ELSEVIER

network SECURITY

ISSN 1353-4858 January 2018

www.networksecuritynewsletter.com

Featured in this issue:

Apache Struts 2: how technical and development gaps caused the Equifax Breach

An Apache Struts vulnerability allowed hackers to steal data on 143 million Equifax customers. What needs closer examination is the cause.

The breach offers a reminder about how security practices play an important role in protecting a company, along with instituting security policies into engineering planning and processes. There's an opportunity for a conversation about stopping hackers in their tracks with tight processes, especially with regard to the use of open source software, explains Jeff Luszcz of Flexera.

Full story on page 5…

Securing the blockchain against hackers

Blockchain technology is transforming the way data is shared and value is transferred. However, security concerns must be overcome before it is ready for mainstream adoption.

Protecting cryptographic keys remains a top concern. Using hardware security modules (HSMs) and trusted computers in place of digital wallets and as blockchain nodes will give security-conscious users and organisations assurance that no matter what blockchain application they choose, they have the means to protect digital assets, argues Olivier Boireau of Design SHIFT.

Full story on page 8…

Blurring the boundaries between networking and IT security

Networking and security used to be largely separate IT methodologies. As such, they could be treated as separate domains of the business.

That's not the case today. There is now a huge overlap between the two areas. It is becoming common to think about the network itself as a security enforcement platform and these two elements of modern technology systems are becoming inextricably entwined. This development will be overwhelmingly positive both for solutions providers and their end customers, says Dave Nicholson of Axial Systems.

Full story on page 11…

North Korea blamed for WannaCry, PoS attacks and Bitcoin phishing

The US Government has now officially blamed North Korea for the recent WannaCry ransomware campaign. The attribution was made with the agreement of the governments of the UK, Australia, Canada, New Zealand and Japan and based on an analysis presented to those countries but not publicly available.

Tom Bossert, homeland security adviser to President Donald Trump, made the claim in a White House press briefing. It was the official confirmation

Continued on page 2...

Contents

NEWS

North Korea blamed for WannaCry, PoS attacks and Bitcoin phishing 1

FEATURES

Apache Struts 2: how technical and development gaps caused the Equifax Breach 5

An Apache Struts vulnerability allowed hackers to steal data on 143 million Equifax customers. This breach offers a reminder that security practices play an important role in protecting a company along with instituting security policies into engineering planning and processes. We can stop hackers in their tracks with tight processes, especially with regard to the use of open source software, explains Jeff Luszcz of Flexera.

Securing the blockchain against hackers 8

Blockchain technology is transforming the way data is shared and value is transferred. However, security issues must be overcome before it is ready for mainstream adoption. How to protect both the cryptographic keys that allow access to the ledger and blockchain applications remains a top concern. Using hardware security modules (HSMs) and trusted computers in place of digital wallets and as blockchain nodes will give organisations assurance that, no matter what blockchain application they choose, they have the means to protect digital assets, argues Olivier Boireau of Design SHIFT.

Blurring the boundaries between networking and IT security 11

Networking and security used to be treated as separate domains. But there is now a huge overlap, partly because of the move to hybrid networks and because escalating threats have led enterprises to implement a wide range of security services. It is becoming common to think about the network itself as a security enforcement platform. This development will be positive both for solutions providers and their end customers, says Dave Nicholson of Axial Systems.

Mitigating replay attacks with ZigBee solutions 13

ZigBee wireless technology is embedded in a wide variety of solutions, including home and building automation, PC peripherals and medical sensors. But it has some significant security weaknesses – most notably its vulnerability to replay attacks. Fadi Farha and Hongsong Chen of the University of Science and Technology Beijing examine the weak spots of the technology and how they might be mitigated.

News in brief 3

Reviews 4

The Firewall 20

Events 20

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

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

of rumours and accusations that have been floating around for some time.

"North Korea has acted especially badly, largely unchecked, for more than a decade," alleged Bossert. "Its malicious behaviour is growing more egregious and stopping that malicious behaviour stops with this step of accountability. The attribution is a step towards holding them accountable, but it's not the last step. Addressing cyber-security threats also requires governments and businesses to co-operate to mitigate cyber-risk and to increase the cost to hackers by defending America. The US will lead this effort."

The full statement is available here: http://bit.ly/2FnB0fS.

In the UK, Foreign Office Minister Lord Ahmad echoed the charge, saying WannaCry was the work of the Lazarus Group, aka Guardians of Peace, which has been on security specialists' radar since 2009 and is known to use DDoS botnets, keyloggers, remote access tools and wiper malware in its activities.

WannaCry is believed to have affected around 300,000 computers worldwide, and the UK included 48 NHS trusts among its victims.

There was no reason given for the timing of this announcement, although it does coincide with the launch of a National Security Policy – available here: http://bit.ly/2DfTIW5. And not everyone is convinced.

"Accurate attribution for cyber-attacks is almost always a difficult task, and it's doubly so when the evidence leading to the conclusion can't be shared," said Tim Erlin, vice-president of product management and strategy at Tripwire. "With global public trust in the US Government at a low point, it's not surprising that there's scepticism. If we're going to have national security organisations delivering these types of conclusions on attribution to the public, we need to find a way to develop trusted output. The mantra of 'trust us' doesn't cut it here."

He added: "This conclusion about North Korea's culpability isn't new. The UK discussed the very same conclusion in October, with the very same caveats about sharing the actual evidence."

Ross Rustici, Cybereason's senior director of intelligence services, goes further and remains convinced that WannaCry was not a state-sponsored attack.

"The overall tone of the US Government's messaging is more about rehashing the fear-mongering strategies that led to the 2003 invasion of Iraq rather than an actual attempt to educate and defend the US and global population against what is rightly considered a large cyberthreat," he wrote in a blog post (available here: http://bit.ly/2DfyiZy).

Cybereason had previously published a post about why it felt it unlikely that North Korea was the source of the campaign.

"Nothing in North Korea's past cyber campaigns or in their conventional military and foreign policy fit this mould," added Rustici. "Looking at national identity, foreign policy and strategic messaging will greatly reduce the likelihood that Pyongyang ordered this campaign."

Despite this controversy over the WannaCry campaign, security firms are not slow to point the finger at North Korea for other attacks.

Proofpoint researchers say they have uncovered what they claim is the first publicly documented case of a nation-state attack on point of sale (POS) systems, with the aim being to steal payment card data. The malware is targeted at the POS terminals of businesses in South Korea and is accompanied by tools for spear-phishing campaigns. Proofpoint's report is available here: http://bit.ly/2menWkw.

Secureworks claims that the Lazarus Group has been targeting executives at crypto-currency firms. A spear-phishing campaign, using the lure of a fake job opening for a CFO position in London, employed a Microsoft Word document with a malicious macro to install a remote access trojan (RAT) which, Secureworks believes, would be used to steal bitcoins and other crypto-currencies.

Meanwhile, AlienVault said it has identified a malware installer designed to load a Monero crypto-currency miner on victims' machines. Any currency that is successfully mined is sent to the Kim Il Sung University in Pyongyang, North Korea. However, there are issues with the malware, including a URL that doesn't resolve. AlienVault believes it may be a test for a later attack or software that has been rendered out of date. There's more information here: http://bit.ly/2FmDIm9.

In brief

Olympic phishing

A phishing campaign is underway targeting people associated with the forthcoming Pyeongchang Winter Olympics in South Korea. A number of groups connected with the event, most notably ice hockey organisations, have been receiving emails with attached Microsoft Word documents containing malicious macros. According to an alert by security firm McAfee: "The attackers originally embedded an implant into the malicious document as a hypertext application (HTA) file, and then quickly moved to hide it in an image on a remote server and used obfuscated Visual Basic macros to launch the decoder script. They also wrote custom PowerShell code to decode the hidden image and reveal the implant." Most of the targeted organisations are in South Korea. However, this time security firms are not (necessarily) blaming its northern neighbour – Russian and China are seen as equally likely candidates. Several sponsors and partners of the games have come under hacking attacks that security firm Anomali has variously attributed to hacking groups Kimsuky (North Korea), RGB (North Korea), APT3 (China), and Nexus Zeta (a hacker known to have exploited the Mirai botnet code). McAfee's report is available here: http://bit.ly/2mhRWMf.

Industrial attacks grow

Kaspersky Lab's latest 'IT Security Risks Survey' suggests that targeted attacks against firms in industrial sectors are the fastest-growing type of threat. In the past year, more than a quarter (28%) of the 962 industrial companies contacted by Kaspersky had suffered targeted attacks – a rise of 8% over the previous year. Some 87% of them consider the attacks to be complex. Worryingly, nearly half (48%) of firms feel they have insufficient insight into the threats they face. There is also a lack of visibility into their own networks, which resulted in attack detection taking anything from several days (34%) to several weeks (20%). While around two-thirds of employees feel the need for more sophisticated security technology, half of the firms (49%) believe that the biggest problem is staff not following IT security policies. The report is available here: http://bit.ly/2D1gljn.

Carphone Warehouse fined

UK mobile phone retailer Carphone Warehouse has been fined £400,000 by the Information Commissioner's Office (ICO) as a result of a major data breach in 2015. Personal information concerning more than three million customers – including names, addresses, phone numbers, dates of birth and marital status – was stolen from the company's online division, which runs the OneStopPhoneShop.com, e2save.com and Mobiles.co.uk websites. In addition, payment card data for 18,000 customers was breached. Elizabeth Denham, the Information Commissioner, said that the ICO had found systemic failures "related to rudimentary, commonplace measures". The fine is one of the largest levied by the ICO but may be reduced to £320,000 if Carphone Warehouse pays within a month. And it's well below the level that could have been levied under the EU General Data Protection Regulation, which comes into force in a few months.

UK draft law eases restrictions on researchers

The Data Protection Bill currently under consideration by the UK Parliament has been amended to avoid criminalising work by researchers. As it stood, the bill would have made it illegal to 'de-anonymise' data sets. However, it's common practice for researchers to test whether data that has been anonymised can be analysed in such a way that individuals can once more be personally identified – something that is often easier to achieve than most people realise. Matt Hancock, the Culture and Digital Secretary, has introduced an amendment that allows for research providing that any successful de-anonymisation is notified to the Information Commissioner's Office within three days. This is in stark contrast to a similar bill under consideration in Australia. When researchers at Melbourne University demonstrated that allegedly anonymised medical data sets published by a government department could be de-anonymised, the Government reacted by proposing a bill that would outlaw such research.

Bitcoin no longer rules

There are signs that the high price and volatility of Bitcoin are resulting in it falling out of favour with cyber-criminals. There have been reports of people on underground forums demanding payment in other forms of crypto-currency for their goods and services. Now a new variant of the HC7 ransomware has been seen in the wild that accepts Ethereum as payment. Nearly all ransomware to date has demanded payment in Bitcoin, with a few examples taking Monero. It has been suggested that cyber-criminals might take advantage of Ethereum's 'smart contract' feature, which would mean that they get paid only if they successfully unlock a victim's files. Knowing that the criminals have this incentive, victims might be more likely to pay up.

Brits happy to be money mules

An experiment by financial firm Santander found that a surprising number of UK residents would be happy to work as money mules. Cyber-criminals running various kind of scams and hacking campaigns use mules to 'cash out'. For example, they may use forged payment cards at ATMs to withdraw cash, or they may use their own accounts to forward incoming transfers – effectively laundering the proceeds of cybercrime. Money mules are often recruited via spam campaigns and online advertising offering fast and easy money. A fake advert by Santander, purportedly coming from a fictitious company called Money Spark and offering a post as a 'financial transaction control analyst' was sent to 2,000 people. While some were suspicious, a third said they would apply for the job and just over a quarter (27%) would be prepared to leave their current jobs. Most (71%) had never heard of the term 'money mule' – only 15% recognised correctly what the advert was actually describing. What's more, 69% believed that being a money mule and handling stolen goods would not lead to a prison term in excess of three years (the maximum term is actually 14 years). A quarter thought the maximum punishment would be a fine. When informed of the true nature and illegality of the work, 7% said they would still take the job.

