ELSEVIER

network SECURITY

ISSN 1353-4858 October 2011

www.networksecuritynewsletter.com

Featured this issue:

Android insecurity

The smartphone and tablet operating system Android is four years old, but its developers seem to have learned little about security in that time. Although loosely based on the Linux kernel, the OS has a number of features that make it intrinsically insecure.

There has been a continuous flow of reports of trojanised malware found not just in rogue online app stores but also in Google's official Android Market. Some analysts compare the situation to the bad old days of Windows and believe that installation of security software is now essential. And still more analysts believe that the most crucial step of all is user education, discovers Steve Gold.

Full story on page 5…

Frametrapping the framebusting defence

Framebusting code can prevent one type of clickjacking, but new features of HTML 5 allow a malicious developer to nullify this protection.

New iframe attributes – currently supported only by Google Chrome but likely to be introduced on other browsers – can bypass the protection mechanisms provided by framebusting code. Although the new iframe attributes have been introduced to improve the user experience, they can also be exploited to launch successful web attacks, including clickjacking, explain Aditya Sood and Richard Enbody of Michigan State University.

Full story on page 8…

Defending the network several times over

Modern networks can be attacked in a variety of ways, meaning that companies need different types of protection. James Harris of ZyXEL explains that companies need to cover all bases when it comes to information security.

Defence in depth is a crucial technique for small to medium-size businesses (SMBs) that want to protect themselves against intrusion. Condensing multi-layered protection into a single device, updated by the vendor, provides the best protection for resource-constrained companies. The more points protection that a company covers, the more likely it is to fend off the majority of generic attacks on the Internet.

Full story on page 12…

Web security under threat

The technologies that secure the web have been under a lot of strain. The hacking of Diginotar, the Dutch Certificate Authority (CA), and the revelation of potentially dangerous flaws in SSL/TSL protocols have renewed debate about whether current technologies are up to the job.

Diginotar was breached by an Iranian hacker who generated more than 530 rogue SSL and EV-SSL certificates. This first came to light when Google users

Continued on page 2…

Contents

Editorial Office:
Elsevier Ltd
The Boulevard, Langford Lane, Kidlington,
Oxford, OX5 1GB, United Kingdom
Fax: +44 (0)1865 843973
Web: www.networksecuritynewsletter.com

Publisher: Greg Valero
E-mail: g.valero@elsevier.com

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

Senior Editor: Sarah Gordon

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

Subscription Information
An annual subscription to Network Security includes 12 issues and online access for up to 5 users.
Prices:
€1112 for all European countries & Iran
US$1244 for all countries except Europe and Japan
¥147 525 for Japan
(Prices valid until 31 December 2011)
To subscribe send payment to the address above.
Tel: +44 (0)1865 843687/Fax: +44 (0)1865 834971
Email: commsales@elsevier.com,
or via www.networksecuritynewsletter.com
Subscriptions run for 12 months, from the date payment is received. Periodicals postage is paid at Rahway, NJ 07065, USA. Postmaster send all USA address corrections to: Network Security, 365 Blair Road, Avenel, NJ 07001, USA

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

...Continued from page

in Iran reported problems, but it's now known that numerous domains have been threatened. The hacker claimed to be the same person who previously breached Comodo, another CA. Diginotar has since been removed as a root CA from all main browsers, and the US-owned company has gone into voluntary bankruptcy.

For a short period, users of Windows XP and Server 2003 were left vulnerable when an update issued by Microsoft, designed to block Diginotar certificates, only removed a limited number of them and would still have treated other certificates as valid.

Meanwhile, two researchers claim to have unveiled a significant flaw in the operation of SSL and Transport Layer Security (TLS). At the Ekoparty security conference in Buenos Aires, Thai Duong and Juliano Rizzo released details of a technique that uses a plaintext recovery attack to break the encryption of online sessions. The weakness it exploits has been known about for some time but, until now, has been regarded as largely theoretical.

The attack exploits the way in which TLS block ciphers operate, using Cipher Block Chaining (CBC). With this method, each block of plaintext is first XOR'd against the previous, encrypted block. This avoids the problem, encountered when each block is simply encrypted individually, of repeated blocks of ciphertext being identical whenever the plaintext is the same. Such repetitions are often the basis for successful cryptanalysis and subsequent decryption. In the CBC approach, the first block of text is XOR'd against an Initialisation Vector (IV).

The weakness in TLS 1.0 is that the IV is not random and unpredictable, as it should be. Instead, the final ciphertext block of the previous message is used. This opens the possibility of an attacker being able to trick the user into sending a given message so that the encrypted version can be compared to the plaintext copy. This might be achieved with a cross-site scripting (XSS) exploit.

Exploiting this vulnerability is not easy. The attacker must have a great deal of control over the network, in order to sniff the traffic, and must be able to inject data into the target's session. It's also slow: decrypting one byte takes a few seconds and a typical encrypted cookie might take as much as half an hour. However, the researchers say they expect this to get faster.

The vulnerability affects TLS 1.0. However, while TLS 1.1 and 1.2 are not affected, they are also not properly supported by the vast majority of browsers and websites. Other technologies that use TLS 1.0, such as instant messaging software and Virtual Private Networking (VPN) systems, may be at risk too.

The researchers have produced proof of concept Javascript code called Browser Exploit Against SSL/TLS (Beast). Working with a network sniffer, this decrypts cookies from a website, which would enable an attacker to gain access to restricted accounts – for example, on PayPal.

Software vendors such as Microsoft and Google have acknowledged the feasibility of the attack but have downplayed the likelihood of exploits appearing in the wild. Google has since released a developer version of the Chrome browser that it says defeats this attack method. At the time of writing, Microsoft said it was preparing a fix, and has also suggested switching to stream encryption – for example, using RC4 – rather than the AES block encryption normally used with TLS 1.0.

Mozilla has stated on its blog that Firefox is not vulnerable. "The technical details of the attack require the ability to completely control the content of connections originating in the browser, which Firefox does not allow," said the post.

In the wake of the controversy surrounding Beast, Qualys has announced its support for the Convergence project, initiated by security researcher Moxie Marlinspike, who has previously disclosed flaws in SSL technology. According to Marlinspike, the SSL ecosystem has too many CAs and too many digital signatures. A breach, like the one suffered by Diginotar, can cause major disruption to the system. The Convergence system uses a small number of loosely confederated and trusted 'notary' servers that can authenticate SSL certificates by comparing the

Continued on page 20...

In brief

Flaws in Chrome

More than a quarter of extensions for Google Chrome analysed by three researchers in the US contained vulnerabilities. Adrienne Porter Felt, Nicholas Carlini and Prateek Saxena at the University of California, Berkeley, analysed 100 extensions, including the 50 most popular and seven that are each used by 300,000 people or more. They found that 27 contained flaws that could be exploited across the web or via unsecured wifi. The weaknesses were all based on Javascript injection vulnerabilities. The researchers identified a total of 51 exploitable flaws across the 27 extensions. There's more information here: <http://www.adrienneporterfelt.com/blog/?p=226>.

German authorities may be using illegal back door

The German police force's use of 'lawful interception' malware may be going beyond the limits of the law, according to hacker collective the Chaos Computer Club (CCC). German courts allow the use of the so-called 'Bundestrojaner' ('federal trojan') in instances where wiretapping has been authorised. This trojan includes functions such as recording Skype conversations. However, the CCC says it has reverse-engineered the code and has discovered functionality that is not allowed by law. This includes the ability to download from the Internet, run remote code and allow remote access to the computer. Sophos says it has also analysed the code and confirms that it is able to eavesdrop on several communications channels, including Skype, MSN Messenger and Yahoo Messenger; record Skype audio calls; log keystrokes in a number of web browsers; take screengrabs; and communicate with a remote website. There has been no confirmation that the malware, also known as '0zapftis' and 'R2D2', that was examined by the CCC is in fact the official police trojan.

Another botnet taken offline

Microsoft has again taken down a botnet using legal avenues. The Kelihos botnet commanded 40,000 machines and was used for distributing spam, mounting DDoS attacks and other criminal activities. Following its successes with Rustock and Waledac, Microsoft mounted Operation b79 as part of its Microsoft Active Response for Security (MARS) initiative. Unlike previous operations, however, this one involved a named defendant – Dominique Piatti, whose dotFREE Group SRO company is alleged to have hosted Command and Control (C&C) servers using the domain cz.cc. Microsoft obtained a court order allowing it to take control of cz.cc, although it is working with Piatti to determine which subdomains might be in use for legitimate purposes. Kaspersky also played a key role in the operation, reverse engineering the bot malware, cracking the communication protocol, and developing tools to attack the peer-to-peer infrastructure and sinkhole the botnet.

New CESG scheme for IT security professionals

The Communications Electronics Security Group (CESG) – the information assurance authority branch of GCHQ – has unveiled details of a new certification scheme for IT security professionals. The scheme will be managed initially by the APM Group and the British Computer Society (BCS, the Chartered Institute for IT). The scheme will focus on developing and delivering an IA Specialist Certification Scheme for anyone working in any government department. It will certify IA specialists against specific IA roles and skills aligned to the competency framework – Skills for the Information Age (SFIA) and BCS' SFIAplus. It will cover six roles: security and information risk advisor; security architect; accreditor; IA auditor; IT security officer; and communications security officer. There will be certification available at three levels for each role: practitioner; senior practitioner; and lead practitioner.

Market expands for database security

As databases connect to an ever-growing list of applications, there is a burgeoning need for products to secure them. Forrester Research has concluded that the market for such products will grow by 20%, reaching $1.2bn by 2014. "The database security market is likely to converge with the overall data security market in the future, as DBMS vendors extend the security features that are bundled with their products," wrote Noel Yuhanna in a recent report. "Larger database security vendors such as Fortinet, IBM, McAfee and Oracle will continue to dominate the database security market and are likely to acquire independent vendors to fill gaps in their security portfolio." Another report by Enterprise Strategy Group (ESG) says there has been consistent under-investment in database security and that, combined with the perceived danger of Advanced Persistent Threats (APTs), a major rise in data volumes and the appearance of multiple access points, including mobile, this is now a major concern for IT departments.

GPU cracks passwords in seconds

A £30 graphics card can now be used to process as many as 158 million passwords a second, claims web hosting firm UKFast. The company carried out research as part of Cyber Security Awareness Month. It found that an nVidia GeForce GT220 graphics card can be used as a processor to run password-cracking software. A six-character password could be cracked in 12 seconds, a seven-character one in under five minutes and an eight-character password in four hours. Using high-end graphics cards, it's possible to run through 10.3 billion passwords a second, so that even eight-character passwords might be brute-forced in just a few minutes.

Worried online banking users

Research by McAfee shows that, while 92% of UK bank account users now access their accounts online, only 33% are happy about it: the rest do not feel confident that their details are completely safe. And they may have good reason: it seems that only 39% of online banking users have comprehensive security software installed on their computers. The majority – 54% – use only basic anti-virus. Password security is also an issue: 16% of users write their login credentials on a piece of paper, 15% keep them somewhere on their computers or smartphones, 23% use an easy to remember password, such as a maiden name or pet's name, and 15% use an easy to remember date – the kinds of details that might be found on their Facebook profiles. Nearly a third (30%) reuse the same password elsewhere.

High-risk mobile users are your best workers

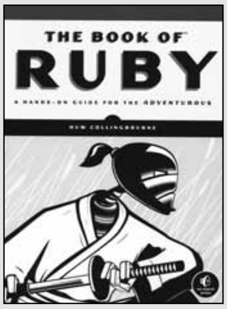
Research by Forrester suggests that mobile workers – regarded as high-risk from a security point of view – might also be an organisation's most valuable people. A survey of nearly 5,000 workers found that the 20% that are mobile, using laptops, tablets and smartphones to connect to the corporate network, also create the most value for money, being highly productive. The report recommends that those firms looking to reduce the risk from mobile systems should not focus on the platforms but on specific applications. This is because it's the applications that actually create the vulnerabilities in an organisation's defences. The report, 'State of the Workforce Technology Adoption 2011', is available here: <http://www.forrester.com/rb/Research/state_of_workforce_technology_adoption_us_benchmark/q/id/60894/t/2>.

