds are also harder to hack than private clouds or an on-premise option, as they are continuously thwarting threats, giving them more experience and ensuring they are ready to tackle any attacks. From a technological perspective, public clouds are also updated more regularly than any other host and often for a fraction of the cost, so they offer more security and less expenditure.

Conclusion

Creating a truly secure app is a challenge for any size of business, in any location. To do so, organisations need to focus on leveraging the expertise of accredited, robust development specialists and penetration testing teams. Once the project is ready for implementation, the app needs to be contained in the right hosting environment to ensure that its security is continued.

This process may take a little extra time – and even a little more cost – but the fact is that cyber-security threats are an everyday occurrence in today's digital world. And in the rush to get an app to market, can any business really afford to short-cut security?

About the author

Nick Thompson is the owner and managing director of DCSL Software, a bespoke software development company originally established in 1994 and which he purchased four years ago.

Security challenges for cloud-based email infrastructure

Akashdeep Bhardwaj

Sam Goundar

Akashdeep Bhardwaj, Sam Goundar

Over the past few years, the recognition and acceptance of cloud-based applications has gained a lot of momentum. Commercial applications that were initially installed inside corporate on-premises server rooms are now hosted on cloud infrastructures. Software applications are provided in the form of commercial services that are accessible anytime, anywhere. Cloud-based solutions also eliminate the need for regular maintenance-related activities, unnecessary downtimes or outages, attention to back-ups or regular infrastructure upgrades.

In addition, new unified communications and other office productivity applications can also be integrated with existing cloud-based solutions. This ensures efficient, lean and effective business processes as compared to an on-premises solution.

Cloud-based email infrastructure systems such as Google's Gmail, Microsoft's Office 365 and Amazon's Simple Email Service are no exception to this cloud advantage and these solutions have also witnessed a huge increase in global usage and user base. Cloud-based email infrastructure resolves operational cost issues, revenue loss, business disruption, scalability, employee productivity and IT support complexities that are typically associated with an on-premises email server.

However, mitigating cloud-based security risks requires the service providers and corporate users to adopt a universal

approach for ensuring that the right-fit solution is in place, especially when application services used over unsecure Internet connections bring forth new threat vectors and cyber-attacks. Given the high usage of cloud applications – and more so for email applications – it is no surprise that cloud-based email solutions tend to be the primary target of cyber-attackers. The intent is to disrupt corporate email operations, which in turn causes business disruptions, financial impact and reputation loss. These attacks may even seek to acquire confidential information from email servers.

Email threats

Email infrastructure systems have to deal with security threats as mentioned below, as outlined in a SANS white paper:[1]

- Credential phishers and sender impersonations.
- Spam, ransomware and virus payload attachments.
- Typo squatting or URL hijacking via DNS exploitation.
- Internal employee data leakage and insider threats.

According to the same white paper, cyber-attackers gain access to user accounts and mailboxes in the following ways:

- Repeated brute forcing combinations of user/passwords using automated tools and keywords.
- Spoofed emails directing employees to a malicious link, enticing them to enter email IDs and passwords.
- Embedded malicious attachments in emails to allow access to the network servers or systems.
- Use of social engineering and human error by sending a direct request from a trusted source.

Limitations of email protocols

Like any cloud- or network-based service, email systems need to provide the following five services for security reasons:

- **Message confidentiality**: This promotes privacy in that the message transfer between sender and receiver is secure and no-one can read or track the message while it is transferring.
- **Message integrity**: The same message/data should arrive at the receiving end as was sent by the sender. No alteration, intentionally or accidentally, takes place during transfer.
- **Message authentication**: This ensures that the message genuinely comes from the sender or a trusted source.
- **Message non-repudiation**: This ensures that the sender should not be able to deny having sent the message.
- **Entity authentication**: This ensures the identification of the user; the user must be verified before accessing the resources and services. This is done by asking for a login ID and password.

There are several key email security protocols, each of which has limitations.

Simple Message Transfer Protocol (SMTP) helps exchange servers send out new mails regardless of the protocol being used for retrieving the emails outside the organisation. This works on port 25, 2525 or 587. Issues with SMTP include not being able to encrypt messages. The communication between SMTP servers is in plain text, so eavesdropping can take place. Also, this protocol can only send messages in NVT 7-bit ASCII format and is unsuitable for languages such as Chinese, Japanese, German or Russian which are not supported by 7-bit ASCII.

Logging in to an SMTP server using a username and password is also in plain text. Messages sent through SMTP contain information about the sending computer and software used which, when captured, could be used for malicious purposes. So SMTP lacks privacy. SMTP does not have any mechanism to authenticate the source. It also does not have functionality to check message integrity and so it is easy to send phishing attacks. SMTP does not have any mechanism to control repudiation. The messages are stored on SMTP servers as plain text. Even if you delete the message, they may reside on the servers and any back-ups for years. So anyone who can access the servers can also access or read messages easily.

Post Office Protocol version 3 (POP3) provides a mechanism to move emails from the email server to a client machine. This works in either 'keep' or 'delete' mode over port 110. Issues with POP3 include the fact that deleting an individual item does not remove it from the server. If mail is left on the server, care should be taken that there is sufficient capacity before senders encounter a bounce-back message telling them that the 'mailbox is full – try again later'. Each service provider sets its own rules as to how much email can be stored for each account. Sending an email that ultimately gets saved in the 'Sent Items' folder is available locally only, not on the server. That means that any messages sent via one device will not be accessible via any of the user's other devices. Contacts, calendar and tasks are local to the specific machine. Those items are not stored on the server regardless of what capabilities exist with a webmail interface.

Internet Mail Application Protocol version 4 (IMAP4) is similar to POP3 but far more complex and powerful. This protocol allows client applications to become email-enabled for two-way exchange of emails between client system and servers. IMAP supports message transports, directories and message store facilities. This allows email folder creation (unlike POP3), and synchronising and mirroring the email server mailbox with the client mailbox. This allows for viewing and synching the same email contents across multiple systems and devices. This works on port 143 and 993. An issue with IMAP4 is that since it is a pull protocol, like POP3, a request is sent to the mail server to access the mailbox using a username and password. These details are not encrypted before sending unless SSL is enabled. Like POP3, you must ensure that your service provider gives you sufficient capacity to store all your email items that you want to maintain on the server. Also like POP3, contacts, calendar and tasks are not handled by the IMAP protocol. This information is either stored locally when created by the email client or on the server via the webmail interface.

Exchange ActiveSync (EAS) is the protocol used to synchronise Microsoft Exchange servers, supporting contacts, calendar and tasks. There are limitations in the EAS protocol. Outlook.com 'Contact Groups' are created with the use of 'categories' whereas the same groups created in Outlook (the desktop client) are created as special contact item types with a specific

Message Class (IPM.DistList), making it compatible with all earlier versions of Outlook using the MAPI interface via the Hotmail Outlook Connector. In short, you cannot synchronise Contact Groups using an EAS Outlook.com account and Outlook 2013.