Botnets grow

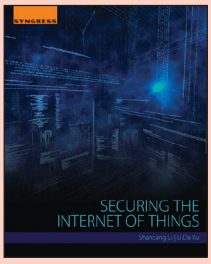
One out of every seven IPs blocked using the Spamhaus Block List (SBL) was a botnet command and control (C&C) server, the firm said. The SBL is used by many organisations to filter email in an effort to reduce spam and malicious emails. In its report on 2017, Spamhaus revealed that the number of C&C servers had increased by 32% last year. The vast majority of these servers were commissioned by cyber-criminals purely for botnet control, rather than piggy-backing on other, sometimes legitimate, servers. This has led to Spamhaus creating an additional resource – the Botnet Controller List (BCL) – which it suggests is used as a 'drop all traffic' list. Any traffic matching this list should be null routed, the firm says, because the hosts are used purely for botnet control and generate no legitimate traffic. In 2017, the number of entries on the BCL increased by 40%. There's more information here: http://bit.ly/2Frn9W4.

Attacks on UK businesses

Each UK business was subjected to an average of 231,028 Internet-borne attacks in 2017, according to figures from Beaming, a business-oriented ISP. Each firm faced 633 attempts a day to breach its firewall and more than 70% of all attacks targeted connected devices such as building control systems and networked security cameras. The volume of attacks shot up by 24% in the last quarter of 2017. Between the start and the end of the year there was a six-fold surge in attacks targeting company databases, a five-fold increase in attempts to hijack DNS services and a three-fold rise in efforts to infiltrate remote desktop systems.

Reviews

BOOK REVIEW



Securing the Internet of Things
Shancang Li, Li Da Xu.
Published by Syngress.
ISBN: 9780128044582.
Price: $59.95, 154pgs, paperback.
E-book editions also available.

There's never been a better example of how technology progresses at a faster rate than our ability to secure it than the Internet of Things (IoT). This is a class of devices that we are welcoming into our homes and businesses but often with little or no thought as to whether that's wise.

The fact that IoT devices are becoming deeply embedded in areas such as healthcare should be a matter of deep concern. But as with so many technologies, the benefits they bring (real or perceived) often outweigh security concerns. And the IoT is flavour of the month as far as technologies go. That inevitably means that vendors are rushing to market with products whose development lifecycle simply doesn't have space to accommodate processes such as penetration testing.

There's also the problem that so few IoT devices can be patched or upgraded to fix security issues. Most of the devices exploited by the Mirai botnet, for example, are still out there and still vulnerable.

To many vendors, attaching new or revamped existing products to the Internet is a 'cool idea' that has enormous marketing appeal. Many of these firms have little in the way of security knowledge or expertise. And often the price of getting it wrong is minimal. VTech, a maker of 'smart toys', exposed the personal data of millions of parents and children on its website – with much of that data having been gathered by the products. This included five million records relating to parents and 227,000 to children. The penalty for this was the recent levying of a $650,000 fine – about $8 per record.

There are inherent problems with many IoT devices, too. While some may run on platforms such as embedded Linux, many IoT solutions are driven by microcontrollers that simply lack the power and capabilities for a proper security stack. There are initiatives to address this, such as the OWASP Internet of Things (IoT) Project and the IoT Security Foundation. But the adoption of frameworks, technologies and best practices is slow and remains so, while the IoT is more about cool ideas and marketing hype rather than genuine benefit.

In this relatively short book, the authors do a good job of laying out the challenges involved in securing IoT devices. They delve immediately into what is required to layer security into IoT solutions, looking both at the device level and the technologies used to 'Internet enable' them. They also spend time pulling apart the various layers – from on-device crypto keys, through authentication and transport encryption to the back-end systems – any one of which can introduce vulnerabilities.

IoT security is very much a work in progress. Standards and protocols are emerging, but the authors wisely spend a chapter looking at what we are trying to achieve with them: what does IoT security even look like? There are also specific chapters on areas of particular concern – healthcare and IoT in social networks.

Many of the chapters – such as the last two mentioned – are very brief: the social IoT one is just a page and a half. However, one of the biggest attractions of this book is just how well referenced it is. The chapters are littered with links to papers and websites and so you could treat this book as a in-depth review of the current literature.

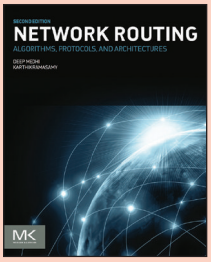
We've witnessed many security breaches and malware attacks enabled by devices such as children's toys, video recorders and security cameras. Some, like Mirai, have been very serious. And more are on the way. So this book is a timely warning that we need to get to grips with this problem.

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

– SM-D

BOOK REVIEW

Network Routing
Deep Medhi and Karthik Ramasamy.



Published by Morgan Kaufman.
ISBN: 9780128007372.
Price: $110, 1018pgs, paperback.
E-book editions also available.

The way hackers get in is by finding the chinks in your armour. And it doesn't help that modern networks have become so complex.

Attackers have been known to exploit weaknesses at every level of networking, from the local (your LAN) to the large-scale (Border Gateway Protocol, or BGP). And the problem isn't just that the technologies employed contain occasional inherent flaws (although they certainly do) – it's also that their complexity inevitably gives rise to inadvertent misconfigurations.

Networking routing is one of those areas that can so easily result in weak spots – and bald spots, as network managers tear their hair out trying to locate a problem, often of their own making. So while this book isn't about security per se, and only a fraction of its 1,000-plus pages deals specifically with the subject, it covers a topic that is too often the root cause of network vulnerabilities.

The book is also extremely thorough about how it does this. It's probably safe to say that there's no aspect of network routing left uncovered. It encompasses the full gamut of network types, including IP-based Internet routing, circuit-switched routing and telecommunication transport network routing – and how they inter-operate.

The book is aimed at practitioners – network architects and senior technical and operational staff – and takes a vendor-agnostic approach. The latter is supported by the fact that, even though its intended readership is people already knowledgeable about the functioning of networks, the book devotes significant space to helping you understand the underlying concepts, protocols and algorithms.

Indeed, one of its appeals might be to people who might know how to configure a Cisco firewall or a DMZ but have a nagging concern that they don't fully grasp what's going on under the hood. The authors have taken quite a lot of trouble to relate the theoretical aspects of networking to everyday practice.

This second edition adds coverage of software-defined networking, datacentre networks and multicast routing, so it's fully up to date not just with how networks look now but where they are heading.

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

– SM-D

Apache Struts 2: how technical and development gaps caused the Equifax Breach

Jeff Luszcz

Jeff Luszcz, Flexera

You already know the story: by identifying an Apache Struts CVE-2017-5638 vulnerability, criminals exposed the personal data of up to 143 million Equifax customers. What needs closer examination is the cause. The coding risk that opened up the door must be identified and closed. And just as important, companies need to examine their development processes for openings that let vulnerabilities in. Open source software (OSS) is widely used in software applications but rarely tracked in detail. Companies don't know what they don't know regarding open source and the breach teaches important lessons about the need to close that gap.

The Equifax breach offers a reminder about the basics – security practices play an important role in protecting a company along with instituting security policies into engineering planning and processes. The Equifax breach opens up the opportunity for a conversation about stopping hackers in their tracks with tight processes.

Let's start the conversation and take a deeper look at the open source technical vulnerability as well as the operational exposure opened up by Apache Struts 2.

Technical gap

Struts 2 is an Apache 2.0 licensed Java web framework used to build large-scale web applications. It is commonly used in government, financial, health and other large enterprise applications. Hackers were able to take advantage of CVE-2017-5638 in Struts 2 in order to steal confidential information.

Flexera's Secunia Research characterises the Apache Struts CVE-2017-5638 vulnerability as highly critical, including this description: "A vulnerability has been reported in Apache Struts, which can be exploited by malicious people to compromise a vulnerable system. An error related to the Jakarta Multipart parser when processing 'Content-Type' can be exploited to execute arbitrary code."[1]

Struts 2 contains another Apache licensed library called Object Graph Navigation language (OGNL). This was the underlying technology that was attacked and exploited at Equifax.

"Struts has suffered from a couple of vulnerabilities using the technique of object-graph navigation language (OGNL) injection"

According to McAfee: "Apache Struts is a model-view-controller framework for creating Java web applications. Struts has suffered from a couple of vulnerabilities using the technique of object-graph navigation language (OGNL) injection. OGNL is an expression language that allows the setting of object properties and execution of various methods of Java classes. OGNL can be used maliciously to perform remote code execution attacks against Apache servers …"[2]

While Apache Struts 2 captured the attention of the news media, the vulnerability was actually the result of the unsafe use of the embedded OGNL library. A defect related to OGNL parsing error messages was exploited in the default Struts 2 file upload functionality. TrendLabs describes the gap: "This particular vulnerability can be exploited if the attacker sends a crafted request to upload a file to a vulnerable server that uses a Jakarta-based plug-in to process the upload request. The attacker can then send malicious code in the Content-Type header to execute the command on a vulnerable server."[3]

"The vulnerability was not the only cause of the breach. Development processes related to managing open source software played a big role"

Versions affected include 2.3.5, 2.3.31, 2.5 and 2.5.10. The recommended action is upgrading to Apache Struts version 2.3.32 or 2.5.10.1, especially when using the Jakarta-based file upload Multipart parser. An option is also switching to a different implementation of the Multipart parser.

But the vulnerability was not the only cause of the breach. Development processes related to managing open source software played a big role.

Development gap

The benefits of open source are readily apparent. It reduces the cost of development, shortens development cycles and

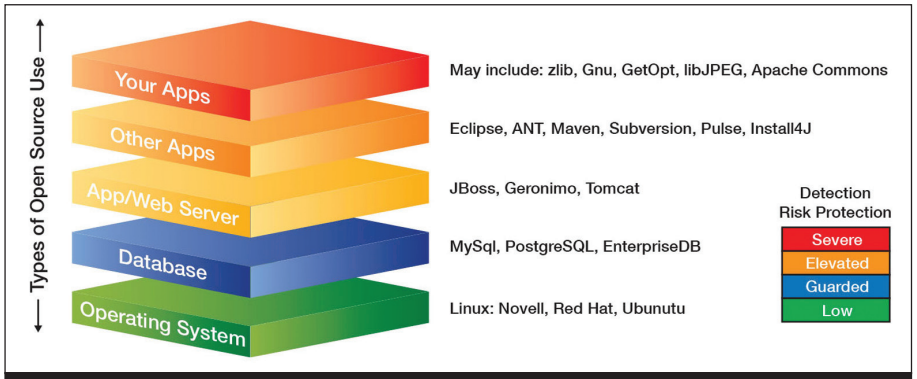


Figure 1: Open source software use in the enterprise.

can lower overall total cost of ownership of your applications if managed well.

Here's the challenge. Open source is being used up and down the application stack as shown below, which means oversight of third-party components is critical. But three big gaps exist.

Gap 1: The intrusion detection, firewalls, web-based authentication and identity management systems used by most IT teams do not offer enough protection. They only manage traffic to the application and do not secure the perimeter. To provide the protection needed, applications must be secured from the inside out by hardening application code or managing vulnerability defects.

Gap 2: Organisations do not monitor open source as it enters the organisation. Years ago, when developers wanted to incorporate third-party code into the applications they were building, a joint development agreement or in-bound licensing contract would be negotiated through a process including a development manager, procurement lead and a lawyer. In today's world of 24/7 and persistent network access, developers dispersed across multi-national sites can include open source, freeware, public domain 'evalware' of commercial software and more into the code they are writing without triggering the usual check-points in the procurement process. And the further up the application stack open source software is used, the less likely its use is detected, monitored and tracked.