Massive ID theft arrests

US law enforcement authorities have made what they claim to be the largest number of arrests connected with an identity theft and credit card fraud operation. Arrest warrants were issued for 111 people, with 86 soon ending up in custody. The remaining 25 are still wanted. At the culmination of the two year-long Operation Swiper, the arrested people – who are said to have operated in five gangs – included bank tellers, retail workers, restaurant workers and alleged professional criminals. They are accused of stealing credit card data, obtaining it from carder forums and from 'suppliers' in places such as Russia, Libya and China. Fake or cloned cards were then used to buy goods in US stores.

Reviews

BOOK REVIEW



The Book of Ruby

Huw Collingbourne.
Published by No Starch Press
(ISBN: 978-1-59327-294-4).
Price: $39.95, 370pgs, paperback.

The Ruby programming language has acquired particular relevance for security professionals and penetration testers. Its simple syntax, weak typing and widespread adoption on all popular platforms makes it ideal for hacking together quick scripts or tools to get the job done. On the other hand, it's an object-oriented environment that supports the creation of complex programs and frameworks. Add the support provided by an enthusiastic community, with thousands of ready-made modules, or 'mixins', and you have a platform for sophisticated programming. And, of course, it is the language of Metasploit.

Author Huw Collingbourne starts off in a very conventional manner. Yes, there is a 'Hello world' program – all one line of it. But, in a manner suiting the nature of the language, before he gets into the basic stuff (control structures and variable types) he quickly tackles the object oriented features of Ruby. To give you an idea of the pace, the author is talking about superclasses and subclasses by page 17.

It will help if you have some programming experience already. In fact, I think this approach probably mirrors how the majority of readers will be approaching this book. While some people may choose Ruby as their first-ever programming language – and it certainly wouldn't be a bad choice – it's more likely that most readers will have at least hacked out some Perl, PHP, JavaScript or possibly Python scripts in the past. They'll be picking up this book because they have seen the rise in popularity of Ruby, and have watched its widespread deployment, and need to get up to speed.

If you're in that position, this is definitely the book for you. Presented in No Starch's usual clean and accessible style, and with Collingbourne's clear prose, you'll be writing basic scripts in no time. Of course, while Ruby lends itself to quick and dirty programming, it also has the structures and features to support complex, large-scale and carefully developed code (we get exception handling introduced in Chapter 9). There's a good section on modules – a fundamental element in developing reusable code – and how they can be used as namespaces.

There are short chapters on YAML and Marshal, Ruby's methods of serialising data for storage and retrieval. And there's another on regular expressions – highly lucid, fortunately, as this is a subject that trips up many people. These sections are exhaustive, but they're enough to get you started producing workable programs. And Collingbourne provides plenty of pointers throughout the book for people who want to explore more.

It's clear, though, that the author expects you to be interested in producing serious code, not just hack scripts. There are separate chapters on threading, for enhanced performance, and debugging.

This is not a book geared around Ruby on Rails, the web-oriented implementation of the language which is how most people encounter the language. As Collingbourne points out, many web developers have used Ruby on Rails without ever properly understanding the underlying language. You do get a chapter on the framework, in which you learn how to write the code to run a blog. But if your only real interest in Ruby is to use it in place of PHP or ASP to create dynamic websites, then you need a different book. The Book of Ruby, on the other hand, is a perfect introduction to Ruby as a versatile, all-round programming language.

Security Risk Management

Evan Wheeler.
Published by Syngress
(ISBN: 978-1-59749-615-5).
Price: $49.95, 340pgs, paperback.

Too few organisations, and even IT security professionals, approach information security from a risk perspective. All too often, security is seen as a technical or networking issue. But in this time of tight regulation and highly damaging data breaches, it's essential that all security professionals get to grips with risk issues.

Evan Wheeler, director of information security for Omgeo, teaches this subject at US universities and also wrote the Security Risk Management course for the SANS Institute. He's therefore well-placed to elucidate both the conceptual and practical facets of the subject.

The emphasis is this book is on the latter. It provides enough of a grounding in information security risk concepts that you understand why certain policies and processes are needed and why they are implemented in certain ways. But the main stress is placed on practical techniques that security professionals can use in their day-to-day work.

The book is in three main sections. The first gives an overview of why risk assessments are necessary, how they relate to the business, and introduces the concept of the risk management lifecycle. The second section gives more detail about assessment and analysis techniques, such as risk exposure factors, and risk evaluation and mitigation strategies.

The third section is where everything is brought together. It's effectively a blueprint you can apply to your own organisation to create and run a risk management programme. If you don't have such a programme in place already, Wheeler's guidelines will help you create one from scratch and give you confidence that nothing has been overlooked. If you already have a risk management programme, it will be worth your while matching it against Wheeler's approach to see where the weaknesses might lie and where you can improve efficiency.

Clearly, the primary audience for this book is people who have direct responsibility for assessing and managing risk in an organisation. And they can use this as a manual.

However, even if your job doesn't directly involve managing risk in a formal sense, this book will help you, as an information security professional, understand why what you're doing is important.

Android insecurity

Steve Gold, freelance journalist

Steve Gold

As an operating system, Android is still relatively young. Originally developed by the Open Handset Alliance, an open source initiative piloted by Google, the company, Android Inc, was acquired by Google back in 2005.[1] After a couple of years gestation, the Android 1.0 OS was formally unveiled in November 2007.

Thanks to the continuing support of the Open Handset Alliance – a consortium of more than 80 software, hardware and telecoms companies – Google has released most of the Android code under the Apache Licence, a free software licence. The platform also enjoys the backup of the Android Open Source Project (AOSP) when it comes to the maintenance and further development of the smartphone/tablet computer operating system.

Structurally, Android consists of a kernel based on the original Linux kernel, with middleware, libraries and APIs coded in C running on an application framework that includes Java-compatible libraries based on Apache Harmony. Overlaying this is a Dalvik virtual machine – the broad coding equivalent of Windows 98 sitting on top of a DOS environment – which runs the apps developed by Google's Android operation, as well as a raft of third-party developers.

Most of the mainstream apps are downloaded from Google's official Android Market – analogous to Apple's iTunes portal – but there are a great many third-party markets, including some run by smartphone and tablet computer vendors.

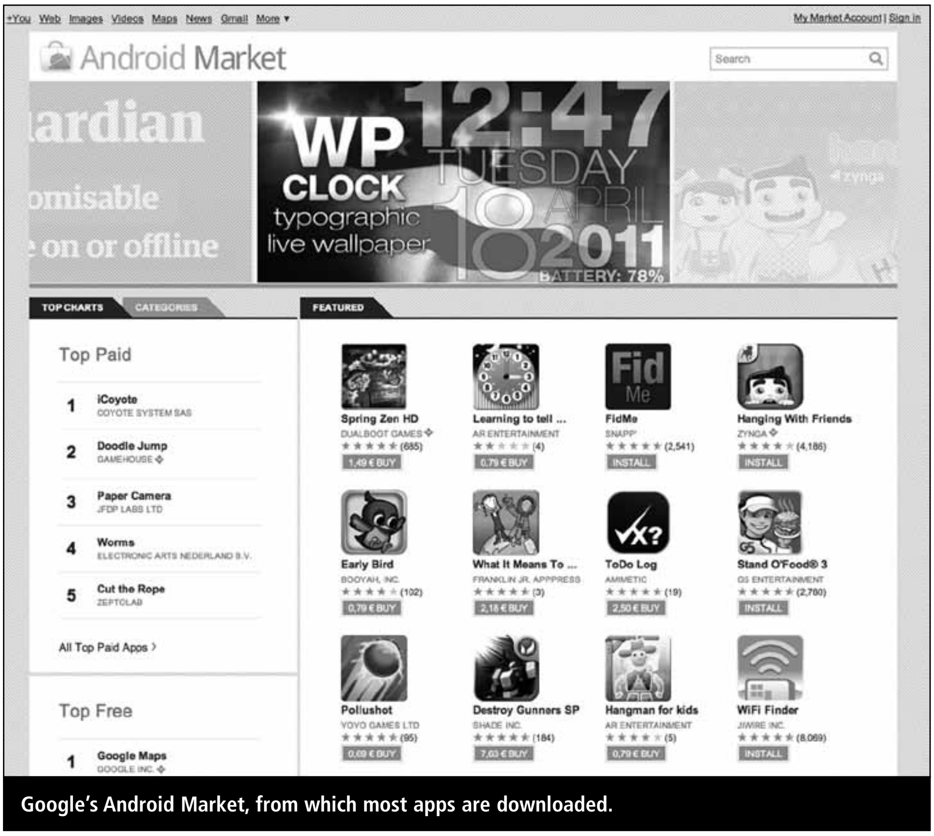
Almost all apps run in a customised version of Java and, although Android's main kernel is derived from the Linux kernel, it is now recognised as a fork or offshoot of the main Linux development stream. From a coding perspective, Android does not have a native X windowing system, nor does it support the full set of standard GNU libraries – limitations that make it difficult to port existing Linux applications or libraries to the smartphone/tablet platform. Data storage is similarly non-standard, as Android uses SQLite, a lightweight relational database, for data storage purposes.

True multi-tasking

Equally atypical is the multi-tasking approach taken by Android. Rather than operate on a threaded basis, the operating system allows multiple applications to run at the same time. It is a true multi-tasking operating system, despite the hardware limitations of many budget and mid-range smartphones and tablet computers seen to date. Just as surprising for a resource-limited environment, Android does not close applications when the user/architecture has 'done' with them. This design specification was mandated by Google to help prevent excessive interactions by smartphone and tablet computer users.

It is also a major security failing, as it possible for an app to be coded to run silently in the background, alongside normal apps in the foreground, and for the user to be none the wiser. In fact, if – as is the case with many of the latest smartphones and tablets – a device never runs out of memory, Android will keep all of these processes running in the background. Even if memory resources are limited, the operating system will look at the process priority of the apps in memory and decide which one to drop. Malware developers have therefore coded their rogue apps to sit in the background, but with a high priority, giving their app the longest possible lifetime in a device power cycle, which can last several days when battery recharging is carried out.

Once Android determines that it needs to remove a process, it does this brutally, simply force-killing the code. The kernel


+You Web Images Videos Maps News Gmail More ▾
My Market Account | Sign in
Android Market
Search
ardian
omisable
on or offline
WP CLOCK typographic live wallpaper
12:47 TUESDAY 18 APRIL 2011 BATTERY: 78%
zynga
TOP CHARTS
CATEGORIES
FEATURED
Top Paid
1 iCoyote COYOTE SYSTEM SAS
2 Doodle Jump GAMEHOUSE
3 Paper Camera JFDP LABS LTD
4 Worms ELECTRONIC ARTS NEDERLAND B.V.
5 Cut the Rope ZEPTOLAB
All Top Paid Apps ›
Top Free
1 Google Maps GOOGLE INC.
Spring Zen HD DUALBOOT GAMES ★★★★★ (685) 1,49 € BUY
Learning to tell ... AR ENTERTAINMENT ★★★★★ (4) 0,79 € BUY
FidMe SNAPP' ★★★★★ (2,541) INSTALL
Hanging With Friends ZYNGA ★★★★★ (4,186) INSTALL
Early Bird BOOYAH, INC. ★★★★★ (102) 0,79 € BUY
What It Means To ... FRANKLIN JR. APPPRESS ★★★★★ (3) 2,18 € BUY
ToDo Log AMMETIC ★★★★★ (19) 2,50 € BUY
Stand O'Food® 3 G5 ENTERTAINMENT ★★★★★ (2,780) INSTALL
Pollushot VOYO GAMES LTD ★★★★★ (95) 0,69 € BUY
Destroy Gunners SP SHADE INC. ★★★★★ (184) 7,63 € BUY
Hangman for kids AR ENTERTAINMENT ★★★★★ (5) 0,79 € BUY
WiFi Finder JIWIRE INC. ★★★★★ (8,069) INSTALL

Google's Android Market, from which most apps are downloaded.

can then immediately reclaim all resources used by the process, without relying on that application being well written and responsive to a polite request to exit. In theory, allowing the kernel to immediately reclaim application resources makes it a lot easier to avoid serious out-of-memory situations, but the bad news is that a rogue app can reboot – perhaps in a less resource-hungry passive state – and sit quietly in the background. Furthermore, because the kernel keeps track of the activities of current and closed apps, a rogue app will normally return to the same state as when it was killed.