Literature survey

A secure certificate-less cryptography emailing system was proposed by Balakrishnan et al.[2] To implement public key exchange, the email system used the Domain Name System infrastructure for user authentication. When accessing the system, secure key token fingerprint authentication was used. For each email, the message payload was encrypted by the system. This involved a symmetric key that was generated from the secret value and the keys (public and private) of senders and receivers. After analysis of the proposed email system, it was found to be secure compared to standard email security models.

Unger et al compared existing messaging solutions and proposed a framework to enhance security, ease-of-adoption properties and usability.[3] The framework included commercial email solutions and security solutions from academia. This paper proposed three unique methods. First, a trust establishment approach was offered for security and privacy, but from the usability and adoption perspective this offered low performance compared to other hybrid email security options. Second, the conversation security lacks adequate security solutions for large email groups, although this worked fine for two or fewer email user groups. Finally, transport privacy, which is the trickiest issue to resolve, did not actually offer any significant performance boost.

A comprehensive design document for the Dark Internet Mail Environment (DIME) was presented by Ladar Levison.[4] This paper included elements required for successfully implementing DIME and details for protocols and message format specifications. An analysis of email security attack vectors was presented along with mitigation techniques.

Chhabra et al evaluated the architecture design and workflow of existing email infrastructures and the security protocols implemented for secure communications and their limitations.[5] The paper proposed use of email forensics as a viable process for analysing email, including the mail content, header information, transit path, sender and receiver information. This paper also proposed collecting relevant specifications as evidence against email offenders and also discussed a few common forensic investigation techniques and tools.

An analysis, presented by Fatima et al, was performed to determine the difference between X.509 and PGP certificates on usage, creation, revocation and authentication procedures.[6] An analysis highlighted the differences between the two certificate systems. The conclusion illustrated that PGP's distribution process of public keys is the biggest drawback while, in comparison, X.509 was considered more flexible and advanced. With X.509, responsibility and decision-making are equally distributed to every stakeholder, which further enhances the personal privacy and security aspects.

Afnan et al introduced various techniques to enhance the security of email systems.[7] The two main enhancements proposed concern email user identity authentication, and confidentiality and privacy during email transmission. These two enhancements vastly improved performance and achieved the required level of security.

A one-way authentication key agreement scheme was proposed by Hongfeng et al based on a multi-server architecture.[8] The paper presented proof and analysis that the proposed key agreement scheme was not only efficient and unique, but also resilient against various attacks and achieved forward security.

Mushtaq et al presented an all-purpose illustration of various cryptographic parameters and methods.[9] The paper proposed that each method and calculation was unique in its own particular terms. As per this paper, three parameters, namely private key, quantum cryptography and crypto steganography are the best methodologies for achieving a high level of security.

An email alias service called Email Cloak was proposed by Dacosta et al.[10] This service had public key encryption features that reduced the load of email encryption processes since it relied on a privacy-respecting third-party encryption system. The Email Cloak workflow involves the inbound and outbound emails of the user being automatically encrypted with the public key. This process happens before the emails are forwarded to or stored by the email system. This system has simplified key management with selective and automatic email encryption, allows for advanced deployment options and displays transparency for third-party applications. The evaluation illustrated that the overhead is sufficient for all email communications and the Email Cloak implementation was made public.

Nemavarkar et al proposed a secure, online picture-based model to remove the requirement for passwords for online email systems and files.[11] To implement this model, a novel multi-level email security design was proposed. This design implements three levels of security via example matching, pressure and cryptography.

A detailed evaluation of the inherent weakness in email infrastructure and existing methodologies was presented by Choukse et al.[12] The paper further suggested options to improve overall email infrastructure security.

Xuan et al examined the way that traditional email servers send data in plain text format over the Internet when sending across domains to other servers.[13] This vulnerability results in information disclosure and misuse risks. The authors reckoned that by applying cryptographic technologies this issue can be mitigated. They proposed an identity-based, cryptographic, independently controllable email system and compared the email systems proposing three unique solutions and provided an academic theory for securing and upgrading email systems.

Hameed et al proposed an affordable, lightweight, energy-efficient free email system infrastructure based on the Raspberry Pi.[14] Email service consumers typically utilise either free webmail options like Yahoo, Gmail or Live while corporates use hosted email services, neither of which offers full control and flexibility for the user. Email data tends to be vulnerable to unauthorised access, resulting in privacy threats. The authors implemented Pi-Mail using the Raspbian OS, Postfix message transfer agent, Clam anti-virus and SpamAssassin anti-spam.

The Pi-Mail system was found to be fully capable of providing full email services.

Bai et al conducted a study to determine how an average user thinks about, or can be made to understand, the trade-offs of using various encryption models.[15] The respondents confirmed that the security was better with the less convenient models, and also confirmed that the security of the proposed mode was appropriate for everyday purposes.

Malatras et al examined the most critical privacy and security risks in worldwide email communications.[16] A set of real-time countermeasures was proposed, based on existing standards. The authors also suggested technical recommendations to be implemented by email service providers. The results displayed enhanced security and at the same time preserved compatibility in the ecosystem.

Anuradha et al proposed email security using an Open PGP certificate in a grid framework.[17] The system implemented an email encryption standard using X.509 certificates. The issue illustrated by this paper was that after issuing the certifications, the certification authority (CA) that was certified by different organisations was appropriate for self-use certificates. However, in a distributed grid infrastructure system, this process becomes insecure. Man-in-the-middle attacks during the sending of alerts to IT teams and admins was possible. This was shown to be mitigated by the use of a framework that uses Open PGP in grid computing environments.

A literature survey on social engineering phishing and techniques used to detect such attacks was performed by Gupta et al.[18] The paper discussed various types of phishing attacks including email spoofing, tab napping and trojans and also discussed the impact on users.

Shukla et al proposed a secure, transparent email client framework to mitigate email security issues in webmail environments. Current email security involves the use of encryption for email content.[19] This approach is inconvenient and increases the size of emails. The authors illustrated the proposed solution was customisable and not integrated into any of the existing email servers.

Fowdur et al proposed an HTTPS webmail anti-spoofing system with a web-based interface.[20] It worked in real time and actively detected, monitored and controlled email spoofing. Once a spoofed message was detected, an alert was triggered. There was also an option to notify the sender and block the email. The authors claimed that most existing spam systems did not provide email users with a sufficient degree of control and information regarding spoofed attack emails.

In order to evaluate email security, virus and spam issues, Khanji et al performed a case study and presented solutions to mitigate the issues.[21] The authors configured two SMTP servers and evaluated six different scenarios. Different anti-spam and filtering techniques were also studied for reporting and analytics features that could help email administrators to better control and monitor SMTP server systems.

Pawar et al evaluated email security issues related to anti-spam filtering by using machine learning systems.[22] The authors performed an extensive security evaluation of anti-spam systems by use of pattern classifiers and analysed the performance of the email systems during spam attacks.