Gap 3: There is little structure around using open source code during the development process. It is becoming very clear that decisions made during the software development lifecycle – from user interface design to embedded third-party components to patch management – will significantly impact the likelihood of security incidents and the success of responding to them. The development decision-making process needs to expand to include engineering and security in third party code decisions.

"It is becoming very clear that decisions made during the software development lifecycle – from user interface design to embedded third-party components to patch management – will significantly impact the likelihood of security incidents"

Development teams need to move beyond applying patches, and address vulnerabilities in processes. Taking preventive action keeps code safer, saving time and money while protecting reputations.

How to close the gaps

To help you close these dangerous gaps, we have six key recommendations:

1. Create a partnership between engineering and security. To end these gaps, it's time for the development team to join forces with a security team that includes IT and legal. The team should develop a two-tier process that protects the organisation. Engineering provides an accurate inventory of open source components in use.

The security team creates a system to associate the open source projects in use with known and published vulnerabilities. By examining vulnerabilities from multiple perspectives and putting a formal process in place, software companies gain the protection needed to avoid costly breakdowns in security.

2. Identify what stakeholders need to prevent a breach. These will include:

- Legal – the legal teams are responsible for legal risk and reputation management. To protect the company, they must understand what is used in code and engage in the process of managing it. If hackers break in, the risks are big from FTC probes, government agency intervention and lawsuits.
- Security – without a detailed bill of materials, looking for the component in products is a very expensive discovery operation. When you scan code and keep track of all components in your code, the company can act faster on a legal advisory.
- Operations – if you have a breach, an alert process for operations is critical. The team needs to start the complicated step of implementing a patch and communicating with customers. By defining a step-by-step approach, you can avoid what Equifax experienced and prevent greater damage.
- Development – engineering plays a critical role in preventing a vulnerability. It starts during the development process by knowing what open source is used and taking the steps to protect code. This process also helps developers save time in the event of a breach. They will know where to look instead of wasting days looking for the component in the codebase.

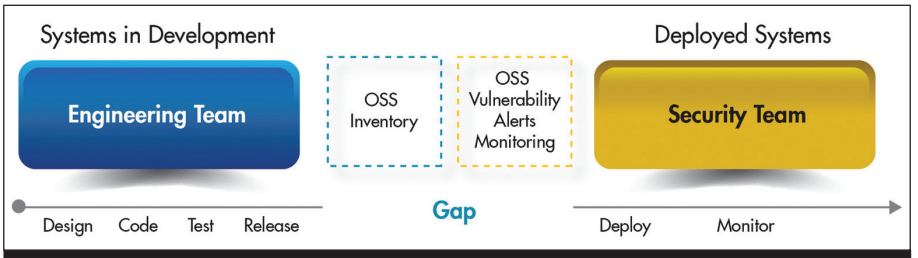


Figure 2: The dangerous gaps between engineering and security teams.

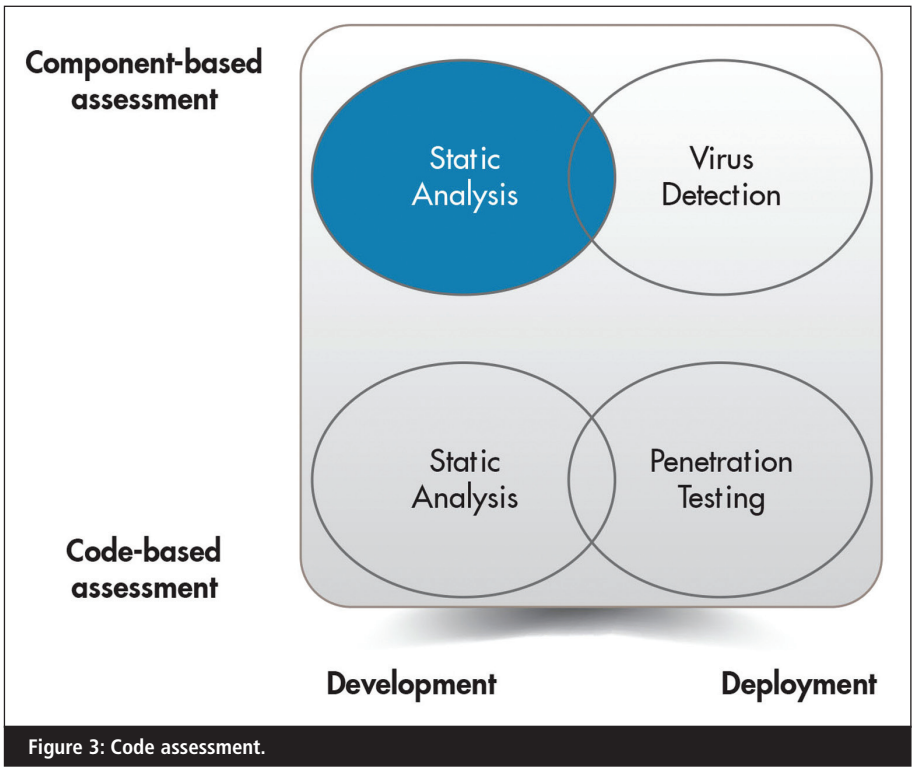


Figure 3: Code assessment.

3. Assess multiple environments. Instead of just monitoring the security traffic to applications, organisations need to go deeper and protect software code during design, development, installation and deployment.

Within each of those areas, code should be assessed at two levels of detail: at the level of source code and at a higher level of code modules or components. For example, the static analysis in the lower left of Figure 3: analysis occurs at the source code level during development and static analysers are the most widely used tools for application security.

Moving to the right side of the graphic, code level analysis at the point of deployment is generally considered the domain of web application security scanners.

4. Dig deeper on OSS use by development. These 10 important questions will help bring out where and how you are using open source software:

1. Where is our OSS inventory, including all versions in use?
2. How accurate is the information?
3. Where does the OSS we use reside inside our code base?
4. How are we using the OSS?
5. Are there vulnerabilities within the versions we're using?
6. Are we on the latest version – if not, why?
7. Have we paid for commercial support for all the OSS projects in our code base?
8. If not, who is responsible for monitoring and upgrading to newer versions?
9. What is our OSS use policy and approval process?
10. Are we compliant/enforcing with our own policy?

5. Monitor in advance. The reality is that OSS patching is very complicated. The Equifax timeframe illustrates the difficulty – up to two months before the first reported unauthorised access and the further delay of the actual detection of the breach on 29 July 2017. The whole software supply chain is involved from design to deployment and it's simply not going to be an overnight fix. With today's risk, a process that can prevent breaches as well as move fast is now essential to protect the company and its reputation.

6. Try software composition analysis (SCA) technology. With the increasing frequency of hacker attacks, companies require a consistent approach to monitoring code. Scanning technology uncovers, manages and monitors the OSS being used. These tools also automate the process of vulnerability alerts and answer important questions. Which open source libraries are being used in my product? What other third-party libraries are being pulled in by default and are potentially

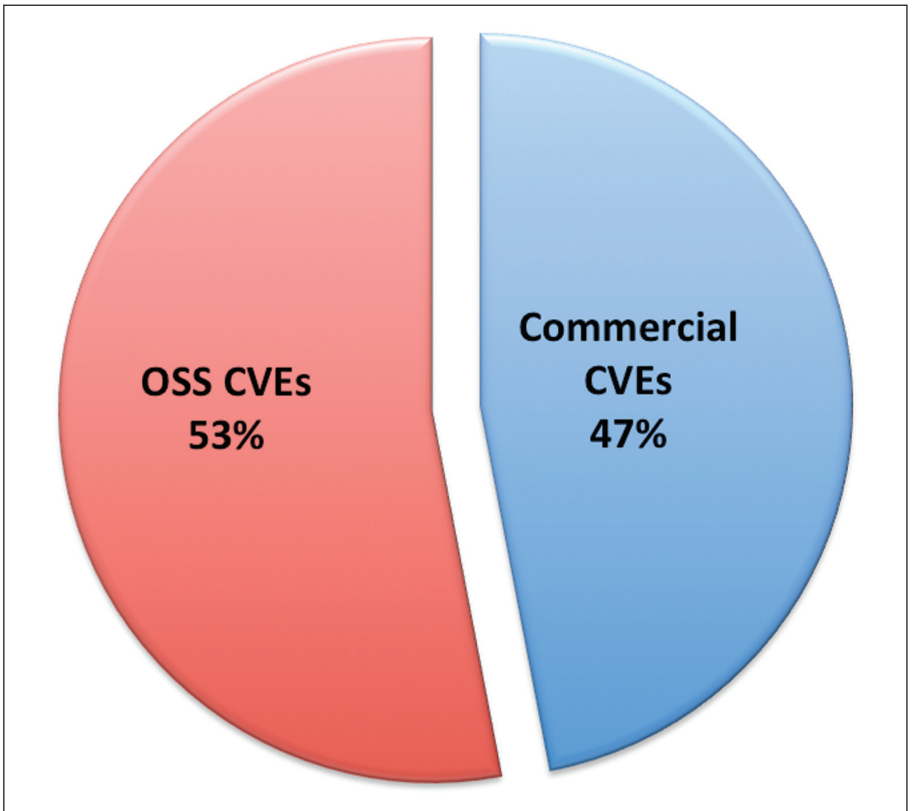


Figure 4: The percentage of Common Vulnerabilities and Exposures (CVEs) on the National Vulnerability Database (NVD) related to open source and commercial projects.

introducing additional risk? What percentage of my proprietary code contains 'stolen' or 'copied' code from other third-party open source libraries without proper attribution?

It's not over

While Equifax holds the spotlight right now, there's a bigger issue that needs attention. The company has fixed the problem and has programmes in place to deal with the ramifications.

"In the cybercrime community, a successful breach gets the attention of other hackers. It starts a long tail of incidents and breaches for months and even years"

The big danger now is an open door for hackers. Heartbleed, which occurred more than three years ago, still leaves a trail of problems for IT security. In the cybercrime community, a successful breach gets the attention of other hackers. It starts a long tail of incidents and breaches for months and even years.

Development teams have the opportunity to play the hero role by initiating processes that produce secure software. Teams can conduct code-level security reviews, in addition to penetration tests, for their internally developed code before deployment. Outsourced development and business partners can conduct code-level audits. Monitoring can be put in place for all other third-party code included in software applications, for security flaws, intellectual property concerns and updated version information. Finally, the institution of internally developed applications with adequate checkpoints enables thorough audit trails.

The technical story behind the Apache Struts 2 vulnerability offers serious lessons and learning opportunities. It's time for development teams to act on them.

About the author

Jeff Luszcz is a VP of product management at Flexera (www.flexerasoftware.com). Previously, he was founder and CTO of Palamida. He has helped software companies learn how to use open source while complying with licence obligations and keeping on top of security issues. Throughout his career, he has been active in the Java, Macintosh and open source software communities. Luszcz is also the author of several well-known Macintosh software utilities and has served as a technical editor for Wrox Press.

References

1. 'Apache Struts Jakarta Multipart Parser Code Execution Vulnerability'. Flexera Secunia Advisory SA75730, 8 Mar 2017. Accessed Jan 2018. https://secuniaresearch.flexerasoftware.com/community/advisories/75730.
2. Shah, Hardik. 'Analysing CVE-2017-9791: Apache Struts Vulnerability Can Lead to Remote Code Execution'. McAfee, 19 Jul 2017. Accessed Jan 2018. https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-cve-2017-9791-apache-struts-vulnerability-can-lead-remote-code-execution/.
3. Sahu, Suraj. 'CVE-2017-5638: Apache Struts 2 Vulnerability Leads to Remote Code Execution'. TrendLabs Security Intelligence Blog, 9 Mar 2017. Accessed Jan 2018. http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2017-5638-apache-struts-vulnerability-remote-code-execution/.

