# network SECURITY

ELSEVIER

ISSN 1353-4858 January 2012 www.networksecuritynewsletter.com

## Featured in this issue:

### AMTSO: the test of time?

**The Anti-Malware Testing Standards Organisation (AMTSO) was intended to raise the standard of testing by providing a forum for testing-related discussion, as well as developing standards and best practices for testing.**

It started well as a coalition of anti-malware vendors and mainstream testers resolved to implement a shift from simple-minded static testing to more realistic dynamic testing. While there is undoubtedly more dynamic (or at least hybrid) testing than there was back in 2008, recent changes suggest that working relationships between some testers and vendors have deteriorated. David Harley asks if AMTSO can really continue to build on its achievements so far, or has it already shot its bolt?

*Full story on page 5...*

### Monitoring bad traffic with darknets

**A common form of 'darknet' used by security researchers and analysts is a block of unused address space on a network. As the address space has never been used, any traffic to it is somehow improper.**

By monitoring traffic hitting the darknet one can build up a picture of aberrant traffic without the false positives that plague other technologies, particularly at scale. The majority of this traffic is likely to be malicious. Simon Woodhead of Simwood discusses the best way of creating a darknet and details some of the results you're likely to find – data that you can use to make your networks more efficient and your organisation more secure.

*Full story on page 10...*

### Rethinking the ESB: building a secure bus with an SOA gateway

**For years the Enterprise Service Bus (ESB) has been seen as a corporate integration and messaging backbone upon which application architectures are built. However, this concept must evolve to meet the requirements of today's corporate landscape.**

Service Oriented Architecture (SOA) gateways, originally designed to provide edge security between enterprises exchanging data via web service standards, have been brought inside the firewall to provide a more flexible solution to traditional integration requirements. Jaime Ryan of Layer 7 Technologies argues that SOA gateways give you the capacity to respond to customer demands and provide new, secure interfaces to the data and applications that drive your business.

*Full story on page 14...*

### Hackers attack security organisations

**Attackers affiliating themselves with activist group Anonymous have succeeded in penetrating US security think-tank Stratfor. And hackers in India have managed to steal source code for Symantec software – and in the process have started a controversy over**

*Continued on page 2...*

## Contents

***NEWS***

***FEATURES***

**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:**
€1165 for all European countries & Iran
US$1304 for all countries except Europe and Japan
¥154 600 for Japan
(Prices valid until 31 December 2012)
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

**Notice**
No responsibility is assumed by the Publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made. Although all advertising material is expected to conform to ethical (medical) standards, inclusion in this publication does not constitute a guarantee or endorsement of the quality or value of such product or of the claims made of it by its manufacturer.

**12987**

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

*Continued from page 1*

**whether Western firms have been assisting the Indian Government in intercepting cellphone communications.**

Anonymous hackers operating under the LulzSec banner stole an email database, nearly 50,000 unique email addresses, over 44,000 passwords and around 50,000 credit card details, with around 9,600 being for active cards. The emails have already been used to spam people on the database with messages luring people to a Rick Astley video. Other members of Anonymous denied the group was involved.

The hackers claimed they had made donations of "over a million dollars" to various charities using the stolen card information, but this is almost certainly a gross exaggeration if not completely untrue. The hackers have started to release some of the information, including emails.

Stratfor said the affected accounts related to members who had purchased publications online and that no details were compromised for "individuals or entities that have a relationship with Stratfor" – presumably a reference to government and military customers. The firm shut down its servers for an extended period.

Meanwhile, an Indian group going by the name of Lords of Dharmaraja posted on Pastebin what it claimed were confidential documents relating to Symantec source code and which Symantec confirmed were details – dating back to 1999 – of an API for the product. The group also posted a source code tree, but this has since been taken down. More documents were posted on Google+.

Symantec later admitted that four or five year-old source code relating to enterprise (but not consumer) products had been stolen. It denied that this would affect the security of current products, although it said it is developing a mitigation programme for customers.