Instead of investigating end-user mail client security or end-to-end email encryption, Baumgaertner et al (2015)[23] analysed the cipher suites and certificates involved.[23] The authors focused on connections to providers' SMTP servers relying on transport layer security. The authors also presented recommendations to mitigate email security issues in existing email systems.

Year	Reference	Email security methodology
2016	Balakrishnan et al	Public key exchange, symmetric key encryption
2015	Unger et al	Email security framework
2015	Ladar Levison	Darknet email security
2015	Chhabra et al	Email forensic investigation process
2015	Fatima et al	Public key exchange using PGP
2015	Afnan et al	Authentication of user & email privacy
2015	Hongfeng et al	Authenticated one-way key agreement
2015	Mushtaq et al	Private key, quantum cryptography, crypto steganography
2014	Dacosta et al	Public key encryption
2015	Nemavarkar et al	Visual cryptography
2012	Choukse et al	Literature survey
2016	Xuan et al	Identity-based cryptography
2015	Hameed et al	Lightweight email system with anti-spam, anti-virus features
2017	Bai et al	Evaluation survey
2016	Anuradha et al	PGP certificates
2016	Gupta et al	Literature survey
2016	Shukla et al	Transparent email security framework
2016	Fowdur et al	HTTPS-based anti-spoofing design
2016	Khanji et al	Literature survey and proposed secure design
2015	Pawar et al	Evaluation survey
2015	Baumgaertner et al	Certificate related analysis

Table 1: Summary of email security research papers.

Research performed

We conducted two surveys: the first involved detailed evaluation of email service providers (ESPs) regarding security features provided to users; the second survey involved 500 users and their email security practices to determine user confidence levels regarding email security.

Email service providers

The authors analysed 12 commercial email service providers to evaluate security features and test the effectiveness of their security protocols against spoofed emails. The investigation was done by initially creating test user accounts and then verifying the security and usability service options offered.

In order to analyse the spam and spoofing features, the test user email accounts

Email services	Accepts spoofed mail		Displays name in email listing	Classifies spoofed mails as SPAM	
	Username only	Username & domain		Username only	Username & domain
Office 365	Yes	Yes	Yes	Yes	Yes
Yahoo Mail	Yes	Yes	No	Yes	Yes
Gmail.com	Yes	Yes	Yes	Yes	Yes
Inbox.com	Yes	Yes	Yes	No	No
Mail.com	Yes	No	Yes	No	No
Live.com	Yes	No	Yes	Yes	No
Zoho Mail	Yes	Yes	No	No	Yes
Outlook.com	Yes	Yes	No	No	No
Mail.com	Yes	Yes	No	No	No
GMX Mail	Yes	Yes	Yes	No	No
Fast Mail	Yes	No	No	No	No
Hush Mail	Yes	No	No	No	No

Table 2: Treatment of spoofed emails by commercial email service providers.

were subjected to spoofed emails from domains that employ legacy security standards or do not follow any security standard – ie, they were not compliant with Domain Key Identified Mail (DKIM) or Sender Policy Framework (SPF). Typically, all email services offered a bulk email option that is theoretically capable of determining the spoofed email Sender ID along with the return path. Most email servers continued to accept spoofed emails, either in username only or in both username and from domains that do not use anti-spoofing protocols, although email header signatures did clearly indicate the email had been sent from a domain that did not follow any compatible security protocol standard.

Service provider results

Positive aspects regarding the email systems were:

- The email service providers we studied have security protocols in place.
- Before delivery of the spoofed email, those email domains that are DKIM-complaint are able to correct the 'From' address field in emails while those domains that follow SPF and Sender ID do not accept spoofed emails at all.
- Email service providers do respond and provide security information and analysis if requested by users.
- Use of SSL and HTTPS for accessing emails through webmail programs is in place.
- Email service providers provided relevant security options for: analysing headers; built-in custom signature; vocational response; and built-in spam protection with customisable blacklisting of sender emails.
- However, the email systems also fell short on a number of security issues:
- Customisable message filtering or ability to add filtering rules by the user.
- Lack of detailed security tutorials on the email portals.
- Lack of information about current attacks or general security information to improve user awareness.
- Lack of best practices for email usage and security.
- Lack of enhanced security features such as detailed header analysis.
- Emails may present human friendly names even when forged, misleading and from spoofed sender IDs.

User email practices

The provider survey was validated by conducting another study on email users regarding email security practices and security protocol knowledge. About 500 respondents using commercial email service accounts were evaluated.

Survey results

The survey revealed some interesting facts. Most of the users access emails via webmail interfaces. The 'anytime, anywhere' access is the main reason, along with the fact that they are free.

The expectation is that the service provider caters for email security. User awareness and knowledge regarding malware, spam or ransomware along with filtering errors was very high.

Very few users actually kept their anti-malware or anti-spam systems updated, nor did they use encryption for email. Header analysis for tracking the email source is offered by the email systems but only a handful of users knew about or utilised the feature. Few users are aware of spoofing although some have experienced it. Some users are aware of security protocols such as DKIM, SPF/Sender ID and S/MIME but very few are aware of all email headers.

User awareness

We also determined the confidence levels of users regarding email security. The respondents were asked if the email service providers made them aware of email security and privacy issues and also if the service provides training on the use of security protocols and header analysis features. The results of their confidence in email systems in terms of the security and usability of security protocols before and after training are presented in Table 4.

Initially very few users knew or utilised the encryption and authentication protocols such as S/MIME or PGP. The survey also revealed that most users have limited knowledge of email security and don't use existing security protocols. User confidence, which is initially poor, tends to rise after simple security orientation. The results of training were encouraging as the confidence level of users on average improved considerably with each parameter.

Most users understand that information in emails is not only insecure but also that the delivery of email is not guaranteed. The usability of security protocols and options is limited.

Advantages of cloud-based solutions

Cloud-based Email solutions such as Office 365 or Google Apps, along with other cloud-based productivity solutions, are transforming the way IT depart-

ments deliver emails, apps and services to their users and adoption of these solutions is continuing to grow.

We compared the security advantages of Office 365 with an in-house hosted email system. In addition to geographic site resilience, cloud providers offer enhanced security in the form of automatic network encryption, multi-layered anti-spam and anti-malware protection and a message protection policy. Secure SMTP, PGP, SPF/Sender ID, S/MIME and DKIM ensure the secrecy and integrity of emails.

Figure 1 describes automatic network encryption for the Office 365 email flow. First, Office Message Encryption (OME) runs a service on the Exchange Azure server which allows sending encrypted emails inside and outside an organisation using Office 365. Second, the Information Rights Management (IRM) service applies usage restrictions to email messages to prevent sensitive information from being printed, copied or forwarded in an unauthorised manner. Third, certificate-based S/MIME encryption solutions allows the sending of encrypted digital signatures for emails, addressing sender authentication.

Message Protection provides for messaging policy and compliance to manage email data and provide audit reports as well as having message flow transport rules for organisation-specific email policies in the form of conditions, exceptions, actions and properties. Email Connectors provide control over routing and email flow; this also allows integration of the cloud server with third-party security systems for enhanced encryption and data leak prevention.