Securing the blockchain against hackers

Olivier Boireau

Olivier Boireau, Design SHIFT

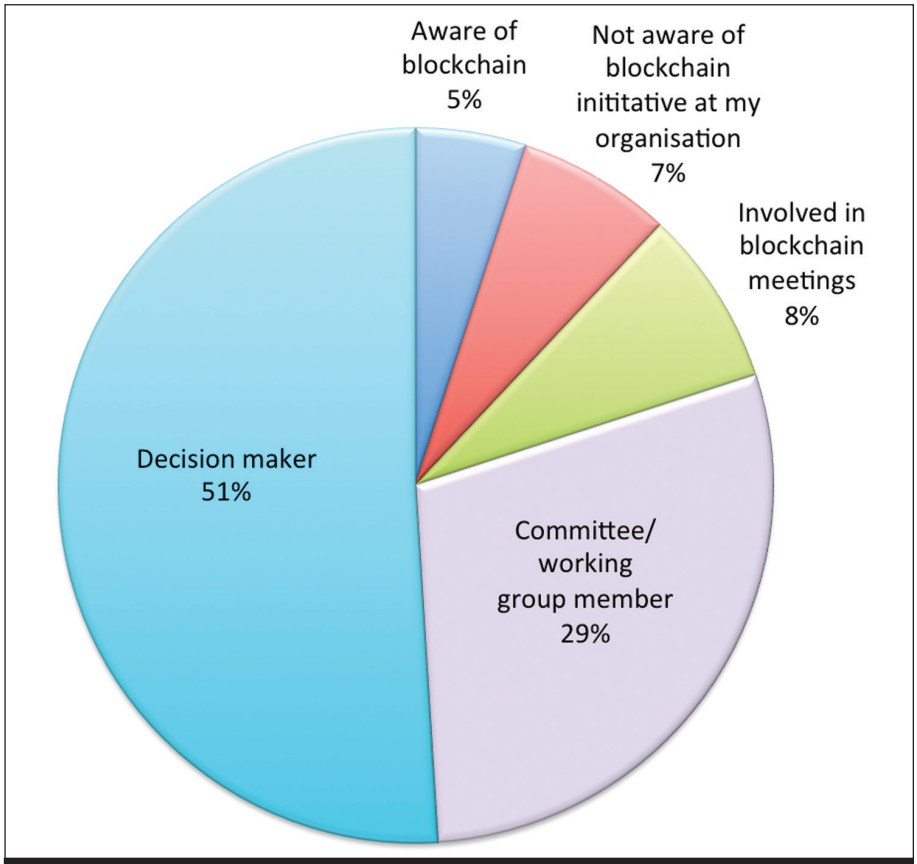
Blockchain technology is transforming the way data is shared and value is transferred. However, there remain significant obstacles that must be overcome before blockchain is ready for mainstream adoption – most notably, security. How to protect both the cryptographic keys that allow access to the ledger and blockchain applications remains a top concern for any organisation or individual interested in using blockchain to transact anything of significant value.

Many hail blockchain technology as a security innovation because it provides a trusted ledger that shifts data storage and protection from a centralised to a decentralised model. Trust comes from the process itself rather than from the status of any one participant. This allows two untrusted parties to efficiently record transactions in a verifiable, permanent way without using an intermediary.

However, while blockchain shows promises in its ability to support an endless number of innovative financial trading, payments, healthcare, government and other critical applications, recent high-profile breaches of exchanges show that blockchain participants and their access to the blockchain represent a security weakness that must be addressed before the technology can reach its full potential.

What is blockchain?

Blockchain is a distributed ledger technology that provides a historical record of all transactions that have taken place



Level of involvement with blockchain initiatives within organisations. Source: Greenwich Associates.

across a peer-to-peer network. Best known as the technology behind the Bitcoin crypto-currency, blockchain takes records – such as proof of ownership, confirmed transactions and contracts – and stores them as 'blocks'. New blocks are linked to previous blocks to form a linear and chronological 'chain' of events.

"Recent high-profile breaches of exchanges show that blockchain participants and their access to the blockchain represent a security weakness that must be addressed"

Any new record is verified by consensus – meaning that various network participants, called 'miners', work together to verify the integrity of the data. Once verified by a majority of the miners, the block is stored in an encrypted and decentralised fashion across the network. This results in a system of record-keeping that is maintained solely by network participants.

Blockchain is revolutionary because it enables the creation and operation of a 'trustless network'. Using blockchain, unrelated parties can transact with one another without pre-existing trust, middlemen or supervisory authorities. In the case of Bitcoin, for instance, blockchain helps create new depository and transaction mechanisms that no longer rely on banks or other third-party intermediaries. This gives blockchain the power to disrupt existing financial systems and create a new financial architecture based on computer algorithms rather than on interpersonal trust.

The power of blockchain to decentralise markets and undermine the control of existing middlemen has captured the imagination of Silicon Valley and Wall Street alike. Moving forward, blockchain isn't just about disintermediating the middleman, but rather about solving problems or seizing opportunities that have eluded current systems.

Despite all the allure of blockchain, significant security challenges still remain. A recent Greenwich Associates survey underscores the importance of overcoming these security roadblocks – 85% of survey respondents are concerned or very concerned that permissioned networks and centralised identity management systems are creating a big target for hackers.

Keys to the kingdom

In blockchain applications, the digital asset and the means to protect it are combined in one token. Nobody can steal or copy the digital asset unless they have the secret code or 'private key' that unlocks the cryptographic protection of the asset. However, storing private keys in software or on a piece of paper is the equivalent of leaving your house keys under the welcome mat.

"Most people currently use software called wallets or multi-signature wallets, but these solutions are driven more by convenience than security. Hardware wallets were designed to offer a higher level of private key security, but even these solutions are vulnerable to hacks"

While blockchain technology secures data in transit from place to place using cryptography, the private key becomes vulnerable to theft when it is stored or displayed at one end or the other – whether that is on a piece of paper, screen, disk, in memory or in the cloud.

To keep digital assets and private keys safe, most people currently use software called wallets or multi-signature wallets, but these solutions are driven more by convenience than security. Hardware wallets, such as Trezor or Keepkey, were designed to offer a higher level of private key security, but even these solutions are vulnerable to various hacks, including fault injections.[1,2]

A fault injection attack is a procedure used to maliciously introduce an error in a computing device in order to alter the software execution. The goal of the fault injection can be to either:

1. Avoid the execution of an instruction.
2. Corrupt the data the processor is working with.

These techniques can be used to compromise the security of hardware wallets

by bypassing security checks or leaking the private keys.

Once private keys are stolen, it does not matter how secure the blockchain itself is – anyone can monetise and exploit the asset and any malicious transfer of value is typically instantaneous and irreversible. Today, hackers commonly target online services that store the private keys for a large number of users or infect network participants with a malware that searches for private keys.

In August 2016, hackers stole $72m worth of bitcoin from accounts at the Hong Kong crypto-currency exchange Bitfinex.[3] In the Bitfinex hack, at least two private keys stored in a multi-signature wallet hosted by BitGo were compromised. Public blockchain participants have lost millions of dollars as a result of compromised security systems.

Lies become truth

Whether executing smart contracts or trading crypto-currencies, the digital assets that blockchains protect exist only in computer code. When stolen, it is possible for hackers to evade detection by rolling back the blockchain to a previous version of the code that existed before the hack. Basically, if more than half of the computers working as nodes to service the network tell a lie, the lie will become the truth.

This is exactly what happened with the Ethereum blockchain when an attacker tried to steal about $50m of the digital currency, Ether.[4] Two other blockchains based on Ethereum, Krypton and Shift, suffered what are commonly referred to as 51% attacks in August 2016.[5,6]

The attack works when hackers are able to compromise over half the nodes participating in the distributed ledger, in which case, they can prevent new transactions from gaining confirmations and halt transactions between some or all users. They also can reverse transactions that were completed while they were in control of the network, meaning they could double-spend coins if attacking a crypto-currency blockchain.

Blockchains (like all distributed systems) are not so much resistant to bad actors as they are 'anti-fragile' – meaning, they respond to attacks and grow stronger. However, this requires a large network of users. If a blockchain is not a robust network with a widely distributed grid of nodes, it becomes more difficult to ensure the immutability of the ledger.

Protecting blockchains

Today, many security-conscious organisations rely on hardware security modules (HSMs) to safeguard and manage their digital keys. An HSM is a crypto-processor that securely generates, protects and stores keys. HSMs typically guarantee a level of regulatory assurance, in compliance with either the Federal Information Processing Standard (FIPS) certification or Common Criteria, an international standard – meaning that each device meets strict industrial-grade security control requirements.

"To execute a successful attack, attackers would either need to have administrative privileges, access to data before it is encrypted, or physical access to the HSM, which makes the attack vector extremely difficult and unprofitable for a hacker"

HSMs are designed to protect potential access points in virtually any application that requires secure, verified digital signatures. People rely on the security provided by HSMs in their everyday life without even knowing it. HSMs housed in bank datacentres verify PIN numbers every time a customer withdraws cash from an ATM and validate transactions at merchant POS terminals when consumers purchase goods.

Using HSMs to protect blockchain ledgers, digital wallets and applications against hacks can provide the trusted computing environment necessary to take full advantage of the blockchain protocol. To execute a successful attack, attackers would either need to have administrative privileges, access to data before it is encrypted, or physical access to the HSM, which makes the attack vector extremely difficult and unprofitable for a hacker. Some 58% of participants in the Greenwich Associates study agreed that HSMs are an essential part of addressing blockchain security concerns.

What makes HSMs so strong?

It seems to be obvious that cryptographic operations must be performed in a trusted environment – meaning no possibility of exposure due to viruses, malware, exploits or unauthorised access. But an ordinary wallet mixes the access code, business-logic and cryptographic calls in one big application. This is a dangerous approach because an attacker can then use crafted data and vulnerabilities to access cryptographic material or steal keys.

HSMs are dedicated hardware systems specifically designed to store and manage private and public keys. The entire cryptographic key lifecycle – from provisioning, managing and storing to disposing of or archiving the keys – occurs in the HSM. Digital signatures also may be captured via an HSM, and all access transactions are logged to create an audit trail.

An HSM is hardened against tampering or damage and may be located in a physically secure area of a datacentre to prevent unauthorised contact. The module may be embedded in other hardware, connected to a server as part of a network, or used as a standalone device offline.

An HSM is a trusted computing environment because it:

- Is built on top of specialised hardware, which is well-tested and certified in special laboratories.
- Has a security-focused OS.
- Limits access via a network interface that is strictly controlled by internal rules.
- Actively hides and protects cryptographic material.

Delivering industrial-grade security to the masses

Previously, HSMs were mainly used to protect digital assets and keys in institutional settings due to the high cost and

complexity of solutions developed to meet the needs of large datacentres. But recently a new category of personal computers has emerged that makes industrial-grade security available to the masses in a form factor that is affordable and easy to use.[7]

"Using trusted computers will give security-conscious users and organisations assurance that no matter what blockchain application they choose, they have the means to protect digital assets"

This next generation of ultra-secure PCs comes with an embedded HSM and requires two factors of authentication (a key and a password) to make sure that unauthorised users cannot access the device. Additionally, the PC is protected against physical attacks with a tamper-proof casing and the private key is erased if any of the PC's physical or logical security controls are breached.

Using trusted computers in place of digital wallets and as blockchain nodes provides the missing link that will give security-conscious users and organisations assurance that no matter what blockchain application they choose, they have the means to protect digital assets using a turnkey solution that is virtually impenetrable.

Innovations in blockchain security will make the technology increasingly attractive – and usable – for a wider number of organisations and consumers. It is difficult to predict where blockchain technology is headed next, but it has all the makings of a truly disruptive technology.