The group said the documents were taken from Indian military intelligence servers. The documents and source code were on these servers because Symantec, like many other firms, complies with requests from governments to provide detailed information on their products. Nevertheless, the hackers claimed that the documents were proof of involvement by Western companies in the domestic surveillance activities of the Indian authorities. The hackers made specific reference to the Tactical Network for Cellular Surveillance (TANCS) and said the documents also included technical agreements between the authorities and companies, including RIM, Nokia and Apple, to provide 'backdoors' into communications networks. The US-China Economic and Security Review Commission (USCC) has requested an investigation into one particular memo that appears to show the USCC being specifically targeted.

## Hackers warring in Middle East

**Israel is threatening to treat hackers like terrorists following the disclosure of thousands of Israeli credit card details by a pro-Palestinian hacker. And the incident has kicked off a series of tit-for-tat attacks.**

Hacker 'oxOmar' claimed to be a member of 'Group-XP', which may be affiliated with the Wahhabi Islamic movement. It was reported that the hacker is based in Saudi, but Israeli blogger Amir Fedida claims to have tracked down oxOmar and said he is a UAE citizen living in Mexico.

Cards issued by three Israeli banks – Cal (Cartisey Ashrai Le'Israel), Isracard and Leumi Card – were compromised. The hackers originally claimed to have stolen the details for 400,000 cards, but the banks claimed that only 15,000 of them were active. Many of the details seem to have been taken from the Israeli sports site One.co.li.

Israel's Deputy Foreign Minister, Danny Ayalon, speaking at an event, said that the attack was, "a breach of sovereignty comparable to a terrorist operation, and must be treated as such" and added, "Israel has active capabilities for striking at those who are trying to harm it, and no agency or hacker will be immune from retaliatory action".

As a result of his statements, Ayalon's personal website came under attack.

## In brief

### Attack code threatens websites

In a dramatic demonstration of the need for rapid patching, hackers have released exploit code for an attack method announced at the Chaos Communication Congress in late December, and which was patched by Microsoft for its ASP.NET platform shortly afterwards. The 'HashDoS' vulnerability (CVE-2011-3414), announced on 28 Dec 2011 by German researchers Alexander Klink and Julian Walde, actually affects a number of platforms, including PHP, Ruby, Python, Java and JavaScript. It is a weakness in the way the technologies use hash tables and can lead to denial of service conditions simply through the use of slow connections from a single machine. A specially crafted HTTP request, sending values precomputed to render the same hash values, can potentially consume 100% of a single CPU core for 90-110 seconds. This is because the server must perform a massive number of string comparisons. It would be simple for an attacker with one PC and a low-bandwidth connection to tie up a server with repeated requests. The researchers believe that a file as small as 6KB could tie up a Java-based server. Microsoft issued a patch in a out-of-band update the following day – the only unscheduled update of the year. Then, on 6 Jan 2012, attack code was published on GitHub by someone called 'HybrisDisaster', who used a phrase in the accompanying text suggesting a link with Anonymous. The code mainly consists of a massive text file. Many websites, including those using ASP.NET but which haven't installed the patch, remain vulnerable.

### Another slow DDoS exploit

In addition to the 'HashDos' exploit (above), Qualys researcher Sergey Shekyan has developed another form of 'slow' denial of service attack, joining the ranks of Slowloris and OWASP's Slow HTTP Post. The new Slow Read attack uses a perfectly legitimate HTTP request, but then accepts the response at a very slow rate. In order to work, the attacker must know the server's send buffer size, and then use a smaller receive buffer while requesting a response that is larger than the send buffer (not difficult to achieve). Shekyan has added the exploit to his slowhttptest tool.

### More Android malware

Researchers have discovered yet more Android malware, including some that is exploiting concern about the services of legitimate yet controversial firm Carrier IQ. Towards the end of 2011, it was discovered that many smartphones automatically send data to Carrier IQ – some of it relating to technical issues such as signal strength, battery performance and dropped calls, but some of which could be used to monitor users' browsing habits and other potentially private information. While the row over Carrier IQ continues, cyber-criminals have released an app for Android phones – Android.Qicsomos – that claims to remove Carrier IQ but actually runs up charges through a premium-rate texting exploit. Currently, Android users in France are being targeted, and the app comes with branding similar to that of a major carrier. According to Irfan Asrar of Symantec, when the user launches the app, it sends four premium-rate SMS messages, then uninstalls itself. The app is signed with a certificate from the Android Open Source Project, which means that it will evade permissions checking on many devices, especially older ones that may trust this certificate by default. Meanwhile, the technique of producing trojanised versions of legitimate apps continues: Symantec also discovered an app called Stevens Creek Software that bundles some popular games, plus a nasty payload. The installation process fools users into visiting a malicious website.