Anti-spam and anti-malware protection offers multiple scan engines and highly accurate spam filtering servers. These offer multiple layers of protection for content filtering based on internal or blacklisted IP lists, protocol filtering for individual mailbox users and content filtering based on words and phrases scanned from an internal listing as well as an automated analysis scan. Figure 2 illustrates the Online Exchange email spam process for inbound emails and attachments, passed through multiple filtering and scanners before being routed to mailbox servers and finally reaching the intended user mailbox.

Evaluation parameters	Results
Email users' perspective of security practices	
Use webmail programs	85%
Installed anti-spam and anti-malware	48%
Keep anti-spam or anti-malware updated	25%
Use encryption/authentication protocols (S/MIME, PGP)	15%
Header analysis for authentication	>1%

Evaluation Parameters	Results
Email user knowledge awareness	
Virus, spam, ransomware	88%
Filtering classification errors	55%
Spoofed emails	21%
Transparent security protocols (SPF, DKIM)	19%
Non-transparent security protocols (S/MIME, PGP)	25%
Infrequently used email headers	12%
Email delivery over Internet is not secure	82%
Email delivery to destination is not guaranteed	76%

Table 3. User email practice and awareness of security protocols.

Awareness/confidence level	Initially on joining	After orientation
Highly secure	23%	85%
Mildly secure	31%	82%
Low security	41%	91%
Use S/MIME and PGP	15%	88%
Utilise SPF and DKM	9%	35%
Utilise header analysis	2%	15%

Table 4. User confidence in email communication.

Conclusion

Add-on email security protocols use encryption, PKI-based cryptographic techniques, IP address verification and DNS-based domain validation for providing security against spoofing and other email threats. However, no protocol independently provides all the required security features. In addition, domains that are not compatible with security protocols continue to pose security threats by allowing the transmission of spoofed emails that are not detected by receiving domains using security protocols.

Spoofed emails from some domains that do not support add-on security protocols can be detected by analysing the trace header field but this is not currently done by receiving domains. Email users are losing confidence in email security because they have insufficient awareness of security protocols and only some users employ these capabilities to secure their emails. There is a need to undertake a major education campaign to raise awareness among email users

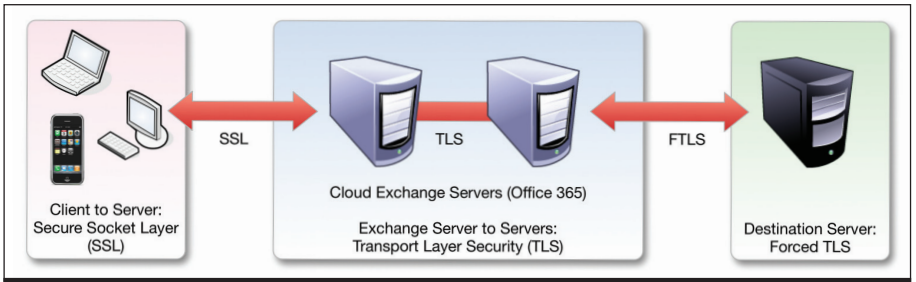


Figure 1: Automatic network encryption.

about security issues and to train them in using security protocols and procedures.

Recommendations

An ideal email security solution needs to integrate most if not all of the following:

- Multi-factor authentication for accessing email when outside the office.
- Network- and application-level DDoS protection.
- Automated screening of each outbound email to prevent data loss and proactively eliminate human error.
- Protection of business confidential data – by classifying attachments, documents or email body information as sensitive wherever appropriate.
- Send alerts to the security team and/or management stakeholders requiring acknowledgement before sending an outgoing email message that has any sensitive information and data.
- The ability to handle compliance needs regardless of user platform or email device.
- Automated key management – including key generation, rotation, discovery and validation.
- Encrypt and sign email messages to ensure confidentially.
- Ensure the email infrastructure is resilient to advanced persistent threats (APTs).
- Minimise the exposure of email metadata.

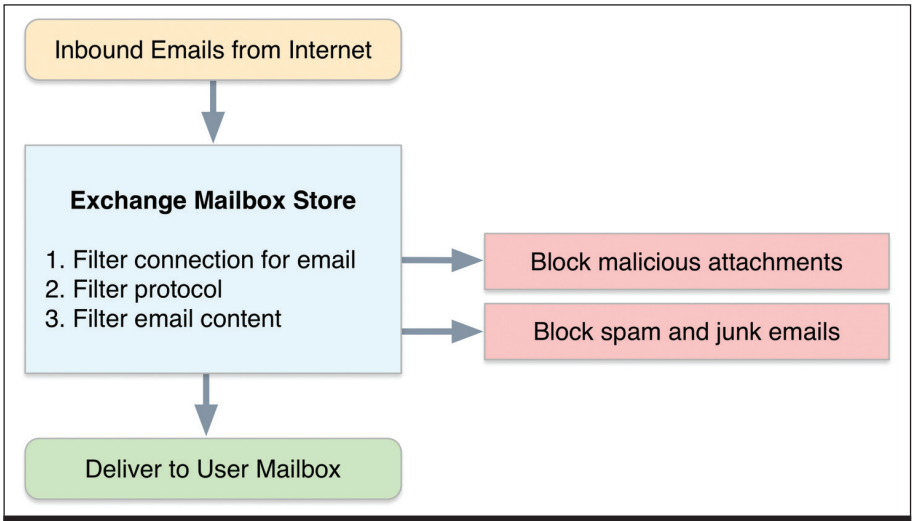


Figure 2: Spam and malware scan flow.

Advantages	Disadvantages
Full control of every activity or configuration as the email platform is self-owned, including mailbox size, webmail, ActiveSync, public folders transport policy rules.	Security, reliability and uptime need constant monitoring due to new threat vectors. There is a constant need to ensure training and skills for the IT team as it needs to resolve any issues.
Flexibility for customising third-party integrations.	Costs associated with hardware upgrading and licensing.
Full control over email data and back-up.	In case of disaster and no back-up contingency plan, all data and hardware can be lost.

Table 5: On-premises email systems.

Advantages	Disadvantages
Scalability to cater to a large number of users; 50GB mailbox size without spending extra on licences or hardware.	Lack of root or administrative level control of hosted provider's servers.
Variety of subscription plans for mailbox, unified communication (Skype, Lync, OCS) and Office Suite (Word, Excel, Power Point) as well as Sharepoint, OneDrive, Sway.	Rolling back to an on-premises option is uncertain once the system has moved to the cloud.
Reduced risk of data loss as back-up and availability is the provider's responsibility.	Migrating from one service provider to another can be difficult.
Online infrastructure offers the latest, patched solutions with options for adding enhancements and innovations to increase user productivity.	Lack of flexibility to integrate with third-party applications or legacy systems.

Table 6: Cloud-based email systems.

About the authors

Akashdeep Bhardwaj is a PhD research scholar from the University of Petroleum & Energy Studies (UPES), Dehradun, India. He received a post-graduate diploma in management and a degree in computer science in 1994. He has over 22 years experience in IT operations and information security. He is trained and certified in compliance audits, information security, ethical hacking and Microsoft, Cisco and VMware technologies.