Malware ahoy

In August 2010, Kaspersky Lab discovered an SMS trojan – Trojan-SMS. AndroidOS.FakePlayer – that came disguised as a media player that runs in the foreground while also sending out text messages, also in the foreground, but without the users' knowledge or consent. Even when shunted into the background by high-priority apps, the trojan continues to generate text messages, usually to Russian premium rate numbers. It took Android until February 2011 before a patch update to the operating system was issued.

A month later, in March 2011, as widely reported at the time, Google withdrew 58 malicious apps – infected with the DroidDream malware – from the official Market. However, during the 10 days the apps were available, they were installed by an estimated 260,000 Android devices. The large number of installs was due to the apps being free (and cracked) versions of previously paid-for software, which led to a predictable swarm of viral downloads.

DroidDream – a turning point in Android malware – was notable for exploiting a bug in versions of Android older than 2.2.2. Although an update to the operating system that killed DroidDream was rolled out in short order, many users of smartphones do not update their operating system, which means many millions of users remained vulnerable – at the time of writing in September 2011 – to the effects of the malware.

Google responded to criticism by rolling out a forced update to those tracked users that had installed the apps, but the vulnerability remains, so perpetuating the problem for older operating system version users of Android that download fresh versions of the infected apps.[2,3] This perhaps explains why, in August 2011, Lookout Security said it estimated that between half a million to a million Android users were infected by malware in the first half of the year. At the same time, the security research firm said it had seen an increase in the number of infected apps from 80 to 400 in the same period.[4]

Cause for concern?

So, how vulnerable is Android – and if you install suitable security software that verifies downloads as clean and periodically checks your smartphone or tablet computer for malware – should you be concerned?

Pavel Luka, ESET.

According to Pavel Luka, CTO of ESET – the Bratislava-based IT security vendor that released a full, free-of-charge security suite for Android earlier this year – as an operating system, Android is still at the beginning of its development cycle. As such, he says, parallels can be drawn with the development of the early PC operating systems seen in the 1980s and early 1990s – DOS, Windows 3.x and Windows 98 are clear examples – and the early anti-virus software seen around that period. However, the difference today, he argues, is that malware authors are far more experienced and sophisticated in their development capabilities, having cut their teeth on the ubiquitous PC.

"You also have to remember that, right up until the end of the last century, most malware authors were in it for the fun and glory," he says. "Today, however, it's mainly about the money."

"I think that users of Android devices must be educated about the need to install suitable software, and only download their apps from known and reputable sources"

Depending on whom you talk to, he explains, the malware market is worth around $6-7bn dollars a year in criminal revenue terms. "It's also alarming that the rewards for programming malware are so much greater on the darker side of the fence. And since Android is so open to malware infections, there is clearly a lot more risk with using the operating system than with other platforms," he says. "I think that users of Android devices must be educated about the need to install suitable software, and only download their apps from known and reputable sources."

The only piece of good news that Luka has to offer about Android is that tech-savvy people today learn quickly from their mistakes, so if they get hit by malware once, they rarely get hit again.

The analyst view

Over at Bloor Research, Nigel Stanley, the IT analysis firm's practice leader on security, also draws parallels between the early evolution of the PC and the recent – and rapid – evolution of Android. As part of his masters degree in security at Royal Holloway, he says he has completed a major dissertation on the insecurity of the Android smartphone and tablet computer operating system – and he found it wanting. Badly.

Stanley adds that he looked at the platform from the data loss and leakage perspective, kicking off with the smudge test – a test of touch-screen devices

Nigel Stanley, Bloor Research.

to see if, after continued input of the same password or lock pattern, it was easy to reduce the number of digits to 'try' before gaining unauthorised access. Android (or, at least, the devices that were tested) failed.

Then there is the data storage medium – in the case of Android, the microSD card. The operating system failed here too, since it was very easy to remove the card – which is not password locked at the operating system level – and access the contents on an external device. This contrasts, Stanley notes, with the microSD cards seen on Windows Phone 7 devices, where the card is typically soldered onto the system board of the handset for security.

Next up on the test front was the ability to interpret data flowing across the cellular, Bluetooth or wifi connections of the device. It was very easy, says Stanley, who installed a debugging app on the handset and watched ID and password data flowing – in the clear – across the various comms channels.

"While there is no individual packet analysis available, it was a trivial matter to install Wireshark on an external system and watch the operating system generate the GPS data – including the latitude and longitude co-ordinates – transmitted at the operating system level in clear text," he says.

SMS bombing

The next stress test that Stanley tried was SMS bombing, measured by the ability of the device to generate text messages in the background without the user being aware of it. And for the reasons outlined earlier in this feature, Android was a dismal failure in this regard.

"Overall, Stanley says he views Android as a massive failure on the security front, as the hardware – and the operating system – is designed without any intrinsic security in mind"

Stanley says that email was also insecure, as there is no mechanism within Android that he found that allows users – or security software – to look at the headers of messages for signs of spoofing and similar subterfuge. You cannot, he notes, verify the sender of an email for this reason.

Overall, Stanley says he views Android as a massive failure on the security front, as the hardware – and the operating system – is designed without any intrinsic security in mind. Even if the operating system were reworked significantly to counter the security shortcomings, he says the hardware lets things down.

"I can't see a way around the security issues," he says, adding that, for the hundreds of millions of Android users worldwide, the security genie is well and truly out of the bottle.

For those users that have committed to the smartphone and tablet operating system, Stanley says that education on security is essential, although he notes that the cellular carriers are now starting to wake up to the task on their hands and beginning the long process of educating users on the need for on-device security.

About the author

Steve Gold has been a business journalist and technology writer for 26 years. A qualified accountant and former auditor, he has specialised in IT security, business matters, the Internet and communications for most of that time. He is technical editor of Infosecurity *and lectures regularly on criminal psychology and cybercrime.*

References

1. Elgin, Ben. 'Google buys Android for its mobile arsenal'. Bloomberg Businessweek, 17 Aug 2005. Accessed Sep 2011. <http://www.businessweek.com/technology/content/aug2005/tc20050817_0949_tc024.htm>.
2. Kincaid, Jason. 'Google responds to Android malware: will fix infected devices and 'remote kill' malicious apps'. TechCrunch, 5 Mar 2011. Accessed Sep 2011. <http://techcrunch.com/2011/03/05/android-malware-rootkit-google-response/>.
3. Messmer, Ellen. 'Google still scrambling to recover from DroidDream Android attack'. Computerworld, 9 Mar 2011. Accessed Sep 2011. <http://news.idg.no/cw/art.cfm?id=1A027DCB-1A64-6A71-CE9D9C2D6D3115FE>.
4. 'Lookout Mobile Threat Report'. Lookout Mobile Security, Aug 2011. Accessed Sep 2011. <http://bit.ly/putdbX>.

Resources

- Markoff, John. 'I, Robot: The Man Behind the Google Phone'. New York Times, 4 Nov 2007. Accessed Sep 2011. <http://www.nytimes.com/2007/11/04/technology/04google.html>.
- 'Android'. Open Handset Alliance. Accessed Sep 2011. <http://www.openhandsetalliance.com/android_overview.html>.
- 'Android 3.0 Platform Highlights'. Android Developers, May 2010. Accessed Sep 2011. <http://developer.android.com/sdk/android-3.0-highlights.html>.
- Rao, Leena. 'Google: 3 billion Android apps installed; downloads up 50% from last quarter'. TechCrunch, 14 Apr 2011. Accessed Sep 2011. <http://techcrunch.com/2011/04/14/google-3-billion-android-apps-installed-up-50-%-from-last-quarter/>.
- 'Android is a malware cesspool – and users don't care'. InfoSecurity, 15 Jun 2011. Accessed Sep 2011. <http://www.infosecurity-magazine.com/view/18692/android-is-a-malware-cesspool-and-users-dont-care>.

Frametrapping the framebusting defence

Richard J Enbody

Aditya K. Sood

Aditya K Sood and Richard J Enbody, Michigan State University

Iframes are interactive frames that are placed in web pages to show third-party content as a part of the parent website. As a result, the third-party content becomes inline with the parent web page. However, iframes can also be used to conduct web-based attacks. One of the most pernicious types of attack, clickjacking, depends on framing the website in an iframe and then using User Interface (UI) redressing attacks to exploit the trust that users have with legitimate websites.[1]

The basic technique of clickjacking is to add a transparent layer of UI objects, thereby tricking a victim into clicking on a hidden button or link to route the victim to a malware-driven domain. The result is a legitimate page with a malicious overlay. Users think they are clicking on the legitimate page, but are actually clicking on objects created by the malicious code injected by the iframe. Legitimate sites can prevent this abusive use of their pages by inserting code to force their page objects on top – busting out of the frame. In order for legitimate sites to prevent the pages being abused in such clickjacking attacks, there are two ways to 'framebust' the code, as discussed below.

Framebusting code

Framebusting code is the common preventive solution against this type of clickjacking attack. Using this code, a developer attempts to force the legitimate page on top, effectively burying any malicious overlay. This means that the application or website is not allowed to be framed within an iframe. Several variations of the code exist, but the most commonly used framebusting codes are presented in Listing 1.

Basically, framebusting code performs a generic conditional check and executes an action based on it. When this code is applied in a website, it is not possible to frame that website in an iframe. However, there are many variations to this code.[2] The generic Proof of Concept (PoC) has been hosted at the SecNiche website.[3] A generic HTML page has been designed which has the following HTML code as presented in Listing 2. The resulting web page is shown in Figure 1. The HTML page is used as a part of the standard method in which HTML 5 iframe attributes are used to frametrap it.

Listing 1: Framebusting code in action

```
// Code (A)
if(top.location != location) { top.
location.href = document.location.href; }

// Code (B) – more robust
if(top != self) top.location.href =
location.href;
```

Listing 2: HTML Webpage with Framebusting code

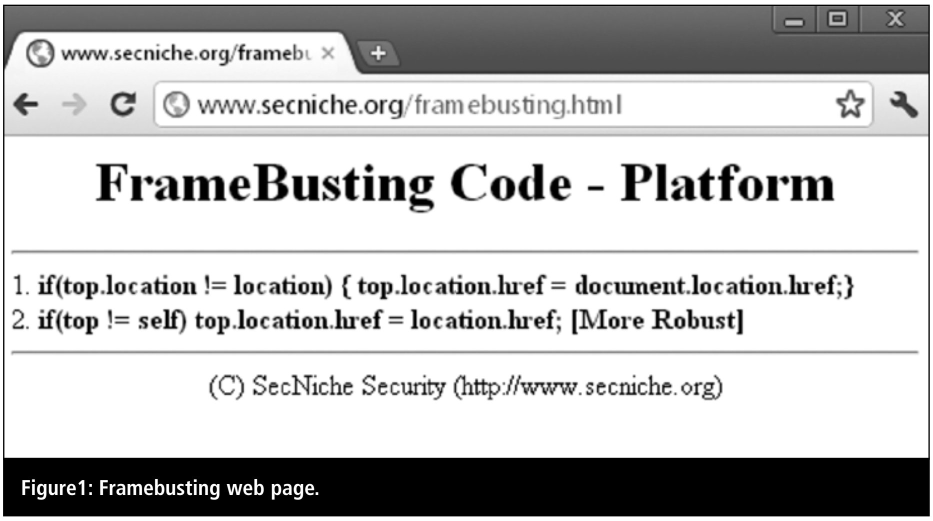
```
<html>
<script type="text/javascript">
if(top.location != location) { top.
location.href = document.location.href;}
if(top != self) top.location.href =
location.href;
</script>
<body>
<center><h1>FrameBusting Code –
Platform</h1></center>
<hr></hr>
1. <b>if(top.location != location) { top.
location.href = document.location.
href;}</b><br>
2. <b>if(top != self) top.location.href =
location.href; [More Robust]</b>
<hr></hr>
<center>(C) SecNiche Security (http://
www.secniche.org)</center>
</body>
</html>
```

Declarative security – X-Frame-Options

Declarative security has been introduced as one of the new browser-based security solutions in order to strengthen client-side security against attacks, including clickjacking attacks.[4] The X-Frame-Options header is one of the major parts of the declarative security mechanism.[5] It is a custom HTTP header that can be used by the applications or websites to send an HTTP response. This mechanism forces the browser (assuming it supports the declarative solution) to framebust the parent website if an attacker tries to iframe it. It is browser dependent, but in reality most of the browsers implement this declarative security solution. In this case, the website throws the X-Frame-Option HTTP response headers as presented in Figure 2.