About the author

Olivier Boireau is the CEO and founder of Design SHIFT. He also develops hardware and software for POS, cameras, smartphones, netbooks and consumer electronics devices. He specialises in defining wireless hardware architecture, developing strategies for hardware device design (original design manufacturer, silicon partners, software platforms) and has received numerous industry awards for his innovations.

References

1. 'Tomshwom'. 'Lessons from the Trezor Hack'. Steemit, Aug 2017. Accessed Jan 2018. https://steemit.com/bitcoin/@tomshwom/lessons-from-the-trezor-hack.
2. Redman, Jamie. 'A Def Con 25 Demonstration Claims to Break Bitcoin Hardware Wallets'. Bitcoin.com, 27 Jun 2017. Accessed Jan 2018. https://news.bitcoin.com/def-con-25-demonstration-break-bitcoin-hardware-wallets/.
3. Baldwin, Clare. 'Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong'. Reuters, 3 Aug 2016. Accessed Jan 2018. www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP.
4. Popper, Nathaniel. 'A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency'. New York Times, 17 Jun 2016. Accessed Jan 2018. www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html.
5. 'Krypton recovers from a new type of 51% network attack'. Crypto Hustle, 26 Aug 2016. Accessed Jan 2018. https://cryptohustle.com/krypton-recovers-from-a-new-type-of-51-network-attack.
6. Redman, Jamie. 'Small Ethereum Clones Getting Attacked by Mysterious '51 Crew'. Bitcoin.com, 4 Sep 2016. Accessed Jan 2018. https://news.bitcoin.com/ethereum-clones-susceptible-51-attacks/.
7. Calore, Michael. 'This ultra-secure PC self destructs if someone messes with it'. Wired, 23 Jun 2017. Accessed Jan 2018. www.wired.com/2017/06/orwl-secure-desktop-computer/.

Blurring the boundaries between networking and IT security

Dave Nicholson

Dave Nicholson, Axial Systems

Networking and security used to be largely separate IT methodologies. They were even built separately. Traditionally, networks were constructed on standard building blocks (switches, routers etc) and security solutions such as perimeter firewalls, intrusion prevention systems and the like were applied afterwards.

As such these two key areas of operational technology could effectively be treated as separate domains by businesses, each with their own set of tools, strategic approaches and dedicated operational teams. IT security departments typically focused on the delivery of time-honoured threat detection methods and perimeter-based security defence mechanisms as well as incident response and remediation. Networking teams were more concerned with issues around latency, reliability and bandwidth.

That's invariably not the case today. There is now a huge overlap between the two areas and that overlap is being driven by a range of factors. First the move to more hybrid networks – physical vs virtual vs cloud – means that traditional approaches simply cannot cope with the scale, automation requirements or the rate of change.

Crossing boundaries

Most modern networks combine the use of physical datacentres, bare metal or virtualised servers, cloud platforms and containers – and all of them require at least the same level of security. By basing an approach on security function such as policy consolidation, micro-segmentation or cloud access brokerage rather than point products and ensuring that all the functions integrate into a framework, providers and their customers can deliver a holistic approach to security that ensures that the whole is greater than the sum of the parts, irrespective of where the data or application resides.

"Organisations need to quickly and cost-effectively reconfigure and update security networks and security and network policies across many locations. It's more viable for them to do this if they have already integrated the two sets of devices and approaches"

Second, the rapidly escalating cybersecurity threat has led larger enterprises, in particular, to implement a wide range of security services from anti-virus and anti-spam software to next-generation firewalls and intrusion prevention systems. But that can cause issues with network latency. In an age where traffic volumes are continuing to ramp up, especially with the exponential growth in Internet of Things (IoT) devices, that can be a serious concern. For this reason alone, it is no longer viable for many businesses to treat networking and security entirely separately.

In addition, enterprises today often need to roll out new services or applications quickly and extend existing technologies or products into new geographical or vertical markets to stay ahead of the competition. That in turn means they will need to quickly and cost-effectively reconfigure and update security networks, and security and network policies across many locations. Again, it's more viable for them to do this if they have already integrated the two sets of devices and approaches.

Largely because of these trends, we are increasingly seeing a change in terminology from 'network security' to 'secure networks'. Moreover, it is becoming increasingly common to think about the network itself as a security enforcement platform.

Taking control

Switches, in particular, are increasingly being used as policy enforcement points of security in this new era of secure networking infrastructures. So, when a business decides to microsegment its network, perhaps even down to a single server rack level, that top-of-rack switch now becomes a security policy enforcement point.

That enhanced control is giving businesses many more options. In the event of an incident, they could decide to shut down the port, move the traffic onto a different virtual LAN (vLAN), or apply encryption to it, for example.

The security enforcement point

To be successful over the long term, this kind of approach needs to be open and inclusive. Few networks are homogeneous – nearly all will have a mix of different vendors' equipment – and all that equipment needs to communicate and operate as a cohesive, standards-based unit. This is especially important since network intelligence – 'wisdom' if you will – can then discover or predict threats and feed this information into a security policy creation function. By abstracting security policy creation to a centralised point and automating it, businesses can utilise network devices as dynamic security policy enforcers – right down to the point of connection.

"Embedding security into the network reduces operational overhead, increases visibility and helps generate meaningful intelligence for the business. By standardising security policy across the landscape, there are fewer errors and less time spent troubleshooting"

That's just one – albeit key – way in which organisations can benefit from blurring the boundaries between networking and security. When you look at the whole picture, many others emerge. Embedding security into the network reduces operational overhead, increases visibility and helps generate meaningful intelligence for the business. By standardising security policy across the landscape, there are fewer errors and less time spent troubleshooting. It also forms a solid foundation layer for a level of automation or, indeed, moving to a full software-defined security network.

From the pure IT perspective, key benefits of this approach include the ability – in an integrated world – to reduce management overheads and the associated costs, and the opportunity to reduce configuration errors using common policy and automation.

Bringing together networking and security also makes it easier for the IT team to facilitate migration to cloud services, where appropriate, and to achieve improved visibility across the network, thereby reducing the time associated with troubleshooting and resolution.

From a broader business value perspective, the benefits are even more extensive and include the opportunity to reduce risk through the delivery of consistent security across all platforms and the chance to reduce costs through the simplification and automation of security policy. A streamlined approach to integrating security and networking can also be key in achieving compliance, helping to meet the demands of regulations such as PCI and the EU's

General Data Protection Regulation (GDPR), for example. Combining security and networking across a single platform can also be key in protecting current investments and avoiding the need for large-scale upgrades.

Bright future ahead

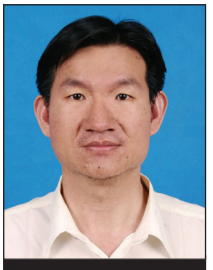
We are living in an age where the boundaries between networking and IT security are already blurred and, over time, those boundaries will blur further as these two key elements of modern technology systems become inextricably entwined. This development will be overwhelmingly positive both for solutions providers and their end customers, who will reap the rewards in terms of lower costs, better operational efficiencies and – of course – reduced risk.

About the author

Dave Nicholson is technical sales consultant at Axial Systems. With 15 years in the IT industry in sales and technical roles, he has delivered major projects in both public and private sectors. His specialisms are wireless networks, campus and DC infrastructure, security (edge to core, authentication, cloud), SDN/NFV and service delivery.

Mitigating replay attacks with ZigBee solutions

Fadi Farha



Hongsong Chen

Fadi Farha and Hongsong Chen, University of Science and Technology Beijing

The ZigBee wireless technology was developed by the ZigBee alliance and is a low-cost communication solution with low power consumption.[1,2] ZigBee applications are often embedded into electrical circuits that are widely used in home and building automation, PC peripherals and medical sensors.[3,4]

The ZigBee protocol stack (shown in Figure 1) is divided into two parts:[5,6]

- A MAC layer and a physical layer defined by the IEEE 802.15.4 standard.
- A network layer and an application layer defined by the ZigBee Alliance.

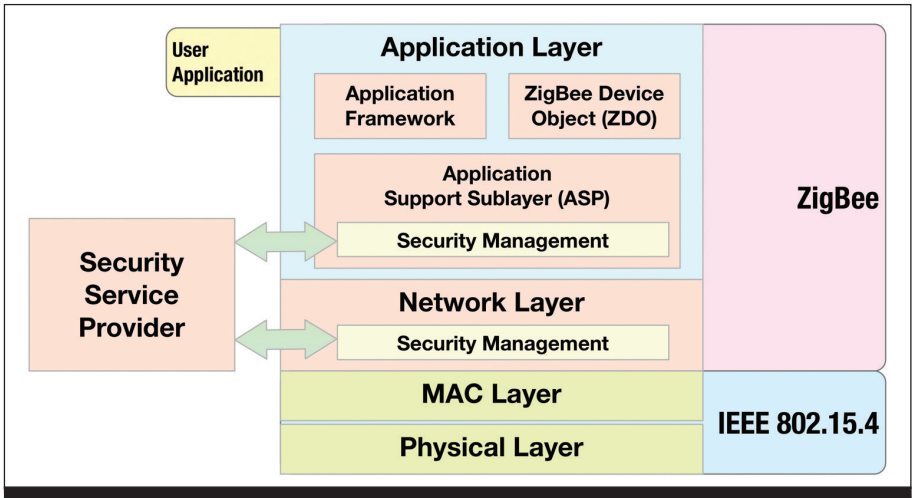


Figure 1: The ZigBee stack architecture.

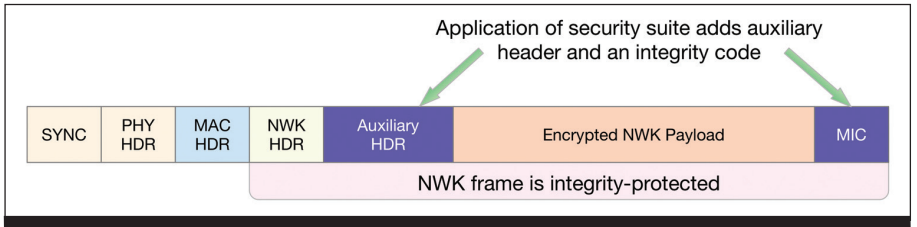


Figure 2: ZigBee frame protected with the NWK layer security.

ZigBee uses the Advanced Encryption Standard (AES) algorithm to make the upper-layer networks secure and IEEE 802.15.4 security for protecting the lower-layer networks. The ZigBee stack defines the security functions at the network (NWK) layer and the application support sub-layer (APS), as shown in Figure 1. Those security services include key management, data encryption and Message Integrity Code (MIC) calculation.[7]

The NWK layer frame-protection mechanism uses AES and CCM* for data encryption at the NWK security level. After implementing the NWK layer security, the ZigBee stack will encrypt the NWK payload using the NWK key, calculate the MIC and add the auxiliary header field to the new frame (as shown in Figure 2). The security parameters carried by the auxiliary header will be used for decrypting and authenticating the frame contents.

One of these security parameters is called the frame counter and its job is to distinguish the repeated frames by comparing the frame counter value of the incoming frame with the last received

frame counter value. Since this technique is the only ZigBee-based method for checking whether the newly received frames are old, threats will present in the ZigBee network, which means there are many opportunities for attackers to use the old copied frames inside this network once the frame counter is reset. The old frames will successfully pass the frame counter checking because they have high frame counter values. In this article, a replay attack will be carried out on a secure ZigBee network. In addition, we propose a solution that looks at all possible cases where attackers may have the opportunity to perform the replay attack.

Related work

The replay attack is a common form of network attack. It is dangerous in many cases, especially when the attacker copies important frames and has the ability to send them back into the network as valid frames. In a ZigBee network, devices use a 32-bit frame counter to help them figure out whether the received frames are old.[8,9] This frame counter increases by one every time a new frame has been sent.[10] As defined by the ZigBee specifications, the frame counter will restore to zero when the NWK key is changed.