Sam Goundar has been teaching IT, IS, MIS and CS over the past 20 years at several universities in a number of countries at all levels. As a researcher, apart from cloud computing and mobile cloud computing, he also researches educational technology, MOOCs, smart cities, artificial intelligence, ICT in climate change, ICT devices in the classroom, using mobile devices in education, e-government, ICT for disaster management, deregulation and control in international education, quality assurance in international education and technical/vocational education. He has published on all these topics. He is a member of the IEEE Technical Society and a panellist with the IEEE Spectrum for Emerging Technologies.

References

1. 'Email Security Threats'. SANS Institute, 2016. Accessed May 2017. sans.org/reading-room/whitepapers/email/email-security-threats-1540.
2. Balakrishnan, S; Jagathy, R. 'Practical implementation of a secure email system using certificateless cryptography and Domain Name System'. International Journal of Network Security, Feb 2017 Vol.18, Issue 1, pp.99-107.
3. Unger, N; Bonneau, J; Dechand, S; Fahl, S; Goldberg, I; Henning, P; Smith, M. 'SoK: Secure Messaging'. IEEE Symposium on Security and

Privacy, Mar 2015, doi: 10.1109/SP.2015.22.
4. Levison, Ladar. 'Dark Internet Mail Environment: Architecture and Specifications'. Darkmail.info. Accessed May 2017. darkmail.info/downloads/dark-Internet-mail-environment-december-2014.pdf.
5. Chhabra, G; Bajwa, D. 'Review of email system, security protocols and email forensics'. International Journal of Computer Science & Communication Networks (IJCSCN), 2015, Vol.5, Issue 3, pp.201-211.
6. Fatima, S; Ahmad, S; Siddiqui, S. 'X.509 and PGP Public Key Infrastructure methods: A critical review'. International Journal of Computer Science and Network Security (IJCSNS), 2015, Vol.15, Issue 5, pp.55-59.
7. Afnan, S; Babrahem, E; Alharbi, T; Aisha, M. Alshiky, S. 'Study of the Security Enhancements in various Email System'. Journal of Information Security. 2015, Vol.6, Issue 2, pp.1-11. doi: 10.4236/jis.2015.61001.
8. Hongfeng, Z; Yifeng, Z; Yan, Z. 'A one-way authentication key agreement scheme with user anonymity based on chaotic maps towards multi-server architecture'. Journal of Information Hiding and Multimedia Signal Processing, 2015, Vol.6, Issue 2.
9. Mushtaq, S; Rafiq, I; Sirshar, M. 'Quality analysis of network security using cryptographic techniques'. International Journal of Computer and Communication System Engineering (IJCCSE), 2015, Vol.2, Issue 2, pp.246-254.
10. Dacosta, I; Put, I, Decker, B. 'Email Cloak: A practical and flexible approach to improve email privacy'. 9th International Conference on Availability, Reliability and Security, 2015.
11. Nemavarkar, A; Chakravarti, R. 'A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography'. IEEE International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, doi: 10.1109/IC4.2015.7375661.
12. Choukse, D; Singh, U; Laddhani, L; Shahapurkar, R. 'Designing secure email infrastructure'. 9th IEEE International Conference on Wireless and Optical Communications (WOCN), Indore, 2012, doi: 10.1109/WOCN.2012.6335534.
13. Bai, W; Kim, D; Namara, M; Qian, Y; Kelly, P; Mazuurek, M. 'Balancing security and usability in encrypted email'. IEEE Internet Computing, 2017, Vol.21, Issue 3, pp.30-38. doi: 10.1109/MIC.2017.57.
14. Malatras, A; Coisel, I; Sanchez, I. 'Technical recommendations for improving security of email communications'. 39th IEEE International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2015, doi: 10.1109/MIPRO.2016.7522355.
15. Xuan, J; Wang, D; Li, Z; Zhang, S. 'Design of Secure and Independent controllable email system based on Identity-Based Cryptography'. 2nd IEEE International Conference on Computer and Communications (ICCC), Chendu, China, 2015, doi: 10.1109/CompComm.2016.7924696.
16. Hameed, S; Asif, M; Khan, F. 'PiMail: Affordable, lightweight and energy-efficient private email infrastructure'. 11th IEEE International Conference on Innovations in Information Technology (IIT), Dubai, UAE, 2015, doi: 10.1109/INNOVATIONS.2015.7381561.
17. Bai, W; Kim, D; Namara, M. 'Balancing security and usability in encrypted email'. IEEE Internet Computing. 2017, Vol.21, (3), pp.30-38. doi: 10.1109/MIC.2017.57.
18. Malatras, A; Coisel, I; Sanchez, I. 'Technical recommendations for improving security of email communications'. 39th IEEE International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Optija, Croatia, 2016, doi: 10.1109/MIPRO.2016.7522355.
19. Anuradha, A; Chopra, A. 'Securing and preventing man in middle attack in grid using open Pretty Good Privacy (PGP)'. 4th IEEE International Conference on Parallel, Distributed and Grid Computing (PDGC), Waknaghat, India, 2016, doi: 10.1109/PDGC.2016.7913249.
20. Gupta, S; Singhal, A; Kapoor, A. 'A literature survey on social engineering attacks: phishing attack'. IEEE International Conference on Computing, Communication and Automation (ICCCA), Noida, India, 2016, doi: 10.1109/CCAA.2016.7813778.
21. Shukla, R; Prakash, O; Phanibhusan, P. 'Open PGP based secure web email'. Third IEEE International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016.
22. Fowdur, T; Veerasoo, L. 'An email application with active spoof monitoring and control'. IEEE International Conference on Computer Communication and Informatics (ICCC), Coimbatore, India, 2016, doi: 10.1109/ICCCI.2016.7480002.
23. Khanji, S; Jabir, R; Ahmed, L; Afridi, O; Said, H. 'Evaluation of Linux SMTP server security aspects – a case study'. 7th IEEE International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2016, doi: 10.1109/IACS.2016.7476120.
24. Pawar, K; Patil, M. 'Pattern classification under attack on Spam Filtering'. IEEE International Conference on Research in Computational Intelligence and Communication Network (ICRCICN), Kolkata, India, 2016, doi: 10.1109/ICRCICN.2015.7434235.
25. Baumgaertner, L; Hochst, J; Leinweber, M; Freisleben, B. 'How to Misuse SMTP over TLS: a study of the (in)security of email server communication'. IEEE Symposium on Parallel and Distributed Processing with Applications, Helsinki, Finland, 2016, doi: 10.1109/Trustcom.2015.386.