The X-Frame-Options header uses the two basic values, which are DENY and SAMEORIGIN. If the X-Frame-Option header is used with a value of SAMEORIGIN, the web page can be framed in another web page provided they are using the same origin policy. If DENY is used, the webpage cannot be framed in any scenario. SecNiche Security has designed a Mozilla Add-on that scans HTTP responses from every web page that is opened in Firefox to detect whether a particular website is using the X-Frame-Option HTTP header as a part of a declarative security solution. The tool is currently in the experimental stages. Figure 3 shows the output of the add-on.

However, the most widely used solution is the framebusting code as discussed earlier. This framebusting solution potentially reduces the attack surface as this code can be interpreted successfully by all browsers.



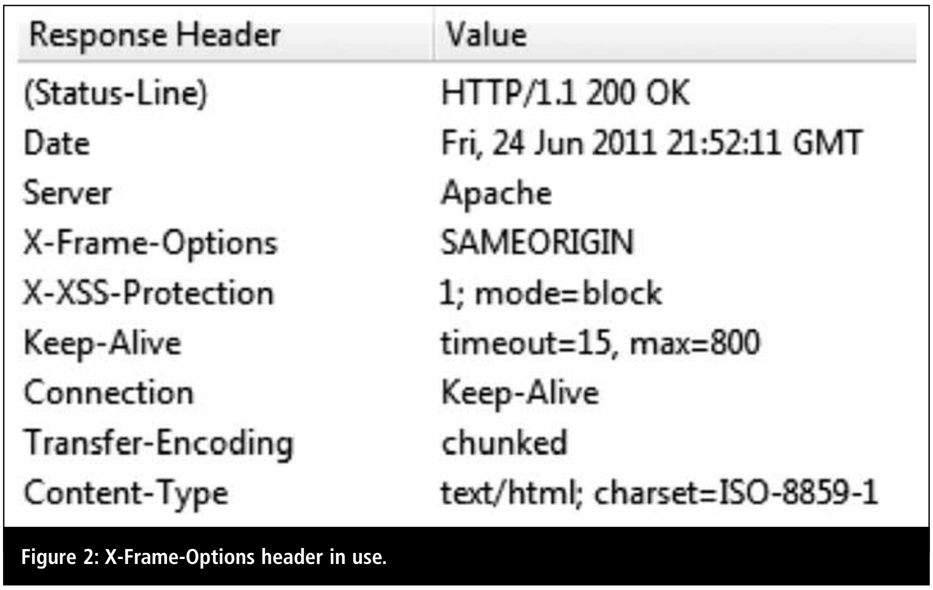
www.secniche.org/framebusting.html

FrameBusting Code - Platform

1. if(top.location != location) { top.location.href = document.location.href;}
2. if(top != self) top.location.href = location.href; [More Robust]

(C) SecNiche Security (http://www.secniche.org)

Figure1: Framebusting web page.



Response Header	Value
(Status-Line)	HTTP/1.1 200 OK
Date	Fri, 24 Jun 2011 21:52:11 GMT
Server	Apache
X-Frame-Options	SAMEORIGIN
X-XSS-Protection	1; mode=block
Keep-Alive	timeout=15, max=800
Connection	Keep-Alive
Transfer-Encoding	chunked
Content-Type	text/html; charset=ISO-8859-1

Figure 2: X-Frame-Options header in use.

Browser design and HTML 5 support

Browsers play a critical role in determining the success of any web attack. There are certain artefacts that should be taken into account in order to understand the web attacks that are browser specific.

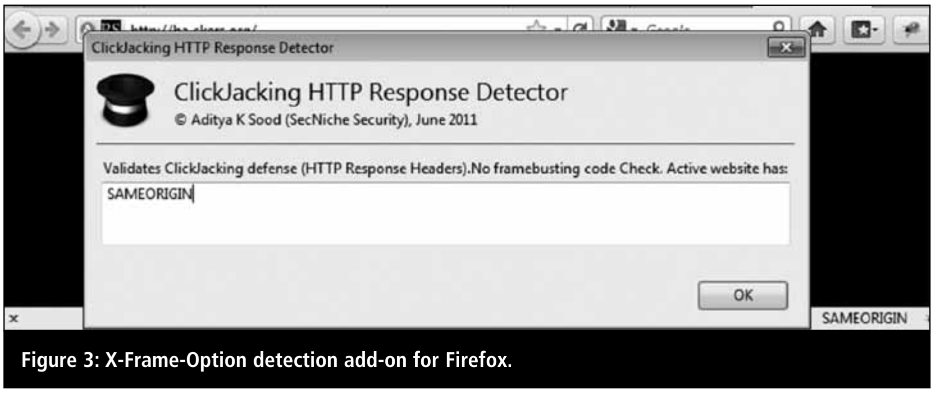
- Different browsers are built on different architectures that have different types of rendering engines. For example, Internet Explorer uses Trident whereas Google Chrome uses WebKit.
- The support for different JavaScript objects and technologies varies widely across browsers. For example, Google Chrome supports HTML 5 advanced tags whereas other browsers such as Internet Explorer and Firefox have not yet completely achieved advanced support for HTML 5. As a result, some HTML 5 attacks can work in Google Chrome but not in the other browsers.
- Design agility varies from browser to browser. Protection mechanisms against client-side attacks depend upon the browser flexibility and extensibility. Thus, the advanced web attacks that can be executed successfully in a specific environment may prove ineffectual in other browsers. For example, Internet Explorer uses the 'restricted' attribute in iframes in order to execute all the content in an iframe in a restricted manner.[6]

The attack that is presented here works only on Google Chrome due to its support for advanced technologies. Google Chrome's support for HTML 5 was tested using the HTML 5 test website, and it was noted that Google Chrome scores maximum points as compared to the other widely used browsers.[7] Figures 4, 5 and 6 show the HTML 5 support provided by Google Chrome, Internet Explorer and Mozilla Firefox respectively.

This rating shows how effectively Google Chrome supports HTML 5. Not surprisingly, Google Chrome is more vulnerable to the HTML 5 attacks than the other browsers. The next section explains the technique of abusing HTML 5 to bypass framebusting mechanisms.

Abusing HTML5 iframe attributes

HTML 5 is the fifth revision of HTML that incorporates more advanced tags



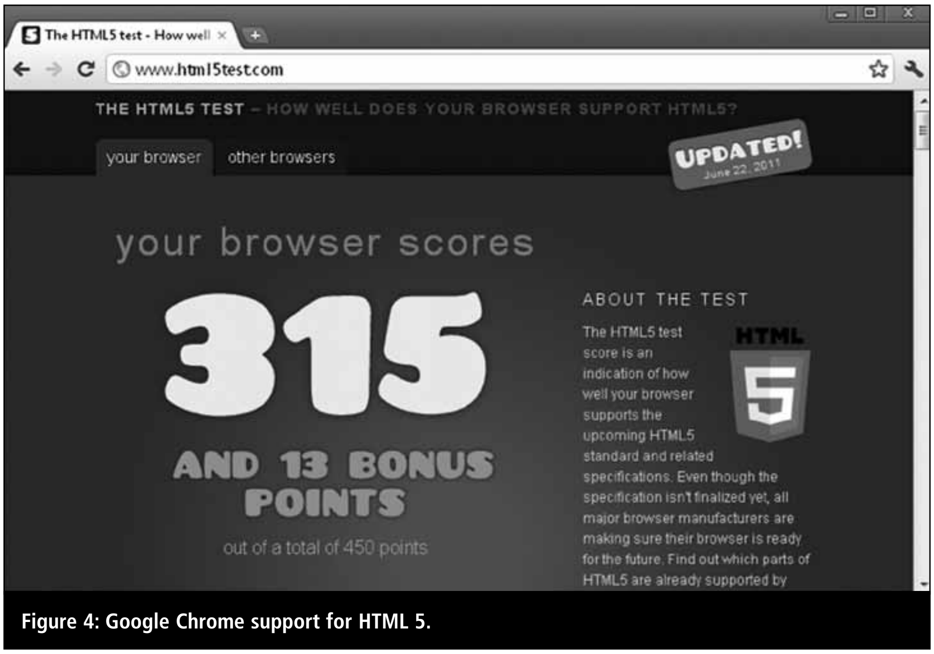
ClickJacking HTTP Response Detector

ClickJacking HTTP Response Detector
© Aditya K Sood (SecNiche Security), June 2011

Validates ClickJacking defense (HTTP Response Headers).No framebusting code Check. Active website has:

SAMEORIGIN

Figure 3: X-Frame-Option detection add-on for Firefox.



The HTML5 test score is an indication of how well your browser supports the upcoming HTML5 standard and related specifications. Even though the specification isn't finalized yet, all major browser manufacturers are making sure their browser is ready for the future. Find out which parts of HTML5 are already supported by

Figure 4: Google Chrome support for HTML 5.

Listing 3: Frametrap code using sandbox attribute in iframe.

```
<html>
<body>
<center><h1>FrameTrapping –
Platform</h1></center>
<b>Dethroning Framebusting
using Sandbox Attribute in HTML
5. You should know how to tap it
appropriately.</b><br />
1. sandbox=“allow-same-origin” <br />
2. sandbox=“allow-scripts” <br />
3. sandbox=“allow-top-navigation”
<br />
4. sandbox=“allow-forms” </br>
<hr></hr>
<center>
<iframe src=“http://www.secniche.
org/framebusting.html” width=“700”
height=“300” sandbox=“allow-
same-origin allow-scripts allow-forms
seamless=‘seamless’”></iframe></
center>
<hr></hr>
<center>(C) SecNiche Security (http://
www.secniche.org)</center>
```

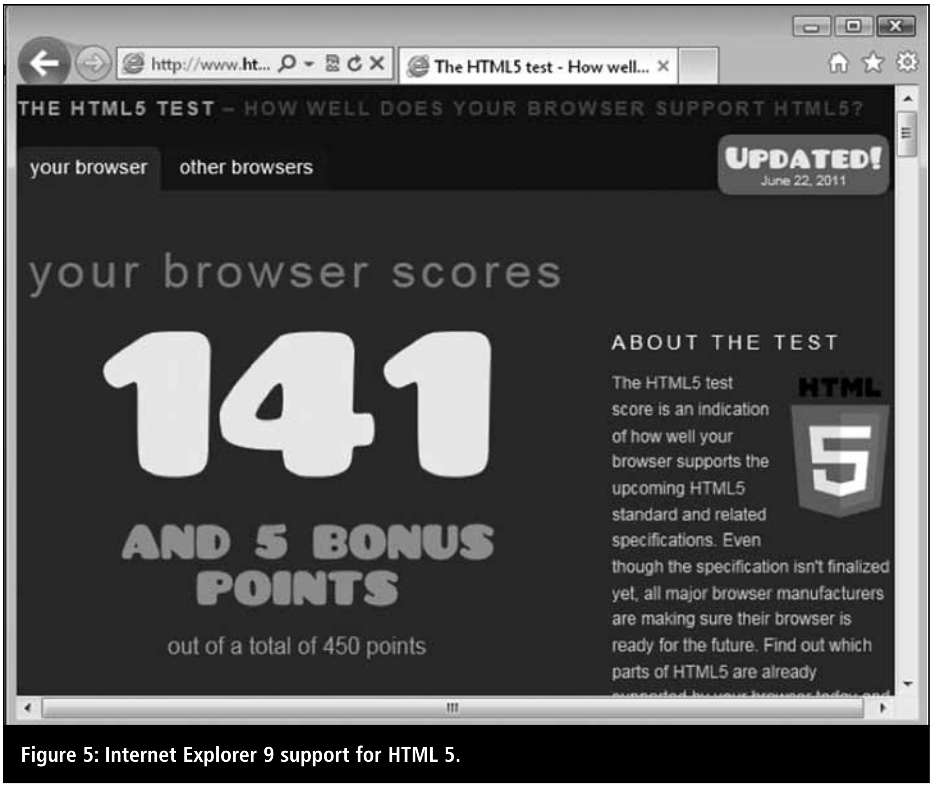
based on the developments taking place in the web technologies.[8] HTML 5 is still in development but some browsers have started rendering the advanced tags. As discussed in the last section, Google Chrome is running way ahead of the other browsers in providing support for HTML 5. At the same time, HTML 5 provides a fresh opportunity for attacks.