"If the replay attack succeeds and the injected frame has a very high frame counter value, the victim will not be able to receive any other frames from the sender address"

As mentioned in some research, secured ZigBee networks that use preconfigured network keys are vulnerable to the retransmission of old captured frames when the sequence number is reset.[11] In fact, that is not enough to perform a replay attack, especially when the network is secured with a network key and configured with a frame counter. As long as the frame counter continues counting, the attack will not succeed.

The method of processing the incoming frames securely is described in the ZigBee specifications as follows. The receiving device will check whether the frame counter value of the received frame is larger than that of the last received one which corresponds to the sender address and is already saved in the receiver memory. If the frame counter value of the received frame is larger than that of the last received frame, the frame will be accepted, otherwise the system will inform the higher layer network of the condition and report it as 'bad frame counter'. In this case, no further security processing will be done on this frame.[12]

What is worse, the receiving device will update the frame counter that corresponds to the sender to the value of 'received frame count + 1'. Therefore, if the replay attack succeeds and the injected frame has a very high frame counter value, the victim will not be able to receive any other frames from the sender address that is included in the injected frame. That is because the frame counter value of all outgoing frames from this sender is smaller than the victim frame counter value which has been updated after the attack succeeded. This situation will continue until the frame counter value of the sender is larger than that used in the replay attack.

Some researchers have claimed that a replay attack can be performed in ZigBee networks only in cases where there is no security policy implemented in the network.[13] However, this article shows that even when network security is implemented, there is still a possibility to perform the replay attack and execute some harmful actions in the network.

Other researchers have suggested that a time-stamping mechanism should be integrated into the encryption process of ZigBee without giving any details about how to do that.[14] ZigBee already uses a sequence number that is included in the encryption process. Thus the attacker can copy the whole frame with its sequence number and the frame will be considered valid after passing the frame counter check. In addition, implementing such a mechanism will cost the co-ordinator more storage space for saving the last timestamp of all the devices in the network, and every end device has to have its own clock synchronised with the co-ordinator. If something goes wrong, such as a power failure or the device rebooting, the end device will not be able to send any data on the network because it is not synchronised. What is more, the end devices in sleep mode still need to keep their clocks counting, which will consume more power.

Another problem arises from the fact that the ZigBee specification does not provide any policy about when the Trust Centre (TC) should change the network NWK key. Instead, it leaves this decision to the ZigBee network administrator to choose the correct time for updating this key.[15] If an attacker physically accesses or steals any connected network device, he will be able to obtain the network key by using appropriate tools. That is because the security keys are stored in the devices in plain text. In this case, the attacker will be able to decrypt the captured frames or inject his own frames to the network. What is more, he will have the ability to start denial of service (DoS) attacks by creating a frame with the maximum frame counter value 0xFFFFFFFF. If any device on the network receives an authentic frame with this frame counter value, it will stop accepting any new frames because the new incoming frames have frame counter values smaller than 0xFFFFFFFF. To solve this problem, the co-ordinator must change the NWK key as soon as possible after this attack occurs.

"If the frame counter has been encrypted along with the NWK payload, it will reduce the chances of the attacker guessing the correct time to start the replay attack. However, there is still the potential for the attack to succeed even if the attacker cannot figure out the frame counter value of the receiver"

This article suggests some specific time points when the co-ordinator has to change the NWK key, based on security and management considerations, which will also help solve this problem. All the solutions suggested so far cannot stop

a replay attack when the frame counter is reset. If the frame counter has been encrypted along with the NWK payload, it will reduce the chances of the attacker guessing the correct time to start the replay attack. However, there is still the potential for the attack to succeed even if the attacker cannot figure out the frame counter value of the receiver.

Another way to prevent the old repeated frames being accepted by the victim is to ensure authentication failure, which means that the MIC should be calculated by using different NWK keys. This is the purpose of this article. If the frame counter resets to zero, the NWK key – which is used by the network – must be changed. Otherwise, the network will be vulnerable to the replay attack.

Subject to attacks

So to recap, the frame counter is, theoretically, an efficient way to block a replay attack. However, the ZigBee network is still subject to attacks because using the frame counter alone seems unable to block the replay attack effectively. The previously suggested solution of using a timestamp is also not sufficient because of its high storage and computing requirements. In addition, no clear strategy is defined regarding when the network administrator should change the NWK key, especially in the case of a physical attack in the network. Also, frame encryption will not prevent the attacker from copying some frames and resending them back into the network when he has the chance – namely, when the network is still using the same old network key of the injected frames, and the last received frame counter value is smaller than that of the injected frame ones.

The following examples show when the network is vulnerable to attacks:

- When the co-ordinator restarts due to some reason such as power failure or the attacker gets access to the power supply and turns off the power, the frame counter will be restored to zero, which will provide the attacker with a chance to start an attack.
- The frame counter hits the maximum value: a deadlock will appear in the network once the frame counter reaches its maximum value 0xFFFFFFFF, which will force the network administrator to restart the network co-ordinator for resetting the frame counter value.[16,17]

Proposed solution

Keeping the same old network key after the co-ordinator restarts must be avoided in a ZigBee network. Since the frame counter cannot be stopped from recounting, this research focuses on changing the network key automatically every time the frame counter resets. To do that, more than one network key needs to be stored in the co-ordinator (in this research, eight keys are suggested). Therefore, the co-ordinator can always switch to a new network key when the frame counter resets.

In addition, these keys should be renewed after being used by the co-ordinator. We suggest two methods for generating the new keys.

"The keys are generated and stored inside the ZigBee co-ordinator, which ensures a high degree of security and is suitable for equipment with limited resources"

First, the ZigBee co-ordinator generates these keys randomly. When the stored keys have been used, the co-ordinator will randomly generate a new group of eight 128-bit keys and store these keys in the non-volatile memory. The advantage of this method is that the keys are generated and stored inside the ZigBee co-ordinator, which ensures a high degree of security and is suitable for equipment with limited resources. By using the C language rand() and srand(time) functions to generate the random keys – with the latter function providing the seed to the former – the sequence of the random numbers will not be repeated, because the seed of the random function is different every time.

Second, the co-ordinator will randomly generate two strings, which are required to generate a group of eight 128-bit network keys (as shown in Figure 3). These strings are variable-length, making them too difficult to be guessed. After the strings are generated, the system will process them by using the hashing algorithms MD5 and SHA-256 to generate a fixed length (512-bit output) for each given string. To make the keys more randomised, the process of hashing algorithms can be repeated many times. Each 512-bit output will be partitioned into four 128-bit keys. As a result, eight keys will be created by using two random strings. This process is executed on the co-ordinator. The ZigBee co-ordinator will store these keys instead of the old keys in its non-volatile memory. Because the random strings could be of any length, the co-ordinator keeps its keys fresh. The advantage of this method is that it depends on variable-length random strings, which makes the keys more randomised and difficult to crack by offline password guessing attacks. The second step of the key-generating process (MD5 and SHA-256) could also run a random number of times. These random times depend on the strength of the hardware equipment of the ZigBee co-ordinator, and also depend on the security environment and requirements.

The other problem of the network deadlock, which happens when the frame counter hits the maximum value 0xFFFFFFFF, is also fixed by renewing the NWK key before the frame counter hits the maximum value. Renewing the NWK key will force the frame counter to be reset to zero and avoid the ZigBee network deadlock. If network deadlock does occur, the whole system needs to be restarted, including the end devices, which will incur serious problems.

The co-ordinator should take the value 0xFFFFF000, which is neither too large nor too small, as a threshold for the frame counter. If the frame counter exceeds this value, the co-ordinator will automatically change the NWK key instead of restarting the network without changing the key. The suggested value will give flexibility to the proposed solution, where the other devices could be very active, and the network can still send 4,096 frames normally without any problems until the co-ordinator successfully changes the key and resets the frame counter value.

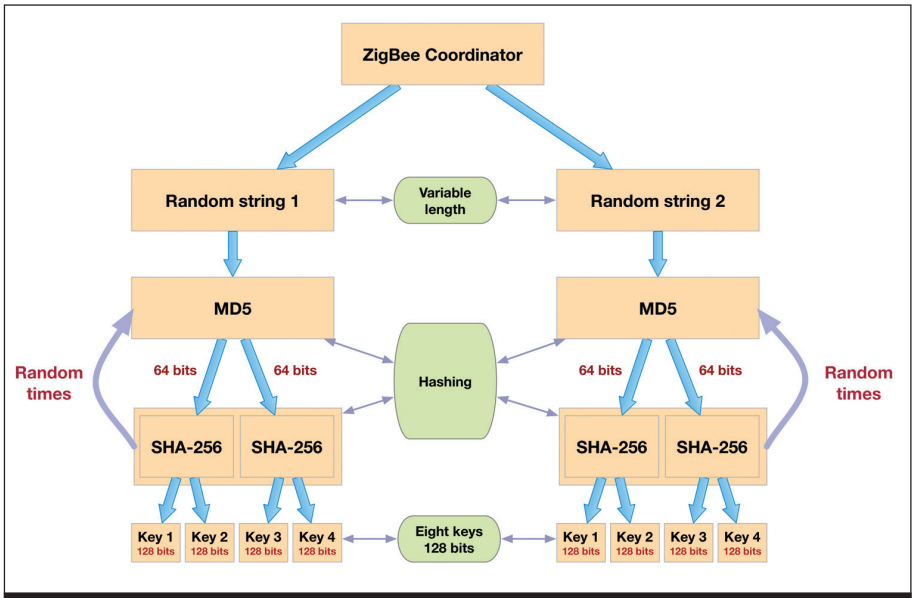


Figure 3: NWK key generating procedure.

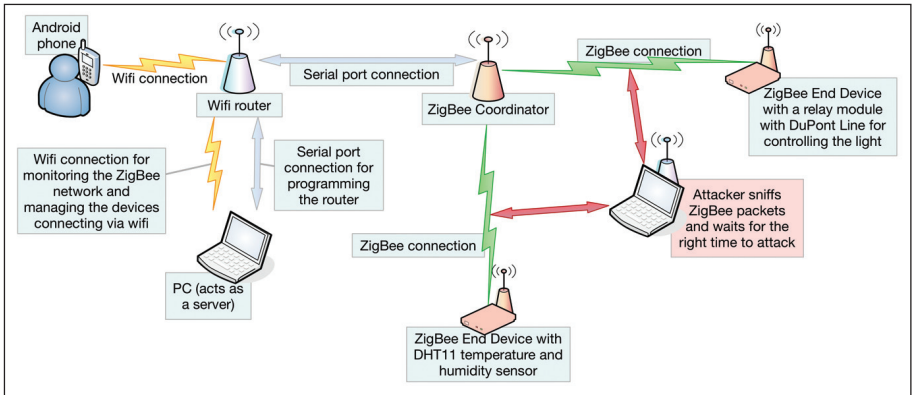


Figure 4: System architecture.

ZigBee and wifi network

In order to carry out the experiment for this research, two networks were installed (shown in Figure 4) as detailed below:

- ZigBee network: composed of a co-ordinator and two end devices (one working as a sensor and the other as a switch).
- Wifi network: composed of a wireless router, a laptop and a smartphone.

Sniffing the ZigBee network

In this system structure, the co-ordinator plays the TC role and the network is secured using NWK layer security. The installed network key is 01 03 05 07 09 0B 0D 0F 00 02 04 06 08 0A 0C 0D. The TC will allow other devices (routers and end devices) to join the ZigBee network. Once these new devices send join requests to the TC and these requests are accepted, the TC will give them the active network key. After that, these newly joined devices will be able to send/receive frames encrypted with the NWK key.