Going critical: attacks against national infrastructure

Steve Mansfield-Devine

Steve Mansfield-Devine, editor, Network Security

There appears to be a dawning realisation that much of the infrastructure on which we all depend, such as the power grid that provides us with electricity, is woefully vulnerable to hackers. Over the past few years there have been repeated warnings – and a few successful attacks. It's not that these dangers were unknown to specialists in the field: but as Edgard Capdevielle, CEO of Nozomi Networks, points out in this interview, both the scale and frequency of these attacks have ramped up and the true scale of the threat to industrial control system (ICS) solutions is finally being recognised.

"Attacks to critical infrastructure have changed dramatically in the past three to four years," says Capdevielle. "This issue was brought into the mainstream conversation in 2010 when Stuxnet became famous when it was able to cross into Iran's nuclear infrastructure."[1]

Even after that watershed moment, though, the security issues of critical national infrastructure (CNI) failed to make much of an impact on governments and commercial organisations. In fact, Capdevielle says, the level of awareness and activity from a cyber-security perspective was so low that there really wasn't a significant market for security firms operating in this field. And he puts that down to two reasons.

"One factor was that it was nation states attacking each other," he says. "The second is that the frequency of the attacks was low. They would happen about once a year. So if you're in an enterprise, it's very hard to say that you need to create a budget to defend yourself against a nation-state attack that of course has no limits, and that could happen maybe once a year, but maybe not."

Edgard Capdevielle has an extensive background in cyber-security and the industrial arena. As CEO of Nozomi Networks, he focuses on the cyber-security challenges facing infrastructure operators around the globe and the role that technology innovation is playing to protect critical systems from escalating threats. He is often invited to share his perspective in panel discussions and as a keynote speaker. Prior to joining Nozomi Networks, Capdevielle held positions with Imperva, Data Domain and EMC. He has an MBA from the University of California at Berkeley and a bachelor's degree in Computer Science and Electrical Engineering from Vanderbilt University.

Rising levels

The most notable change in the past few years, says Capdevielle, is the frequency of attacks. "In the US, for example, the Department of Homeland Security is the one tracking self-reported attacks on industrial control networks supporting critical infrastructure and they reported that in 2015 there were almost 300 self-reported attacks. As you know, self-reported figures are vastly under-reported, so it's probably three or four times that number. So that means that we've gone from once a year to multiple times per day."

Governments are still behind many of the attacks, especially the ones that hit the headlines. Ukraine, for instance, has twice suffered major electricity blackouts as the result of attacks commonly believed to have originated from Russia and with the backing, if not direct involvement, of the Kremlin (see box).

Another change has been in the nature of the attacks – what Capdevielle refers to as the 'use cases'. Cyber-attacks against CNI aren't just for governments anymore.

"We're talking about a multiplicity of use cases," he says. "Nation-state attacks are the ones that make the news. The other use cases are not as well known because they may not be public. The nature of the attacks is now more 'traditional', corresponding to what you would see on the IT side of the house – you see insiders being compromised, you see malicious insiders, you see profit-oriented or ransomware use cases and so forth."

Becoming critical

Technology has woven its way into the fabric of our lives and there are few businesses that aren't dependent on it in some way. So is there a problem that more computers are now running processes that could be classed as 'critical'? A lot depends on how you define things, says Capdevielle.

"When you say critical infrastructure, a lot of people translate that to mean industrial control networks, and industrial control networks have a very specific application towards oil and gas, electric grids, transportation, mining, pharmaceuticals and so on," he says. "Industrial control networks power things that move – physical processes. So that's the technical term that differentiates itself from the traditional IT. You have traditional IT on one side and industrial control networks on the other side – it's very binary. When you move away from the technical definition into more of a business or mainstream definition that is not necessarily technical, then critical infrastructure takes on a whole new meaning, because it may include banking, voting machines for elections and other things that do not tra-

Manufacturing under attack

The most recent 'Threat Landscape for Industrial Automation Systems' report from Kaspersky Labs, covering the first half of 2017, shows sustained attacks against industrial control system (ICS) solutions, with manufacturing being the most heavily hit.

Of the ICS solutions that Kaspersky monitors (numbering in the tens of thousands) more than a third (37.6%) came under attack. The three countries that saw the most problems were Vietnam, Algeria and Morocco, where the level of attacks has remained steady. However, in China there was a slight increase. In about a fifth of cases, the attacks that were blocked were attempts at malware infections or connections to known malicious or phishing websites. Kaspersky ascribes the prevalence of this issue in ICS contexts as being due to the connections between business and operational networks within industrial organisations.

Ransomware has also proven to be a problem: 0.5% of computers within the IT infrastructure of these organisations were affected by this form of malware, impacting firms in 63 countries. Several ransomware families featured in the top 10 list of malware.

The report is available here: http://bit.ly/2hnQAOv.

ditionally use industrial control networks, they use regular IT networks. But because they're critical to the company, the person or the country, they're labelled as critical. We need to clarify what we mean by critical, because to a technical person it means it uses industrial control networks, and to a politician or the average person, it may mean it's critical to the country."

Less isolated

There was a time when most, if not all, ICS solutions were isolated. They used proprietary protocols (and many still do) and networks. Viewed from the Internet, they were effectively 'air-gapped' and unreachable. But in terms of security, Capdevielle characterises air-gapping as a "failed strategy".

"The historical reasons that air-gapping used to work is that industrial control networks adopted common technology standards late in life," he says. "While traditional networks adopted the TCP/IP Ethernet standard 15 or 20 years ago, industrial control networks adopted the standard only five to seven years ago. Before that they were copper-to-copper connections, or highly proprietary networks and isolation played well – it works in your favour. But as soon as you touch the Ethernet TCP/IP stack then the opposite happens. You have now a standard network – a standard switch, a standard set of low-level protocols – and you're speaking the same language, you can get from one side to the other pretty easily. And Ethernet has an almost gravitational force wanting to connect. So now air-gapping is really not a viable alternative."

There are multiple reasons for the adoption of these standards, such as the desirability of being able to manage the whole of your infrastructure – both the industrial, operational side and your business systems – with a single set of tools and solutions. So it has a lot to do with convenience. Organisations have also installed solutions such as remote telemetry and management over TCP/IP networks that often traverse the Internet.

Alas, says Capdevielle, during all this change and development, "security has always been an afterthought". And for a long while that didn't matter so much. Because the ICS protocols and solutions were so obscure, there were few attackers with the knowledge and skills to compromise them. But that's changing too.

"Before this surge of automation and digitalisation, it didn't really make sense to create attacks against that infrastructure because it was hard," says Capdevielle. "But now it's in the limelight, you're going to have a lot of attacks happening in this space."