HTML 5 supports different uses for iframes by introducing a new set of iframe attributes. HTML 5 has created a ‘sandbox’ that has greatly enhanced and changed the functionality of iframes. It has introduced four new values: allow-same-origin, allow-top-navigation, allow-forms and allow-scripts. The enhanced iframe is one of the major changes that have been incorporated into HTML 5 compared to HTML 4. There are more details about the workings of the HTML 5 iframe at w3schools.com.[9]

This advanced functionality can be used to bypass the framebusting code, as the sandbox attribute allows the framing of a website that has framebusting code enabled. Listing 3 shows the code to bypass framebusting in Google Chrome.

The attacker can frame the web page even after the framebusting code is applied at the website, as presented in Figure 7 which shows the framebusting page displayed in a frame.

In Listing 3, the attacker has not used the attribute value **allow-top-navigation** in the code because this attribute allows the framed page to navigate itself as a parent web page. As a result, this **allow-top-navigation** value effectively allows busting the iframe – something the malicious page developer wants to avoid. On the other hand, an attacker typically uses the other three values to allow script communication and to treat the content in the iframe as being from the same domain as the legitimate web page. This attack using HTML 5 advanced features results in the bypass of the framebusting code. This attack is currently not successful in Internet Explorer and Mozilla Firefox,



The HTML5 test score is an indication of how well your browser supports the upcoming HTML5 standard and related specifications. Even though the specification isn't finalized yet, all major browser manufacturers are making sure their browser is ready for the future. Find out which parts of HTML5 are already

Figure 5: Internet Explorer 9 support for HTML 5.

but might still be helpful in executing successful clickjacking attacks. Since it is a characteristic property of HTML 5, it requires more attention.

> ***"The HTML 5 iframe sandbox attribute can be used to bypass protection mechanisms such as framebusting code, which itself is meant to prevent clickjacking exploits"***

If the website is using a CSS trick to set the display of the malicious objects to nothing (ie, invisible), then the framed web page won't display anything. This is because framebusting is used in collaboration with CSS in order to prevent the loading of a website. However, this solution has not been deployed in very many websites.

Conclusion

We've outlined a new technique based on the HTML 5 iframe sandbox attribute that can be used to bypass protection mechanisms such as framebusting code, which itself is meant to prevent clickjacking exploits. These advanced features in HTML5, which have been introduced to enhance the functionality of browsers by providing a better interface to the users, are vulnerable and can be exploited to execute web attacks successfully.

About the authors

Aditya K Sood is a security researcher, consultant and PhD candidate at Michigan State University. He has worked in the security domain for Armorize, COSEINC, and KPMG and founded SecNiche Security. He has been an active speaker at conferences such as RSA, Toorcon, Hacker Halted, TRISC, EuSecwest, XCON, OWASP AppSec, CERT-IN and has written content for HITB Ezine, ISSA, ISACA, Elsevier, Hakin9 and Usenix Login. He may be reached at adi_ks@secniche.org.

Dr Richard Enbody is an Associate Professor in the Department of Computer Science and Engineering, Michigan State University. He joined the faculty in 1987 after earning his PhD in Computer Science from the University of Minnesota. His research interests are in computer security, computer architecture, web-based distance education and parallel processing. He has two patents pending on hardware buffer overflow protection, which will prevent most computer worms and viruses. He recently coauthored a CS1 Python book, The Practice of Computing using Python. *He may be reached at enbody@cse.msu.edu.*

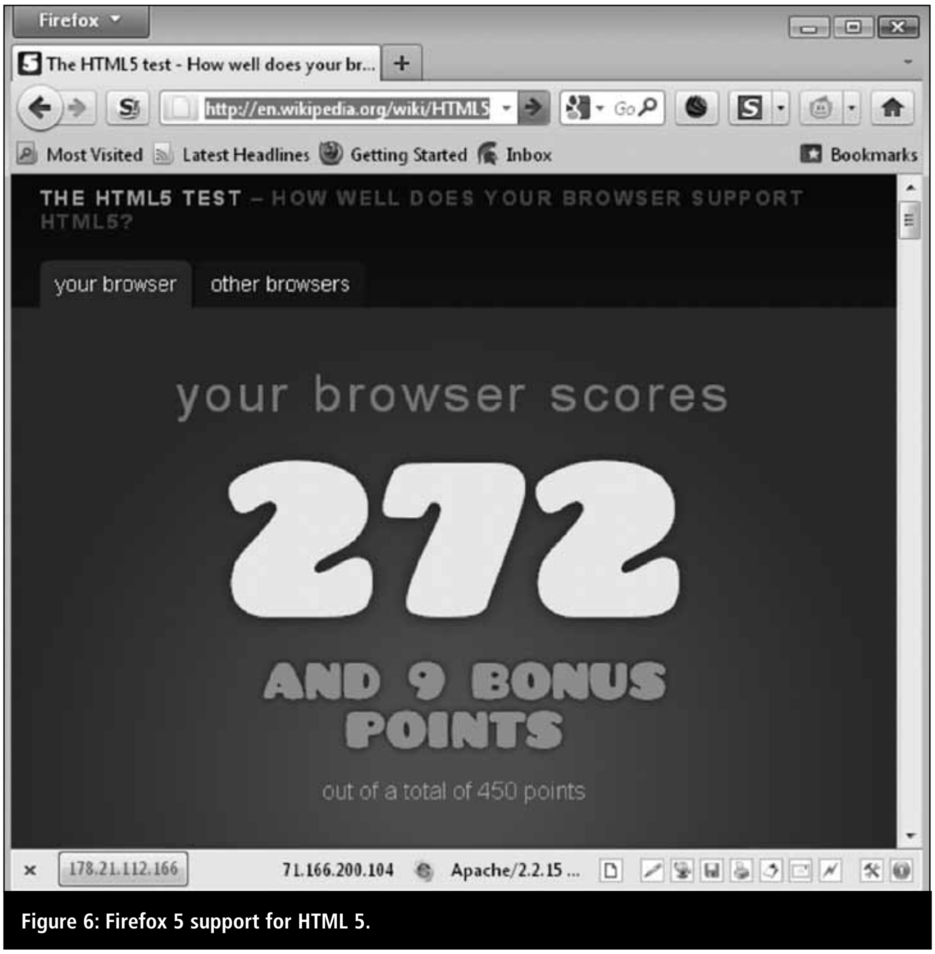
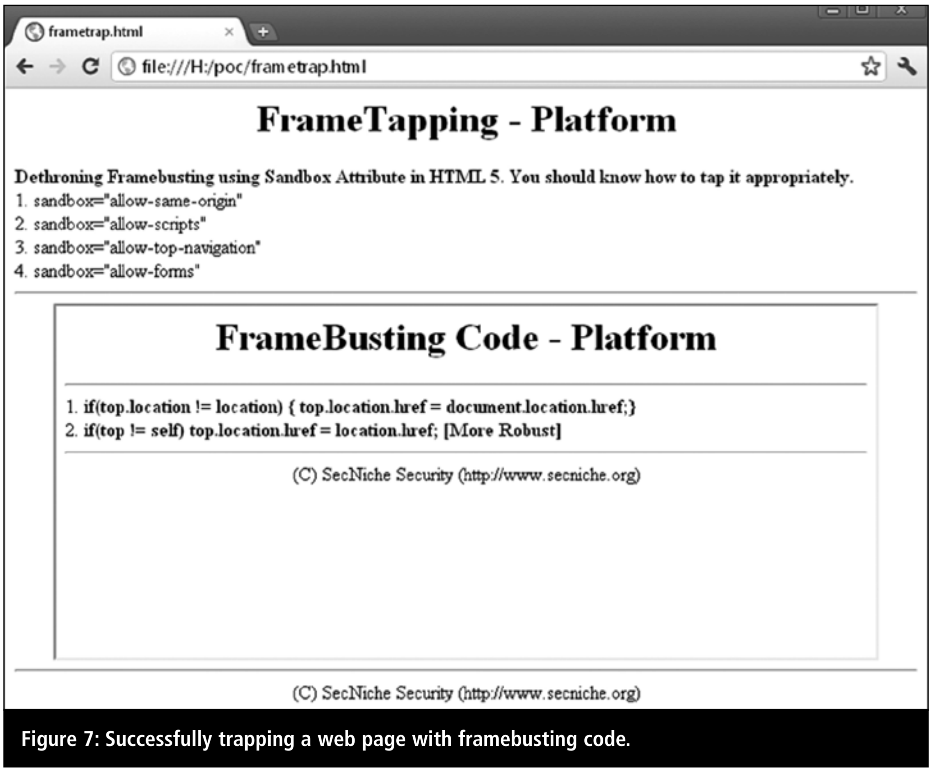


Figure 6: Firefox 5 support for HTML 5.



frametrap.html

file:///H:/poc/frametrap.html

FrameTapping - Platform

Dethroning Framebusting using Sandbox Attribute in HTML 5. You should know how to tap it appropriately.

1. sandbox="allow-same-origin"
2. sandbox="allow-scripts"
3. sandbox="allow-top-navigation"
4. sandbox="allow-forms"

FrameBusting Code - Platform

```
1. if(top.location != location) { top.location.href = document.location.href;}
2. if(top != self) top.location.href = location.href; [More Robust]
```

(C) SecNiche Security (http://www.secniche.org)

(C) SecNiche Security (http://www.secniche.org)

Figure 7: Successfully trapping a web page with framebusting code.

References

1. Hansen, R; Grossman, J. 'ClickJacking'. SecTheory, 9 Dec 2008. Accessed Sep 2011. <http://sectheory.com/clickjacking.htm>.
2. Rydstedt, G; Bursztein, E; Boneh, D; Jackson, C. 'Busting frame busting: a study of clickjacking vulnerabilities at popular sites'. Stanford University, 20 Jul 2010. Accessed Sep 2011. <http://seclab.stanford.edu/websec/framebusting/framebust.pdf>.
3. 'FrameBusting Code – Platform'. SecNiche Security. Accessed Sep 2011. <http://www.secniche.org/framebusting.html>.
4. Sood, A; Enbody, R. 'The Conundrum of Declarative Security HTTP Response Headers: Lessons Learned'. Michigan State University. Accessed Sep 2011. <http://www.usenix.org/event/collsec10/tech/full_papers/Sood.pdf>.
5. 'The X-Frame-Options response header'. Mozilla Developer Network. Accessed Sep 2011. <https://developer.mozilla.org/en/the_x-frame-options_response_header>.
6. 'SECURITY Attribute'. Microsoft Developer Network. Accessed Sep 2011. <http://msdn.microsoft.com/en-us/library/ms534622.aspx>.
7. HTML 5 Test website. Accessed Sep 2011. <http://www.html5test.com/>.
8. 'HTML5'. World Wide Web Consortium. Accessed Sep 2011. <http://dev.w3.org/html5/spec/Overview.html>.
9. 'HTML5 <iframe> sandbox Attribute'. W3schools.com. Accessed Sep 2011. <http://www.w3schools.com/html5/att_Iframe_sandbox.asp>.

Resources

- Sood, A; Enbody, R. 'The state of HTTP declarative security in online banking websites'. Computer Fraud & Security, Jul 2011, pp.11-15.