Figure 5 shows a secure ZigBee network frame which is sniffed by a sniffing tool CC2531 dongle USB and displayed with the Ubiqua protocol analyser application. This network contains two devices – a co-ordinator with the network address 0x0000 and an end device with the network address 0x41E8. The end device is attached with a switch to be able to turn the light on and off. As shown, the network runs normally. End devices send data (humidity and temperature values) and receive commands (switching the light). Wifi network users can access the ZigBee network resources and control the ZigBee end devices. The attacker listens to the ZigBee network frames and may sniff them for many frames. Since the frames are encrypted, the attacker cannot figure out the contents of these captured frames. The packet analyser application can display the information about the captured frames, such as which layer these frames belong to and which security policy is implemented for these frames.

In this experiment, the frame 41 88 B8 33 33 FF FF 00 00 08 02 FF FF 00 00 1E 5A 28 E9 00 00 00 6A CA C4 08 00 4B 12 00 00 7F 8C 6A 4F A2 DE 2F 3D 7F 97 3C 1C 1C FF FF with ID 289 is chosen to perform the attack. It is a NWK layer data frame and sent by the co-ordinator. The frame counter of this frame is 0x000000E9 hex (233 decimal).

To replay this frame into the network, the frame counter of the co-ordinator outgoing frames must be less than 233. When the co-ordinator is restarted, the frame counter will be initialised to zero. That will give the attacker the chance to perform the replay attack. Otherwise, this frame has no effect on the network and will be considered as an old frame because its frame counter value is less than the co-ordinator outgoing frame counter value.

In this experiment, the co-ordinator had been restarted. After that, the co-ordinator establishes the ZigBee network again with the same old network key. The frame counter automatically reset to zero and the network works normally again. The attacker injects the frame which is responsible for turning on the light mentioned above. In this experiment, SmartRF Studio 7 has been used for the injection process. As shown in Figure 6, the frame is injected into the network. The victim device receives the injected frame and the light is turned on (shown in Figure 7). Even though the security process is implemented, the attack still succeeds and the injected frame passes the security check as explained below:

- Frame integrity check: the injected frame will be validated as a valid frame because the frame content is not changed. It has been copied and resent into the network. Therefore, it does not matter whether the bit length of MIC is 0, 32, 64 or 128.

- Device authentication service: the injected frame will also pass the authentication check which is based on the same security key. That is because the received frame is already an authentic frame that was sent over the network.
- Data encryption: the injected frame is encrypted with the same security key, which is the network layer key. Therefore, after the injected frame arrives at the victim device, the victim device will decrypt the payload and the command carried by the frame will be executed.

Blocking the attack

Now let's look at the same network with the same replay attack but after the proposed solution is implemented. The keys (shown in Table 1) are stored in the co-ordinator and some programming code is added to the booting process of the co-ordinator.

During the booting process of the co-ordinator, this code lets the co-ordinator check the key index parameter and pick a new key to serve as a network key. This method maintains the refreshment of the network keys. In addition, after the co-ordinator is restarted, the network frames are encrypted and the MIC is calculated using a different NWK key. Therefore, the frames that are copied by the attacker to be used after the co-ordinator is restarted will be useless and considered as 'bad frames'. As shown in Figure 8, when the attacker copied the frame, the NWK key was 01 03 05 07 09 0B 0D 0F 00 02 04 06 08 0A 0C 0D. After the co-ordinator is restarted, it starts using the next key, which is 0A 0A 0A 0A 0A 0A 0A 0B 0B 0B 0B 0B 0B 0B 0B. The injected frames did not pass the security tests (authentication and encryption), so the light is still off and the attack failed as shown in Figure 9.

The proposed solution has no extra cost other than asking the co-ordinator to change the key when it is restarted. There is no extra cost for the end devices because, in all cases, they will ask for the NWK key when they join the network. Compared with the other solution (timestamp), this proposed solution will just take few

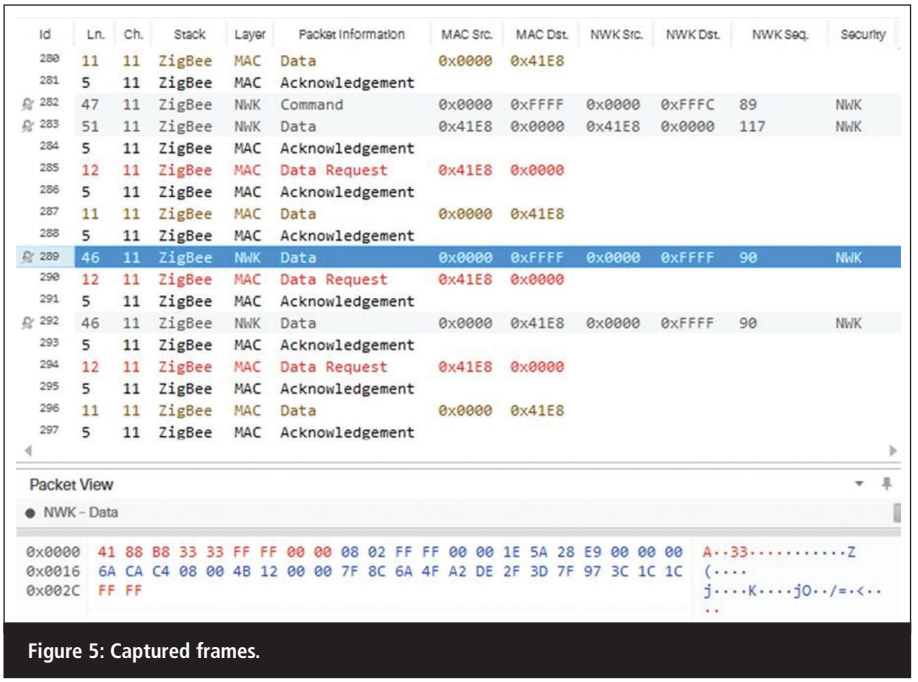


Figure 5: Captured frames.

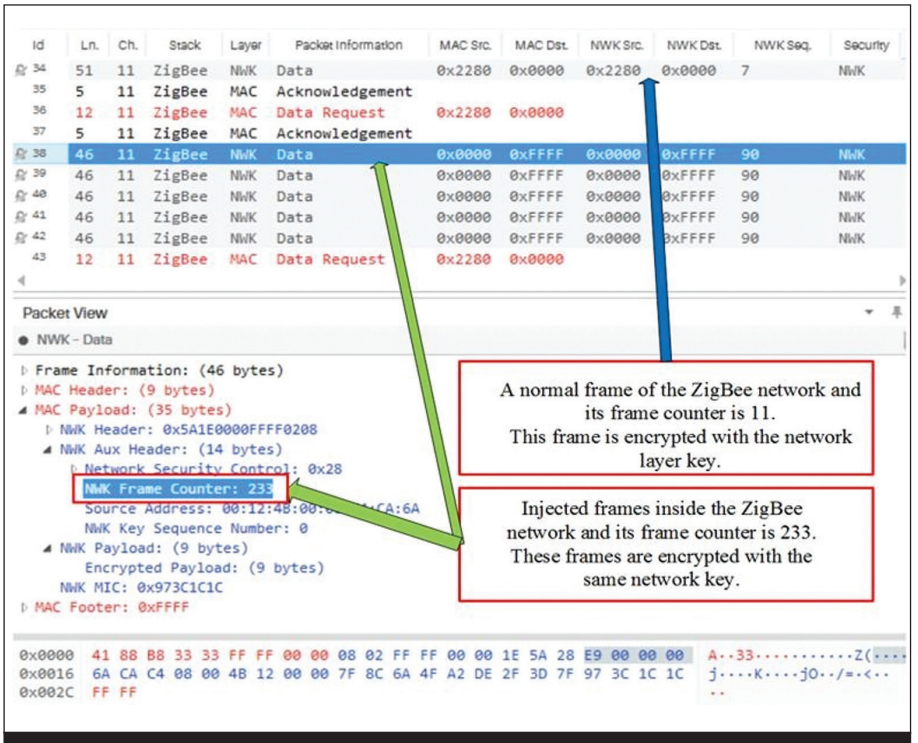


Figure 6: Injection into the ZigBee network using the same NWK key.

Key Index	Key value
1	01 03 05 07 09 0B 0D 0F 00 02 04 06 08 0A 0C 0D
2	0A 0A 0A 0A 0A 0A 0A 0B 0B 0B 0B 0B 0B 0B 0B
3	3C 5A BC BA 5C 06 F2 E2 13 23 B3 02 0D 3B A3 13
4	89 B0 44 7E A7 C6 80 37 CB 25 18 61 83 CE A0 37
5	2A A1 AB A4 31 7F 80 E1 BE 17 AC 7D B2 FC 3F 1F
6	50 C2 0D 6F E8 C5 A7 5B 3A 80 6A D2 FC 44 15 92
7	C4 8D A7 82 63 8B 05 B9 8F 71 B6 9A BD F3 59 C7
8	C3 EA 34 A4 73 58 CA E8 C1 36 E9 46 AA 9B D6 E8

Table 1: NWK keys stored in the co-ordinator.

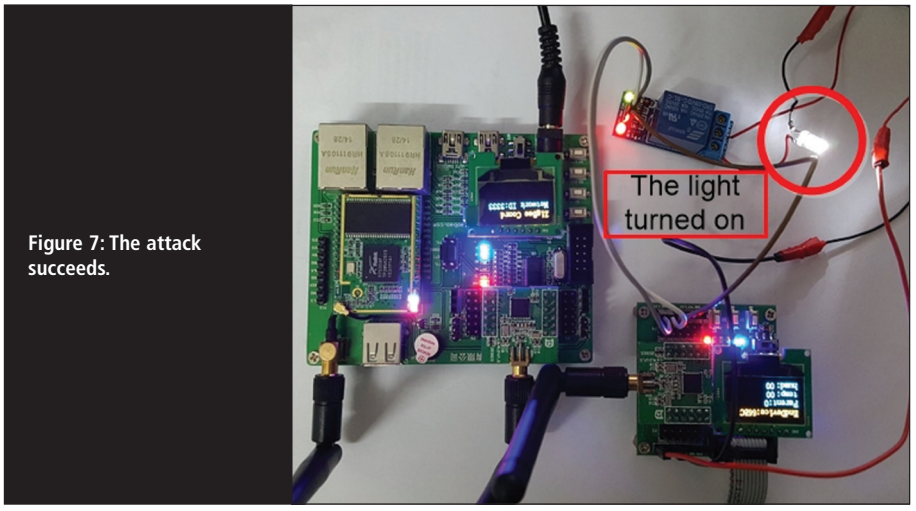


Figure 7: The attack succeeds.

moments when randomly generating the new NWK keys. The proposed solution requirements are illustrated in Table 2.

Conclusion

ZigBee technology offers reliable communication techniques by using devices with low power consumption. It uses a variety of security mechanisms. But some scenarios have proved that there are still some threats to ZigBee security.

As we've seen, ZigBee security can be invoked when the frame counters are restarted and while the ZigBee network still uses the same network key. What is more, preconfiguring the network key in the devices but being unable to change this key is very harmful to ZigBee security since it is available for a replay attack. It is not recommended to use this type of security because there is no other way to block the replay attack except by changing the network key.

We suggest storing multiple network keys in the co-ordinator and renewing these keys when they are used in the network, and we offer two key-generating methods to prevent a key-guessing attack. Our key-renewing method and key-generating methods can block the replay attack efficiently.