Linking ICS solutions to business systems, explains Capdevielle, exposes critical systems to all the vulnerabilities that computer networks are heir to – from ransomware through all varieties of malware to malicious insiders. In a business setting, the latter might include disgruntled employees taking your client database with them when they leave. In an ICS context, says Capdevielle, "it could be significant damage. It could be damage to the equip-

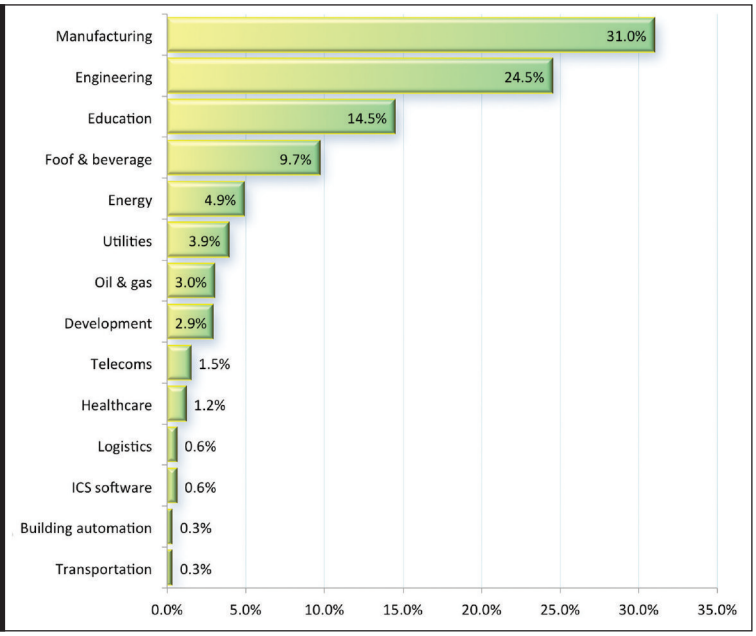
Power down in Ukraine

In December 2016, around a fifth of Kiev was plunged into darkness. Hackers had targeted Supervisory Control and Data Acquisition (SCADA) systems belonging to the nation's electricity grid.[8] The blame was levelled at the Fancy Bear group, which has carried out numerous hacking attacks against targets considered to be in conflict with the interests of the Russian Government.

Researchers at ESET claimed that the attack could have been a large-scale test of a piece of malware they dubbed 'Industroyer'.[9]

The software, the firm says, is capable of controlling electricity substation switches and circuit breakers directly. The malware is also capable of data wiping and its modular design means it can be repurposed for a wide range of attacks against critical national infrastructure.

It wasn't the first time Ukraine's power grids had been knocked offline. A year earlier, almost to the day, an engineer at a control centre that manages the electricity grid for a large part of Western Ukraine, witnessed unusual activity on a screen.[10] Someone had taken control of the system and was clicking on buttons to trip circuit breakers and take sub-stations offline. The attacker logged out the engineer and changed his password. At the same time, there were attacks in progress on two other power stations. Some 30 substations were taken offline and back-up power supplies disabled. Around 230,000 people were left without electricity for up to six hours. Even after power was restored there were problems. The attackers had overwritten firmware on serial-to-Ethernet converters, making some breakers impossible to control remotely.



Attacks on organisations using industrial control systems, by sector. Source: Kaspersky Lab.

ment, damage to the physical process, damage to the environment. We have seen quite a few of those cases."

Readiness level

The question then becomes, are we ready for these attacks? In August 2017, the US National Infrastructure Advisory Council, which advises the US President, warned that the nation was not prepared to face an attack on its power grid. Its report stated that: "There is a narrow and fleeting window of opportunity before a watershed, 9/11-level cyber-attack to organise effectively and take bold action."[2] It recommended the creation of separate communications networks for critical systems and the declassification of threat information that could be shared among the firms responsible for running the infrastructure.

In the UK, a survey carried out by security firm Corero Network Security using Freedom of Information requests suggested that many organisations – perhaps over a third – providing critical services had not even completed basic security initiatives.[3] The 338 organisations contacted (of which 163 responded) included fire and rescue services, police forces, ambulance trusts, NHS trusts, energy suppliers and transport organisations. Of the respondents, 39% had not completed the UK Government's '10 Steps' programme and this figure rose to 58% among NHS Trusts.[4] Many organisations refused to reply on security grounds, raising the suspicion that the true figure may be much higher.

A month before Corero's report came out, the UK's National Cyber Security Centre issued a warning that hackers may already be exploiting some of these weaknesses. In a report sent out to selected organisations and subsequently leaked to Motherboard, it stated: "The NCSC is aware of connections from multiple UK IP addresses to infrastructure associated with advanced state-sponsored hostile threat actors, who are known to target the energy and manufacturing sectors."[5] Engineering and water sector companies as well as others using industrial control systems are also coming under attack, the report claimed and the hackers may have already scored some successes. "NCSC believes that due to the use of widespread targeting by the attackers, a number of Industrial Control System engineering and services organisations are likely to have been compromised," the report said. And even earlier in the year, a report issued by the US Department of Homeland Security and the Federal Bureau of Investigation said that hackers had been penetrating the networks of energy companies, including those running nuclear power stations.[6]

Poor security

There is a big question mark over whether some critical infrastructure organisations are up to the task of protecting themselves.

"Security is absolutely not up to scratch," says Capdevielle. "Governments and the military bodies are trying to bring organisations up to speed, but of course they themselves move fairly slowly. Some modern companies are advancing quickly and in some geographical locations they move faster than others. The Middle East is fairly innovative and advanced when it comes to cyber-security."

Organisations in all sectors have had to face the new realities of cyber insecurities and many have been found wanting. So what is it about some critical infrastructure businesses, such as electricity generation and distribution, that seems to have made them worse than the average business? Capdevielle points again to the fact that, on the operational technology (OT) side of the organisation, they have only recently adopted the kinds of technologies (such as TCP/IP) that most firms have used for decades. And now they're linking OT and IT elements of their networks. But there's also the fact that, given the historically low level of cyber-attacks, budget just hasn't been assigned to addressing these issues. "A lot of things have changed," says Capdevielle, "but unfortunately the security posture hasn't changed."

Why now?

The increase in attacks against critical infrastructure has a number of causes, Capdevielle believes. First is the aforementioned increase in the number of systems with Internet or TCP/IP connections. However, there has also been a shift in the kinds of skills out there.

"Five to seven years ago, if you wanted to attack an industrial control network, assuming that you had access to it, it required a lot of skill sets and knowledge around industrial control networks," explains Capdevielle. "Nowadays, starting with Stuxnet and all its derivatives, we can see that the toolsets that are available to these malicious actors have increased dramatically and you don't need to be an expert anymore. You almost don't need to be very good at all, because the toolset is so good – it has levelled the playing field for the bad guys."

Responding to the threat

As many of the new threats stem from the adoption of standard business technologies, it would be tempting to assume that standard security solutions would be the answer. However, Capdevielle doesn't think it's that easy.

"Security has to be different because the processes are different," he says. "Traditional security – such as firewalls and intrusion detection systems – that work well in IT do not work well in industrial control networks. This is because even though they have some of the same underlying protocols – like TCP/IP and Ethernet – the upper layers of the stack, the industrial protocols, are very different."

Critical infrastructure organisations need to seek out specialised solutions and the incentive to do so is certainly there – and for a couple of reasons. One is that they are waking up to the new reality of attacks that can not only take down facilities on which a nation depends but can also threaten the commercial viability of the organisation. And the other is that their arms are being twisted.