Defending the network several times over

James Harris

James Harris, ZyXEL Communications UK

Modern networks can be attacked in a variety of ways, meaning that companies need different types of protection to cover all bases when it comes to information security.

Consumerisation, for example, is a problem facing every IT department. Once upon a time, home and corporate computing were entirely separate. During the 1980s, the PC was purely a business tool. Then, during the 1990s, it became the primary machine for home use as well. During the following decade, the Internet took many applications into the cloud. Today, employees use the same computer and browser architectures at home as they do at work. This has blurred the lines between computing at home and in the workplace – and has created some unique security challenges in the process.

A new and more dangerous web

Dazzled by the Web 2.0 sites that permeate their lives at home, employees want the same comforts in the office. Modern websites offer far more than the one-way, passive Internet experience so common in 1995, where users simply read the information on websites.

Instead, today's web offers a bidirectional, many-to-many experience, in which users are encouraged to participate by submitting their own content. Sites ranging from social networks to online photo-sharing services invite users to submit their own information, and even to chat in real time. Facebook, LinkedIn, Wikipedia, Flickr and a panoply of other sites fall into this category.

These technologies have brought Small to Medium-sized Businesses (SMBs) the same benefits as their larger counterparts. Online applications, advanced search capabilities, and real-time messaging technologies enable SMBs to build scalable, highly-responsive technology infrastructures to support their businesses. Virtual teams of contractors can now be assembled easily with a collection of free instant messenger clients and a cheap account on a collaborative website, for example.

However, these benefits come at a cost. Many web 2.0 sites have repeatedly been found wanting in terms of security. More functionality breeds more vulnerability, and attackers have been quick to exploit weaknesses. Malicious software (malware) that infects computers and connections spreads via a variety of channels, including hacked websites, email, social networks, and instant messenger programs. Even simple search results are being 'poisoned' by search engine optimisation experts who want to direct unwitting users to malicious web pages instead of legitimate ones.

> ***"Even simple search results are being 'poisoned' by search engine optimisation experts who want to direct unwitting users to malicious web pages instead of legitimate ones"***

The dangers extend to the unintended egress of information. Employees may inadvertently send sensitive data outside the company via several channels. Pasting customer information into an email is one example, although it can also be pasted into Web 2.0 sites, or sent via instant messaging programs.

An example of the danger: real-time chat

The encroachment of real-time chat into corporate networks began as long ago as 1996-7, when Mirabilis launched the ICQ chat service, and AOL launched its Instant Messenger program. The software began creeping onto corporate desktops without the IT department's permission and knowledge.

"The irony underlying most instant messaging programs is that although they are legitimate, they act like malicious software. They are designed to get around network firewalls that might try to block them"

That is the problem with the corporate desktop – it is very difficult to manage effectively. For SMBs especially, which often have a lot of IT expertise within the business, trying to lock down desktops is a challenging task. Even those organisations with the wherewithal to do it risk irritating employees who want those comforts on the desktop. With instant messaging becoming an important work tool, it could even be deemed counter-productive for companies to ban it from the desktop altogether. AOL Instant Messenger, MSN Messenger and Skype are all useful for business purposes, as are other programs such as Google Talk.

The irony underlying most instant messaging programs is that although they are legitimate, they act like malicious software. They are designed to get around network firewalls that might try to block them, by 'port hopping' – effectively trying different digital 'doors' separating a company's network from the public Internet, until they find one that is unlocked.

The problem of real-time chat as a potential attack vector has been exacerbated with the introduction of web-based online chat mechanisms that need no desktop client at all. Facebook's built-in instant messaging feature is a good example of this.

Defence in depth

SMBs with little resource to spare for complex IT security therefore find themselves battling not only real, external threats, but also their own well-meaning employees. They need simple, turnkey solutions to secure their networks, but as we've seen, the threats operate at multiple levels. For this reason, security products for SMBs should provide multi-layered protection (otherwise known as 'defence in depth') to protect all of the available channels.

Defence in depth goes beyond the traditional firewall, which has historically been the main method used to protect the corporate network. These devices did little more than block specific ports on a network to stop external attackers from using them to attack a company's computers. They did nothing to analyse the actual content of the traffic passing over the company's network connections.

Unified Threat Management (UTM) appliances monitor the network for a variety of threats by combining smart firewall technology with email and web content scanning. They can be programmed with rules that stop employees from doing specific things on the Internet at particular times, and can look for suspicious traffic flowing over the network.

Protecting the network

Network security features heavily in UTM systems, which build on traditional firewall systems with a host of new features. Modern UTMs feature stateful packet inspection, which not only monitors specific ports, but also watches what traffic passes through them over time.

This ability to watch the traffic passing across the network also allows modern network security products to offer Intrusion Detection and Prevention (IDP) capabilities. The security device monitors network traffic activity to look for patterns that could indicate an attack. An example of a malicious pattern might be a single PC in the organisation that suddenly begins rapidly contacting other PCs using a single port, which could indicate a rapidly spreading piece of malware. The IDP database is constantly updated with new patterns identified by the vendor of the device as new vulnerabilities and attacks appear.

"An example of a malicious pattern might be a single PC in the organisation that suddenly begins rapidly contacting other PCs using a single port, which could indicate a rapidly spreading piece of malware"

Modern network security devices also feature application firewall capabilities. These use a technique known as deep packet inspection to look inside the data that flows over an Internet connection. By examining the content of these packets, a device can determine the type of traffic that they represent. They may be video, Voice over IP (VoIP) or web traffic directed at a particular application on the company's network. By analysing the packets, the device can determine whether they are performing legitimate tasks.

Higher-level protection

Multi-layered devices also monitor the content of those packets for warning signs, enabling them to scan incoming and outgoing emails for suspicious content. This enables an organisation to stop spam messages from reaching recipients, using a mixture of spam signatures updated by the vendor and intelligent heuristic techniques that allow the device to estimate the likelihood of a particular email being 'spammy'.

Finally, web security works to protect users both at a content prevention and a URL filtering level. It watches the URLs that users attempt to visit, and can block known malicious sites (such as phishing destinations, or 'drive-by download' sites) before the user's browser has a chance to download malicious or inappropriate content. URL filtering has the added benefit of enabling a company to implement policies controlling social network use. Perhaps managers only want users visiting Facebook pages during their lunch hour, for example. Web security mechanisms will also scan content, watching for content such as pornography, and for malicious code contained on a web page that might compromise a user's computer.

"Condensing multi-layered protection into a single device, updated by the vendor, provides the best protection for resource-constrained companies"

Covering all your bases

It is easy to see how these functions work in unison with each other. For example, attackers often use email to send malicious URLs to users. These may be spotted by email protection functions within a unified threat management system or Internet security appliance. However, if they slip through, they will be caught by the web filtering mechanism, making it doubly hard for attackers to compromise users. Anti-virus mechanisms built into the device will also scan for malware separately, providing yet another level of protection.

Defence in depth is a crucial technique for any modern SMB that wants to protect itself against intrusion. Condensing multi-layered protection into a single device, updated by the vendor, provides the best protection for resource-constrained companies.

Modern Internet security is an exercise in probability. It is impossible to guarantee 100% security – a determined hacker may still be able to gain access to a company's system. But the more points protection that a company covers, the more likely it is to fend off the majority of generic attacks on the Internet. Can you afford not to cover your bases?

About the author

James Harris is a product manager at network equipment manufacturer ZyXEL Communications UK. Working in the industry for the past 10 years he has held various technical and product management positions specialising in wireless, Ethernet and routing technologies.

Mitigating denial of service attacks in hierarchical wireless sensor networks

Rohan Nanda

P. Venkata Krishna

Rohan Nanda and P Venkata Krishna, School of Computing Science and Engineering, Vellore Institute of Technology, India

Due to the considerable research and development invested in new networking protocols, Wireless Sensor Networks (WSNs) have proved to be an important emerging field. WSNs are widely used in homeland security and military applications, in hospitals for medical monitoring, and in industry. However, their limited battery and power options, processing capability and memory make WSNs vulnerable to a variety of network attacks.

The use of the wireless medium is the major weakness, allowing any adversary to attack the network or compromise the nodes. The security of WSNs is an important factor because confidential data communicated between the sensor nodes needs to be protected from untrusted third parties who can misuse or modify this data by malicious means.

The aim here is to develop a key management scheme to protect the server in a hierarchical sensor network from a Denial of Service (DoS) attack. A DoS attack would make a server in a hierarchical WSN unavailable to its intended nodes or clients. The server gets saturated with external requests so that it cannot respond to legitimate requests from other nodes. Even if the server responds, the response is so slow that it is rendered effectively unavailable. DoS attacks attempt to consume the resources of the target server so that they are depleted to the point where a reset is forced. The server has the capability to handle only a fixed number of requests at a time. When the number of requests exceeds this maximum number then the time taken by server to respond to each request increases significantly. As the frequency of attack increases, the server becomes completely unavailable to service any kind of request. Thus the requests of legitimate users are denied.

The key management scheme for hierarchical WSNs, outlined here, also uses a hierarchical structure from server (base station) to cluster heads and finally to sensor nodes. Organisation across the network uses cluster formations and the establishment of a derivative key between all three hierarchical layers. Then keys are established for secure communication between sensors belonging to the same cluster head. Finally, we'll define key management processes used to identify a DoS attack and defend the server.

Related work

There are many publications and proposals that suggest different ways of handling DoS attacks using a key management protocol. Public key cryptographic techniques prevent DoS attacks that exploit draining the battery through WSN ephemeral key establishment.[1] They combine a DoS mitigation scheme with self-certified, ECC-based key generation to yield a resource-efficient security framework. The cluster adaptive rate-limiting scheme for preventing denial of sleep attack introduces cluster adaptive rate-limiting, which is based on current host-based intrusion detection techniques.[2] This technique might be used to reduce energy consumption to an arbitrarily low level until a denial of sleep attack is lifted. Another scheme provides a framework to discover the number of malicious packets among a massive flood of packets by using a probabilistic approach.[3] This approach achieves a better overhead than the HCF computation method.

"This method forces multiple hashing calculations and numerical factors in order to falsify the first intercepted data packet and win time in broadcasting trusted message packets"

Another scheme proposes a multi-user DoS containment and signature-based broadcast authentication scheme.[4] The authors also discuss Routing and Remote Access Service (RRAS), a lightweight scheme to effectively contain a DoS attack. In one scheme, the authors propose a new broadcast key management scheme for distributed WSN, which prevents a potential DoS attack where a packet has been intercepted.[5] This method forces multiple hashing calculations and numerical factors in order to falsify the first intercepted data packet and win time in broadcasting trusted message packets to cover the whole network. Another new scheme discusses a remote access framework incorporating a virtual home and a Distributed Denial of Service (DDoS) defence server, which increases the difficulty of launching a low-level DDoS attack against a WSN.[6] The authors propose a DoS defence approach consisting of three entities: Virtual Home; Remote Home Server; and DDoS Defence Server. Out of all these schemes, very few have used key management techniques to mitigate DoS attacks. However, key management is an integral part of a WSN even if it is not originally used for the purpose of mitigating a DoS attack.