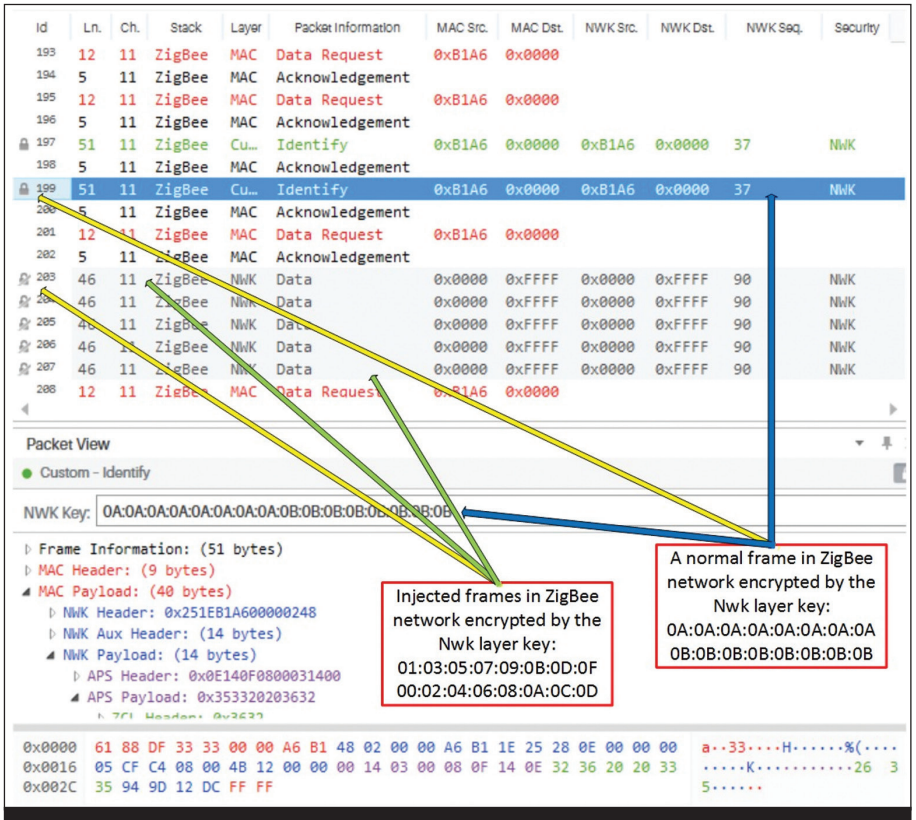


Figure 8: Injection into the network using a different NWK key.

Device type	Number of keys	Memory requirement for storing keys	The moment of changing the key
Co-ordinator	8	8*128= 1024 bits	Every time it is being restarted
End device	1	1*128=128 bits	When joining the network

Table 2: Storage needs of the proposed solution.

About the authors

Fadi Farha received his MS degree in computer science from the University of Science and Technology, Beijing, China in 2017. His current research interests include computer architecture and hardware security.

Chen Hongsong received a PhD from the Department of Computer Science at the Harbin Institute of Technology, China in 2006. He was a visiting scholar at Purdue University in 2013-2014. He is currently an associate professor in the Department of Computer Science, University of Science and Technology, Beijing, China. His current research interests include wireless network security, attack and detection modelling and cloud computing security.

References

1. Gislason, D. 'Zigbee Wireless Networking'. Newnes, 2008. Accessed Jan 2018. www.sciencedirect.com/science/book/9780750685979.
2. Iyengar, SS, Parameshwaran, N; Phoha, V; Balakrishanan, N; Okaye, C. 'Fundamentals of Sensor Network Programming: Applications and Technology'. John Wiley & Sons, 2011.
3. '802.15.4-2011 – IEEE Standard for Local and metropolitan area networks – Part 15.4: Low-Rate Wireless Personal Area Networks(LR-WPANs'. IEEE Computer Society, 2011. Accessed

Jan 2018. http://ieeexplore.ieee.org/document/6012487/.
4. Imran A; Zualkernan, AR; Al-Ali, M; Jabbar, A; Zabalawi, I; Wasfy, A. 'Info Pods.: ZigBee-based remote information monitoring devices for smart-homes'. IEEE Transactions on Consumer Electronics, vol.55, no.3, Aug 2009, pp.1221-1226.
5. Li, H; Jia, Z; Xue, X. 'Application and Analysis of ZigBee Security Services Specification'. In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing (vol.2, pp.494497). IEEE.
6. Sun, M; & Qian, Y. 'Study and Application of Security Based on ZigBee Standard'. In 2011 Third International Conference on Multimedia Information Networking and Security (pp.508511). IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/6103824/.
7. Choi, K; Yun, M; Chae, K; Kim, M. 'An enhanced key management using ZigBee Pro for wireless sensor networks'. In The International Conference on Information Network, 2012, pp.399403. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/6164409/.
8. Alcaraz C; Lopez, J. 'A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems'. IEEE Transactions on Systems, Man, and Cybernetics, Part C Applications and Reviews, vol.40, no.4, July 2010.
9. Vidgren, N; Haataja, K; Patino-Andres, JL; Ramirez-Sanchis, JJ; Toivanen, P. 'Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned'. In 2013 46th Hawaii International Conference on System Sciences, pp.51325138.

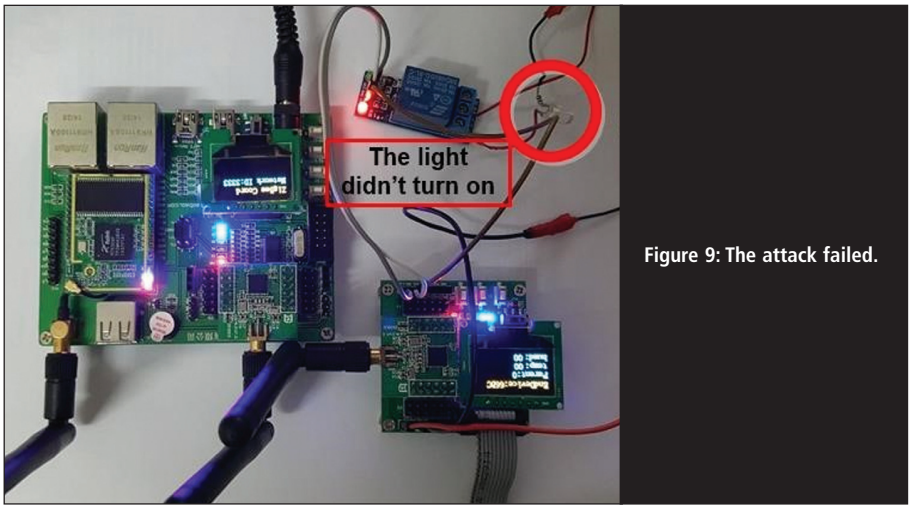


Figure 9: The attack failed.

IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/6480466/.
10. Cache, J; Wright, J; Liu, V. 'Hacking Exposed Wireless: Wireless Security Secrets and Solutions'. McGraw-Hill, Second Edition, Jul 2010.
11. Durech, J; Franekova, M. 'Security attacks to ZigBee technology and their practical realization'. SAMI 2014 – IEEE 12th International Symposium on Applied Machine Intelligence and Informatics, Proceedings, 345349. Accessed Jan 2018. http://ieeexplore.ieee.org/document/6822436/.
12. Li, H; Jia, Z; Xue, X. 'Application and Analysis of ZigBee Security Services Specification'. In 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp.494497. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/5480941/.
13. Yang, B. 'Study on Security of Wireless Sensor Network Based on ZigBee Standard'. In 2009 International Conference on Computational Intelligence and Security, pp.426430. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/5376148/.
14. Olawumi, O; Haataja, K; Asikainen, M; Vidgren, N; Toivanen, P. 'Three practical attacks against ZigBee security: Attack scenario definitions, practical experiments, countermeasures, and lessons learned'. In 2014 14th International Conference on Hybrid Intelligent Systems, pp.199206. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/7086198/.
15. Lee, JS; Su, YW; Shen, CC. 'A comparative study of wireless protocols: Bluetooth, UWB, ZigBee and Wifi'. Proceedings of the 33rd Annual Conference of the IEEE Industrial Electronics Society (IECON), pp.46-51, Nov 2007.
16. Chunqing, L; Jiancheng, Z. 'Research of ZigBee's Data Security and Protection'. In 2009 International Forum on Computer Science-Technology and Applications, vol.1, pp.298302. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/5385074/.
17. Kulkarni, S; Ghosh, U; Pasupuleti, H. 'Considering security for ZigBee protocol using message authentication code'. In 2015 Annual IEEE India Conference (INDICON), pp.16. IEEE. Accessed Jan 2018. http://ieeexplore.ieee.org/document/7443625/.

The Firewall

Tackling push payment scams

Colin Tankard, Digital Pathways

The Payment Systems Regulator (PSR) has announced an industry-wide action plan to tackle push payment scams. A push payment is where a bank or other payment service provider (PSP) is instructed to transfer money from a customer's account to another account. When a customer gives consent for a transaction to be processed, it becomes an authorised push payment.

Push payment scams are the second-biggest cause of payment fraud in the UK, claiming £100m from 19,000 people between January and June 2017 alone. Authorised push payment scams occur when customers are tricked into authorising payments to an account that doesn't belong to their intended payee.

From a digital security perspective, authorised push payment scams are a type of man-in-the-middle attack. These attacks happen when digital communications between two systems are intercepted by an outsider. There are several forms of man-in-the-middle attack, but two are especially common.

Email hijacking: Hackers intercept email communications between an organisation and its customers. They use this tactic to take advantage of scenarios where a customer is about to transfer money. Businesses, such as law firms or builders, are prime targets due to the large sums of money typically involved in a transaction.

Once they have breached a company's systems, the hackers will monitor emails, or even VoIP calls, until the company requests a payment from its customer; the hackers will then intercept the communication. Their aim is to trick the customer into paying money into their account instead. They do this by sending emails that are indistinguishable from the company's genuine ones. By changing account details, customers unwittingly transfer thousands of pounds to the fraudsters, in the belief that it is a legitimate account.

Wifi eavesdropping: Using a portable wifi node, such as the Pineapple, a hacker will broadcast a free wifi hotspot from a public place, such as a coffee shop, and give it a legitimate-sounding name. The hacker will seek to exploit anyone who connects to the hotspot by spoofing web pages to collect log-in details, or by breaking the connection once you log in – for example to your online banking – leaving the connection to your account open for themselves to access.

Companies need to ensure their communications are secure and authenticated. For example, emails should always be encrypted and verified both on receipt and at opening. These verifications should be part of the process and not affected by the receiver switching off read receipts, such as in Outlook. Likewise, if data is stored in the cloud and clients are directed to services, the site should be secured with encryption, with the keys held outside of the hosting provider of the service and always with a secure communication tunnel between the client and the data source.

Users also need to be aware that communications they receive could be compromised and so they need to take care in checking the validity and even double-checking the instructions with the originator.

The PSR is bringing in regulations to force organisations to take better steps to prevent man-in-the-middle-attacks, as victims are not covered for losses under current legislation. However, one strand of the PSR's approach is to enforce a reimbursement in the event of these scams. This would shift a large proportion of liability from customers to financial organisations.

The direct consequence will be that all organisations and PSPs will have to reinforce their identification and authentication mechanisms, as well as their transaction data analytics systems, to reduce the number of opportunities to commit such scams.

EVENTS CALENDAR

2–4 February 2018
REcon Brussels
Brussels, Belgium
https://recon.cx

7–8 February 2018
Manusec Europe
Munich, Germany
www.manusecevent.com/europe/

9 February 2018
Hackron
Canary Islands, Spain
www.hackron.com

16–18 February 2018
Munich Security Conference
Munich, Germany
www.securityconference.de/en/

20 February 2018
European Information Security Summit
London, UK
https://biztechevents.co.uk/teiss/

22–24 February 2018
International Conference on Information Systems Security & Privacy
Funchal, Portugal
http://www.icissp.org/

22–23 February 2018
DevSecCon Singapore
Singapore
www.devseccon.com/singapore-2018/

27 February – 3 March 2018
NullCon
Goa, India
http://nullcon.net/website/

2–4 March 2018
Hacktech
Pasadena, CA, US
http://hacktech.io