"Regulation is playing an effective role," says Capdevielle. "It's either changing or being more heavily enforced. In the US, for example, for the electrical community we have NERC CIP [North American Electric Reliability Corporation Critical Infrastructure Protection] which is now being used more actively and you have fines and fees associated with non-compliance."[7]

Regulations cover a wide range of subjects, from technical requirements, including the monitoring of networks, to communications procedures. But is it enough? Where does Capdevielle think the regulations are lacking?

"We need more regulation and more enforcement associated with the cybersecurity requirements," he says.

Into the future

So are critical infrastructure organisations heading in the right direction? Are we ever going to get to the levels of security we need?

"We are going to get there," reckons Capdevielle. "I'm fairly optimistic. It will be organic, proactive or reactive. Organic – it's going to happen because it's better. A lot of security solutions provide better operational visibility, so there are benefits that are native to these type of solutions. Customers will eventually adopt them for their own benefit. The proactive angle is people trying to follow regulations and staying ahead of the game, because they're seeing some of their neighbours being affected by negative impacts. And then reactive, of course, is that a lot of us in this industry think that, sooner or later, you will have an equivalent to a 9/11 situation – a highly publicised, highly impactful industrial attack. When that happens, this market will accelerate dramatically."

About the author

Steve Mansfield-Devine is a freelance journalist specialising in information security. He is the editor of Network Security *and its sister publication* Computer Fraud & Security. *He also blogs and podcasts on infosecurity issues at Contrarisk.com.*

References

1. 'Stuxnet'. Wikipedia. Accessed Oct 2017. https://en.wikipedia.org/wiki/Stuxnet.
2. 'Securing Cyber Assets: Addressing urgent cyber threats to critical infrastructure'. The President's National Infrastructure Advisory Council, Aug 2017. Accessed Oct 2017. www.dhs.gov/sites/default/files/publications/niac-cyber-study-draft-report-08-15-17-508.pdf.
3. Leyden, John. 'UK infrastructure failing to meet the most basic cybersecurity standards'. The Register, 29 Aug 2017. Accessed Oct 2017. https://www.theregister.co.uk/2017/08/29/critical_national_infrastructure_cybersecurity/.
4. '10 Steps to Cyber Security'. National Cyber Security Centre. Accessed Oct 2017. https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
5. Cox, Joseph. 'GCHQ Says Hackers Have Likely Compromised UK Energy Sector Targets'. Motherboard, 17 Jul 2017. Accessed Oct 2017. https://motherboard.vice.com/en_us/article/9kwg4a/gchq-says-hackers-have-likely-compromised-uk-energy-sector-targets.
6. Perlroth, Nicole. 'Hackers are targeting nuclear facilities, Homeland Security Dept and FBI say'. New York Times, 6 Jul 2017. Accessed Oct 2017. www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?mcubz=0.
7. 'CIP Standards'. NERC. Accessed Oct 2017. www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.
8. Condliffe, Jamie. 'Ukraine's power grid gets hacked again, a worrying sign for infrastructure attacks'. MIT Technology Review, 22 Dec 2016. Accessed Oct 2017. www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.
9. Cherepanov, Anton; Lipovsky, Robert. 'Industroyer: Biggest threat to industrial control systems since Stuxnet'. WeLiveSecurity, ESET, 12 Jun 2017. Accessed Oct 2017. www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/.
10. Zetter, Kim. 'Inside the cunning, unprecedented hack of Ukraine's power grid'. Wired, 3 Mar 2016. Accessed Oct 2017. www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

The Firewall

BYOE: New kid on the block

Colin Tankard, Digital Pathways

The cloud has opened up incredible opportunities and efficiencies for businesses. However, with these opportunities there is also an increase in security risks. How can you be sure your data is safe in the cloud?

Traditional ways of protecting data, such as passwords, firewalls and other defensive strategies are no longer enough. For greater protection, encryption protects your data from being accessed by anyone without the corresponding key.

Cloud service and storage providers have been keen to demonstrate their commitment to securing their customers' data. This is why many offer cloud encryption as part of their service.

However, it is not just news of major breaches that have made companies think again about entrusting their cloud provider to manage their data security. Regulations that require a closer control over who can see the data and where it resides, plus national defence rules such as the Patriot Act, which could require a service provider to hand over data without notice to the data owner, have all had an effect. Whether the data is encrypted or not, the service provider would have to hand over the keys, thus removing any value provided by the encryption.

This is one of the reasons 'bring your own encryption (BYOE) – aka 'bring your own key' (BYOK) – has become increasingly popular. The concept is that you manage your own keys. You decide on their strength and how frequently they are used. The data sent to your cloud service provider is encrypted either before the provider receives it or at the point of storing in the cloud. Thus the provider cannot read the content as it does not have the keys to unlock it and, if ordered to hand the data to a government organisation, the data would remain encrypted as the provider does not have the keys to hand over.

Keys are centrally managed either by the data owner or a third-party key management specialist. All levels of controls can be applied dependent on the organisation's needs. An example is key rotation, a requirement for many data protection regulations, where the encryption key needs to be changed regularly. This is complex in itself and often not an option with cloud providers, but is compounded when the original key needs to be stored in the event of an old back-up needing to be retrieved. This is almost impossible to achieve without a good key management solution, not something most cloud providers think of.

Another advantage to BYOE is that the solution can work across all cloud providers, thus eliminating point solutions, possible weak encryption technology and the threat of keys being lost. Furthermore the solution is not limited to a type of platform, so data access from a PC or smart device can be achieved through the same system, with keys being shared seamlessly.

Data also needs to be protected outside of the cloud and BYOE can be used here too. Encryption can be applied and managed to data on-premise in servers, virtualised environments, remote locations or even third-party organisations with which the organisation wishes to share information. BOYE is truly versatile and quick to deploy and remove.

Managing your own keys comes with a significant increase in responsibility. You must not lose your key, or else you won't be able to access your data! But, the flexibility it brings in leveraging great cloud services, without the need to compromise data encryption, is invaluable. Plus, it ensures your organisation meets one of the most common compliance requirements – encrypting all data.

EVENTS CALENDAR

2 December 2017
B-Sides Cape Town
Cape Town, South Africa
www.bsidescapetown.co.za

4–7 December 2017
Black Hat Europe
London, UK
www.blackhat.com

6–7 December 2017
Cyber Security Indonesia
Jakarta, Indonesia
www.cybersecurityindo.com

6–8 December 2017
Botconf
Montpellier, France
www.botconf.eu

8–10 December 2017
International Conference on Digital Security and Forensics
Thessaloniki, Greece
http://bit.ly/2wzR2iU

11–14 December 2017
World Congress on Industrial Control Systems Security
Cambridge, UK
http://wcicss.org

11–14 December 2017
World Congress on Internet Security
Cambridge, UK
www.worldcis.org

8–11 January 2018
FloCon 2015
Tucson, AZ, US
http://bit.ly/2iVp6Tn

8–11 January 2018
International Conference on Cyber Security (ICCS)
New York, US
http://iccs.fordham.edu