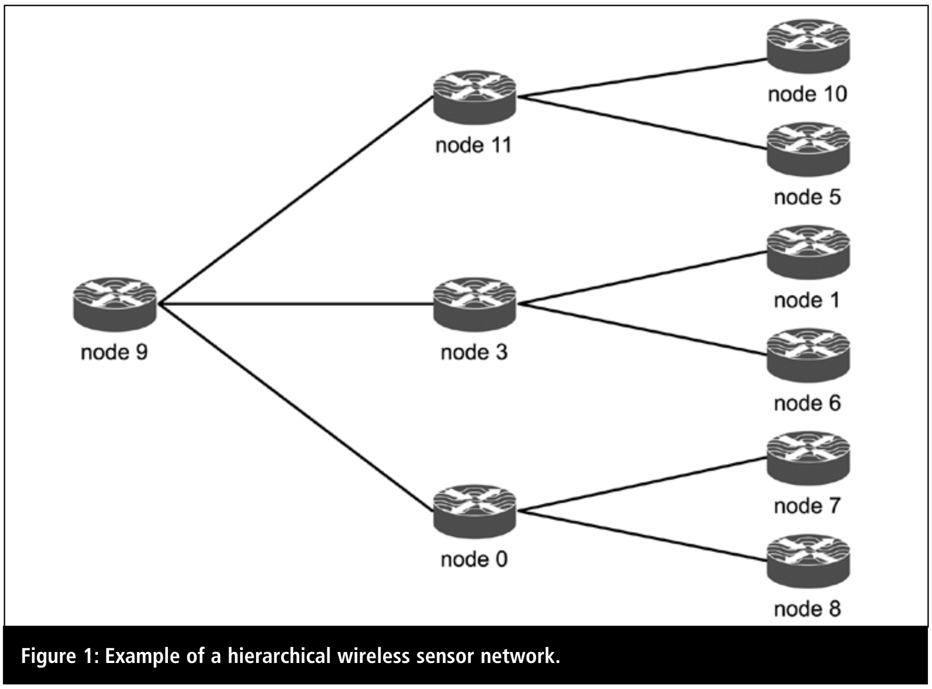


Figure 1: Example of a hierarchical wireless sensor network.

The proposed model

The main aim of the work detailed here is to develop a new key management scheme using the concept of timestamp and delay that combats a DoS attack on WSNs. We consider the same structure of a hierarchical WSN as discussed in a previous paper on a self-enforcing and secure protocol.[7] The server operates in place of the base station as the topmost root node of the hierarchy. The second hierarchy level contains the cluster heads that are responsible for co-ordination and management of nodes present under that particular cluster head. Each cluster head groups some sensor nodes under it, and these are used for various purposes depending on the application in use. The complete hierarchy is illustrated by Figure 1 where a server has three cluster heads and each cluster head controls two sensor nodes. The cluster heads can communicate with each other and with also with the server. In addition, they can communicate data to other cluster heads and the server. Similarly, the sensor nodes can communicate with other sensors of the same cluster and with the cluster head.

In our scheme each node, including the server (base station), has a unique ID and an inbuilt key (K). Before the deployment phase, each sensor node has been provided with a pseudo-random function (f) so that the sensor nodes are resilient towards outsider attacks.[8] Therefore each sensor node computes its own new key by using the previous key (K_s) and its unique ID.

$$K = f (K_s, ID)$$

Now all the nodes, including the server, cluster heads and sensors, have computed their keys. This key is called the original key.

Network organisation using derivative key

The base station or server identifies the cluster heads deployed under it. To choose each cluster head, the server makes use of the original key with the ID of a particular cluster head to establish communication. This is done by the derivative key calculation K' as follows:

$$K' = H (K \| ID_i)$$

Here, K is the original key, ID_i is the ID of the cluster head and H is the hash function which is computationally unfeasible to revert. All the cluster heads can be chosen using the derivative key.

Subsequently, the server organises the network by sending a list of sensor nodes deployed to each cluster head in a message encrypted by derivative key K' as follows, as described by Hu Bai and Yang.[10]

$E_{K'}$ (M || ID_{list})

Here, ID_{list} contains the IDs of all the sensors that are deployed under that particular cluster head and M is the message for sensor nodes. After receiving this message the cluster heads decrypt it using the same derivative key K' to extract the information of the list of sensors. Now the cluster heads establish the same derivative key with the sensor nodes by assigning each of them a particular ID.

K' = H (K || ID_{ij})

Here ID_{ij} is the ID of a particular sensor node. After this step, each cluster node includes all the sensor nodes under it. Now the sensor nodes can even transmit data or messages directly to the server by using key K'. The sensor nodes can send a message to the server informing it of its ID. The message is encrypted using the derivative key K'.

$E_{K'}$ (M || ID_{ij})

The encrypted message is received by the server and it decrypts it using K' to retrieve the necessary information. Now, finally, the network is organised and all the nodes are using the same key K' for communication.

Cluster key usage

After the hierarchical WSN is organised, there needs to be a secure communication between the sensor nodes and cluster heads and also between sensor nodes belonging to the same cluster head. Suppose the sensor node Sij wants to transmit data with Si(j+1) – again, Sij encrypts the message with key K' and sends it to Si(j+1), as in Hu et al, but with the technique described here the message uses a different key and method.

EK' (M, IDij)

Si(j+1) decrypts the message using the same key K' to obtain the necessary information present in message M.

Authentication check at each hierarchical level

To secure both the server and the whole network, it is essential to check the authenticity at each hierarchical level. If there is a malicious node present among the sensors, and the server or cluster head establishes a key with it, then the adversary can easily launch attacks on the network, and it would be very difficult to combat that attack. Therefore we propose a sensor node authentication model for the given scheme.[8]

When a cluster head has to authenticate the sensors under its hierarchy it then it computes a value called B_{pq}, where p is the cluster head and q is the sensor node to be authenticated.

B_{pq} = H (ID_p || T)

Here, T is the current timestamp of sensor p and ID_p is the unique ID of sensor p. The cluster head p sends a message AUT=<B_{pq}, T> to sensor node q. After receiving the message AUT, the sensor node q validates the timestamp if (T'-T) ≤ ΔT where T' is the current timestamp of sensor node q and ΔT is the expected time interval of the transmission delay. If this condition is not true then authentication fails and cluster head p gets to know that q is a malicious sensor node and terminates the communication with sensor q. If the condition is true then sensor node q computes:

B_{qp} = H (ID_p || T)

Here, T is the current timestamp of sensor q. Now sensor q compares the value of B_{qp} with the received value of B_{pq}. If B_{pq} = B_{qp} holds true then cluster head p knows that sensor q has been authenticated successfully and now it is safe to establish a key with sensor q. In the same manner, the server also authenticates the cluster heads before the key is shared.

Mitigating a DoS attack

DoS is a highly dangerous attack that cripples the server by flooding the network with excess service requests to the server. A server can only service the request of a client if it can allocate resources to that client. A DoS attack depletes the resources of the server so that it cannot allocate the necessary resources. The server can handle a fixed amount of service requests over a given period. If the number of requests exceeds this value then the server is under DoS attack and is not able to process the requests of legitimate users or clients.

Suppose the server's capacity to process requests has been exceeded or is on the verge of crossing the maximum number of requests per unit of time.[9] At this stage, the server encrypts a message using the key K' which contains the IP address of the server, and it broadcasts this message over the entire network but only to the cluster heads.

$E_{K'}$ (IPADDR || ID_i)

Here, IPADDR refers to the IP address of the server and ID_i is the unique ID of each cluster node. The cluster node decrypts the message to obtain the IP address of the server. The cluster head now needs to identify the attacker who induced the DoS attack on the network. All the requests to the server from the sensor nodes are passed through the cluster heads. Now the cluster heads again encrypt a message with the key K' with a timestamp value and broadcast it to all their sensor nodes with a message:

$E_{K'}$ (IPADDR || M || T)

Here the message M contains the instruction for execution by the sensor nodes upon receiving the message. After receiving the message, the sensor nodes decrypt the message using the key K' to obtain the contents of the message. The message M contains an urgent delay function that commands the sensor nodes to delay their request to the received IP address by the value of the timestamp specified in the encrypted message. Upon receiving this message, all the sensor nodes that are currently requesting the service of the server will delay their service requests by the time specified in the timestamp. The value of the timestamp is computed by the cluster heads on the basis of the acuteness of the DoS attack. So all the sensor nodes that are not requesting service from the server will continue to process their service requests. Since each request will now be delayed by a timestamp T, the server recovers its depleted resources and the effect of the attack is nullified. However, if after receiving the message a node is still not slowing down the number of requests to the server then it means that this node has initiated the DoS attack. Now the corresponding cluster head traces the IP address of this node, encrypts it and broadcasts it over the network with the message BLOCK, which indicates to every other node to discard the packets coming from this IP address, IPATTACK.

$E_{K'}$ = (IPATTACK || BLOCK)

Suppose the attacker node also delays service requests when the delay timestamp packet is issued, and that after that time period is over, it again starts fetching a number of requests. In this case, the server should issue this delay timestamp packet periodically so that the attacker is compelled to reveal its identity. In another scenario, the server can block the requests from a particular cluster head by simply discarding the requests from that cluster so as to identify the cluster in which the attacker is actually present. After identifying the cluster head, the legitimate users from other clusters won't be denied service requests, while the cluster head containing the attacker can use the delay timestamp packet to identify the attacker. Hence this scheme mitigates the DoS attack in all cases and makes the server available for user requests.

Key features of the proposed model

The main idea of this scheme is to ensure the security of hierarchical WSNs in almost all scenarios by providing a secure and self-enforcing scheme implemented on the sensor nodes in a hierarchical fashion. The following outlines the key features of the scheme in an algorithmic manner:

1. The scheme uses a pseudo-random function that enhances the network security before the nodes are even deployed by the sensors.
2. A derivative key is established by the server with the cluster heads and the cluster heads in turn establish derivative keys with sensor nodes.
3 The network is organised such that the whole network uses the same derivative key.
4. Sensor nodes belonging to the same cluster establish communication through derivative keys.
5. The cluster heads authenticate the sensor nodes and similarly the server authenticates the cluster heads.
6. In case of a DoS attack, the scheme combats the attack and makes the server available for legitimate users.

Analysis of the proposed model

For evaluating the performance and efficiency of the scheme, there are some important factors, such as security and overhead.

Overhead: the computational overhead is mainly imposed by the derivative key calculation, authentication check at each hierarchical level and the emergency message broadcast when the DoS attack occurs. Due to the high efficiency of the pseudo-random function, the computational overhead before deployment is negligible. The time complexity of the hashing functions is estimated to be O(1), due to which the overhead of the entire scheme is highly reduced. In total, we have used four hash function computations, two of which are used in derivative key calculation and the other two in authentication checks at each hierarchical level. Although authentication at each hierarchical level incurs some computational overhead, because of the verification of the nodes, it is an indispensable part of the scheme that enhances the overall security. In case of a DoS attack, the main aim is to keep the server working so that its resources are not compromised, so it is essential to broadcast the delay timestamp packet, which also incurs a computational time overhead.

Security: from the start of the scheme, where the pseudo-random function keeps on generating fresh keys until the authentication check, the scheme provides resilience towards network security attacks and maintains data integrity and privacy within the network. The derivative key, established after the random function, is symmetrically organised throughout the network, which makes it very difficult for an adversary to find a weak point in the network. The authentication check at each hierarchical level further shields the scheme by verifying the identity of the sensor nodes with which the key is going to be established. The steps taken during a DoS attack, such as delaying the service requests of clients and discarding the packets of the attacker, play an integral role in successfully defending the server against the adversary. Due to authentication checks and the derivative key, node compromise also doesn't yield any secure information about the keys of other nodes. Even in the case when the attacker is not identified, application of the alternative strategy defeats the DoS attack on the server.

Conclusion

We have proposed a key management scheme for hierarchical wireless sensor networks that not only defends the network against DoS attacks but also maintains confidentiality, integrity and authenticity of data transmitted between sensor nodes. It uses a derivative key that is derived symmetrically between the hierarchy of sensor nodes. This key enables the successful data communication between sensors, cluster heads and server. It also authenticates the sensor nodes with cluster heads and cluster heads with the server by using the timestamp method. Moreover, the timestamp delay packet plays a key role in mitigating a DoS attack. This scheme also provides a lot of scope for future development.

About the authors

Rohan Nanda is a B.Tech CSE student of the Vellore Institute of Technology (VIT), Tamil Nadu, India. He is carrying out his research under Dr P Venkata Krishna. His research interests include wireless sensor networks security, key management and DoS attacks. He has published two papers on sensor networks security in IEEE International conferences.

Dr P Venkata Krishna is professor and division leader of computer networks at VIT. He has authored more than 80 research papers in various national and international journals and conferences. He is a reviewer of journals such as IEEE Trans on Mobile Computing, IET Journal on Communications *and the* International Journal of Security and Networks. *He is the editor for the* International Journal of Systems, Cybernetics and Informatics.

References

1. Arazi, O; Qi, H; Rose, D. 'A public key cryptography method for denial

of service mitigation in wireless sensor networks.' In Sensor, Mesh and Ad Hoc Communications and Networks, June 2007. SECON 07, San Diego, CA, pp.51-59.

2. Midkiff, S; Raymond, D; 'Clustered adaptive rate limiting: defeating denial of sleep attacks in wireless sensor networks'. In Military Communications Conference, October 2007. MILCOM 2007. IEEE, Orlando, FL, US, pp.1.
3. Swain B; Sahoo, BR. 'Mitigating DDoS attack and saving computational time using a probabilistic approach and hcf method'. In Advance Computing Conference, March 2009. IACC 2009. IEEE International, Patiala, pp.1170.
4. Gan X; Li, Q. 'A multi-user DoS containment broadcast authentication scheme for wireless sensor networks'. In Information Technology and Computer Science, July 2009. ITCS 2009. International Conference, Kiev, pp.472.
5. Zeng, Y; Xia, Y; Su, J; Zhao, B; Yu, W. 'A new broadcast key management scheme for distributed wireless sensor networks'. In Mobile Adhoc and Sensor Systems, Oct 2009. MASS '09. IEEE 6th International Conference, Macau, pp.882.
6. Gill, K; Yang, S. 'A scheme for preventing denial of service attack on wireless sensor networks'. In Industrial Electronics, Nov 2009. IECON '09, 35th Annual Conference of IEEE, Porto, pp.2603.
7. Nanda, R; Krishna, P Venkata. 'A Self Enforcing and Flexible Security Protocol for Preventing Denial of Service Attacks in Wireless Sensor Networks'. In press. Recent Advances in Intelligent Computational Systems, 2011.
8. Nanda, R; Tiwari, S; Krishna, P Venkata. 'Secure and efficient key management scheme for wireless sensor networks'. In Network and Computer Science (ICNCS), 2011, Kanyakumari.
9. Misra, S; Krishna, P Venkata; Kiran, Isaac Abraham; Sasikumar, Navin; Fredun, S. 'An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks'. In Computers & Mathematics with Applications, Volume 60, Issue 2, pp.294-306, July 2010.
10. Hu, J; Bai, E; Yang, Y. 'A novel key management scheme for hierarchical wireless sensor networks'. In Communication Technology (ICCT), 2010 12th IEEE International Conference, Nanjing,

Cloud computing: new challenges and opportunities

Richard Morrell

Akash Chandrashekar

Richard Morrell and Akash Chandrashekar, Red Hat

We are witnessing a shift in the cloud computing and virtualisation landscapes as a new model of security arises in response to the demand for clarity into how to harness the consumption of elastic computing resources. If we look back at traditional server-based and hosting provision for security, it was very much belts and strong vendor-supported braces that allowed customers to have a perimeter-based security that enclosed their assets and provided assurance. How is this changing as a result of the move to a cloud-based model? Is the emphasis on assurance and privacy, especially in a multi-tenant environment in an outsourced location, changing the way we are approaching security?

Cultural change

Many organisations have already embraced virtual hosting and have used datacentres under contract for a decade or more to provide simple web-based hosting or clustered web application hosting. Does moving these into the cloud enforce a change in culture? What are the pressures to regulate the industry in the post-WikiLeaks and LulzSec hacking scandal world?

One of the most interesting aspects of the movement of Service Oriented Architecture (SOA) application development and hosting from corporate and on-premise firewalls to outsourced cloud providers is its effect on the way the audit model works and the way it can be assessed as part of an overall corporate governance model. The use of SAS 70 (II) certification as a standard across cloud deployments is a start but not sufficient on its own to provide assurance of a cloud provider's ability to provide security controls that reflect customers' needs. SAS 70 (II) is not and cannot be taken as applicable to the needs of enterprise customers using cloud computing as it is more of an accounting standard than a standard related to virtualised elastic computing environments. The reality is that customers would benefit from a more transparent and practical regulatory framework, one that takes into account governance, risk and control.

The importance of governance

As we move to outsourced cloud environments, a practical and sensible approach to understanding governance, risk and controls in SOA environments is of paramount importance. It is essential to negotiate the balance of risk between customers and providers, or data controllers and data processors, and ensure that services are aligned in order to secure operations and ease of audit.

Security must be engineered into the cloud solution itself. Providers of cloud stacks or application stacks should be working ahead of customers to implement business rules to meet their governance requirements. Having security as one of the core factors in developing a cloud solution should be a primary influencing and decision-making step that will reduce the risks associated with cloud adoption. Security and governance should not be a retrofitted control, or a paper-based exercise at the point of audit: audit should be built into the cloud design and a 365/24/7 activity, keeping in mind governance, risk and control as primary components.

Architects as well as decisionmakers need to take into consideration all three aforementioned components:

1. Governance – ie, understanding what your requirements are at present and will be in the future and the model you need to employ to meet specific IT requirements.
2. Risk – understanding properly who ‘owns’ what risk and what that means to your business.
3. Control – going beyond the traditional paper-based risk register and focusing on how to mitigate the risk. This has important implications for reputation in the marketplace. We have seen several times already how a loss of confidence after data leakage, intrusion or Distributed Denial of Service (DDoS) attack can be detrimental to a brand.

Standards will continue to emerge, especially as ISO, PCI-DSS, Cobit, Basel and SOX are beginning to understand that cloud bursting and multi-tenant environments are often aligned with geographical controls around transmission, storage and processing of data.

Getting cloud security right

As companies start using multiple cloud providers, the ability to develop an application, publish it anywhere and then manage it becomes absolutely critical. It is important to continually re-assess the security model impacted by that application, as well as the data provisioning and authentication model that depends on it. A company must understand the storage requirements associated with cloud computing and ensure that a move to the cloud is not accompanied by an ‘out of sight out of mind’ approach to security.

Using the principles of on-premise enterprise computing when moving to the cloud is critical and ensures peace of mind. As a customer, always look to engage with a provider that will demonstrate thought leadership in post-SAS 70 (II) certifications. Try to identify ISO 27001/2 audit capabilities. Engage with your provider – for example, a BITS Shared Assessments programme can provide great assistance. If externally audited, engage with your auditor now, not after migration. Look for a provider that will document the ‘gaps’ between governance, risk and control. Avoid the ones that use a contract as a means of security assurance. It is important to note that data privacy guidelines by the European Union, or the Dutch guidelines ‘Wet Bescherming Persoonsgegevens’, are very specific when it comes to responsibilities of data controllers when engaging with cloud providers.

The Cloud Security Alliance

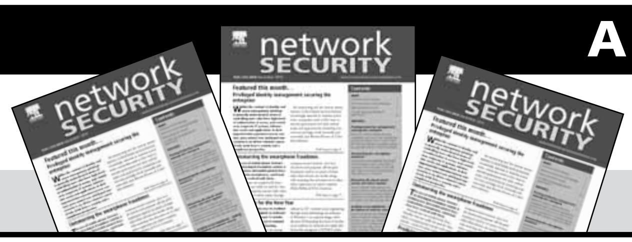
We have witnessed the emergence of the Cloud Security Alliance (CSA), a powerful body that understands the gap in knowledge and the assurance space. The CSA has an incredibly important role and a lot of dedicated work has gone into the creation of security control matrices that have given back control to decisionmakers at customers’ companies.

Providers that support the principles of open source give customers the tools needed to own an entire ‘cloud stack’ with no vendor lock-in and transparent standards. Open source code – a veritable software DNA – helps to make the cloud a secure and regulated place to work, regardless of the hypervisor or provider used. And new Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) environments extend the principles of openness to public, private and hybrid clouds and further into application development, testing and deployment as well as lifecycle management in the cloud.

About the authors

Richard Morrell heads up the Red Hat technical team for cloud in EMEA as the company's senior solutions architect. Having worked for over 15 years in the open source world he also heads up Red Hat's security architecture team in EMEA around cloud and the use of Linux to above top secret environments.

Akash Chandrashekar is a solution architect at Red Hat US, where he works on the systems management subject matter expert team. He holds Red Hat Certified Engineer (RHCE) and Red Hat Network Satellite certifications, and has been in the information technology industry since 1996. He has a bachelors degree in computer information sciences from Devry University in Pomona California and a bachelors degree in mathematics education from California Polytechnic University in Pomona.



...Continued from page 2

certificate downloaded by a browser with one downloaded by the notary. This can help eliminate Man in the Middle (MitM) attacks. Qualys will now provide two of these servers – one in the US and one in Europe. Currently, the system is supported only by Firefox with a beta-level plug-in.

The Convergence project is here: <http://convergence.io/>.

Social networking in the workplace

Many organisations have been caught off-guard by the rise of social networking. And while most firms believe social media is important to their business, a majority of IT security professionals feel the phenomenon represents a threat, according to a Websense survey carried out by the Ponemon Institute.

Some 63% of respondents feel that the use of social media in the workplace is a threat to the business. Only 29% believe they have the necessary security controls in place to deal with it. Networking with colleagues inside the company is widely regarded as acceptable use (85%). But only a minority of firms believe that downloading or watching videos and posting uncensored content during worktime is acceptable.

The chief negative consequences of social networking are diminished productivity (89%) and clogging the organisation's Internet bandwidth (77%). Security risks are the third and fourth most important factors, being data leaks (54%) and an increase in malware infections (51%). In fact, slightly more than half of the surveyed organisations believe they have suffered an increase in malware as a result of employees using social media in the workplace. A further quarter were unsure.

The amount of time workers spend on social media sites varies considerably, and it's something of a mixed picture when it comes to business and non-business use. In the survey, the biggest group consisted of those spending 11-30 minutes a day on such sites, and this was predominantly for business (44%) rather than personal (16%) purposes. Those who spend more time on the sites tend to be doing it more often for non-business reasons.

Kaspersky has also done some research in this area and found that 72% of firms are now blocking access to social networking sites.

The Websense/Ponemon report is available here: <http://www.websense.com/content/ponemon-institute-research-report-2011.aspx>.

Lurid launches attack on Russia

Trend Micro says it has uncovered a concerted campaign of cyber-attacks, dubbed 'Lurid', that has compromised 1,465 computers in 61 countries. So far, the company has identified 47 victims. But the campaign has a number of unusual characteristics, not least of which is that Russia is one of the main victim states and the source of many of the attacks is the UK and US.

Other target countries include Vietnam, Kazakhstan and several members of the Commonwealth of Independent States (the former Soviet Union). For the most part, the attacks were highly targeted – against regions or specific individuals. Many of the victims have been diplomatic missions, government agencies and aerospace-related organisations.

The Lurid malware downloader, also known as Enfal, has been seen before, but is not commonly traded on the cybercrime underground, says Trend. It has been used in the past to attack US Government targets and NGOs. Infections occur via malicious PDF and RAR files.

Inevitably, fingers were pointed at China. However, analysis of the 15 domain names and 10 IP addresses used for the Command and Control (C&C) servers shows that they are mainly in the UK and US. Nevertheless, Trend says that analysis of the domain registrations still suggests a Chinese link. Enfal has been used before in the cyber-espionage networks that became known as GhostNet and ShadowNet, but Trend has found no other links between those networks and Lurid.

EVENTS CALENDAR

2–3 November 2011
RSA Conference China 2011
Beijing, China
Website: www.rsaconference.com/events.htm

3 November 2011
HouSecCon2011
Houston, Texas, US
Website: http://houstonseccon.com

10–11 November 2011
6th Annual Data Protection Practical Compliance Conference
Dublin, Ireland
Website: www.pdp.ie/conference

11–19 November 2011
SANS Sydney 2011
Sydney, Australia
Website: www.sans.org/info/78514

21–22 November 2011
Oil and Gas Cyber Security Forum
London, UK
Website: www.smi-online.co.uk/2011cyber-security1.asp

22–23 November 2011
Information Security Solutions Europe Management
Prague, Czech Republic
Website: http://www.isse.eu.com/

23–25 November 2011
International Conference on Communications, Information and Network Security
Venice, Italy
Website: www.waset.org/conferences/2011/Venice/iccins/

12–15 December 2011
Black Hat Abu Dhabi 2011
Abu Dhabi, UAE
Website: www.blackhat.com