### Mixed picture for infosec professionals in the UK…

If the importance of information security is reflected by the money paid to specialists in the field, then there seems to be some confusion, at least in the UK. According to recruitment firm Acumin Consulting, salaries in the information security and risk management sector were generally stagnant in the past quarter. However, CISOs have seen starting salaries rise from £115,000-180,000 to £120,000-200,000. Network security engineers and information security directors also saw average salary increases of £5,000 during the quarter. Yet security consultants saw a drop of about the same amount, and information security and risk managers in SMEs also saw a slight decline. So it seems that those at the senior end of the scale – who set policy – continue to enjoy ever-greater benefits while those who actually implement and manage security are not so well rewarded.

### …but recruitment on the rise in the US

The Information Security Media Group has analysed US Bureau of Labor Statistics data and concluded that, while most areas of employment are seeing a slump, there are more jobs than ever for information security professionals. In the last quarter of 2011, infosecurity jobs rose to more than 51,000, compared to 37,000 in the first quarter. And the figures showed no joblessness in this sector throughout 2011. Infosecurity professionals constitute around 1% of IT positions. In the IT sector generally there was an unemployment rate of 3.9%, which is still lower than the 8.8% rate for all sectors of industry.

### US-CERT falls victim to phishing

Cyber-criminals have launched a phishing campaign with emails purporting to come from US-CERT. The activity appears to be carefully targeted with many of the recipients being at large private sector firms, government contractors, federal agencies and local government. The campaign has been so heavy that US-CERT encountered problems with receiving legitimate mail. The emails carried a zip file containing a malicious executable attempting to look like a saved email file: 'US-CERT Operation Center Reports .eml.exe'.

### Maturity model for US cyber-security

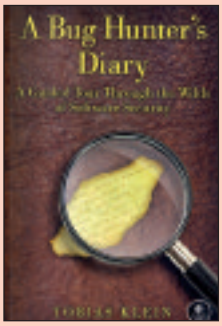
The US Department of Energy is leading a new initiative, sponsored by the White House and supported by the Department of Homeland Security, to provide utilities with a maturity model against which they can assess their cyber-security. The Electric Sector Cybersecurity Risk Management Maturity project is aimed at utility companies and grid operators and will help them measure their current capabilities and analyse gaps in their defences. More than a dozen electric utilities and grid operators are expected to participate in the pilot programme to test the maturity model, assess its effectiveness and validate results. This public-private partnership and pilot programme will help develop a risk management maturity model that is expected to be made available to the electric sector later this summer.

### UK firms and young workers too complacent

While cyber-attacks are on the rise across the world, only 10% of UK companies believe themselves to be at risk, according to a report from Kaspersky. Elsewhere in Europe, 30% of firms are concerned. "While indiscriminate attacks still form the lion's share of cybercrime, it is clear that the number of targeted attacks is increasing," said David Emm, senior security researcher at Kaspersky Lab. "This year we have seen a steady stream of attacks focused on specific organisations. UK companies need to protect themselves in order to avoid becoming a victim of a targeted cyber-attack." Meanwhile, research by Cisco has shown that, around the world, security policies are routinely ignored by around 70% of younger employees. The Cisco Connected World report suggests that it may need to be the organisations and their policies that need to change, not the workers, as the breaches are often connected to a desire to be more connected and use a range of mobile devices. Among the reasons for breaking the rules were: a need to access unauthorised programs and applications to get the job done (22%); not having time to think about policies when working (18%); the inconvenience of the policies (16%); forgetfulness (15%); and lack of supervision (14%).

# Reviews

## BOOK REVIEW



**A Bug Hunter's Diary**
**Tobias Klein.**
**No Starch Press**
**(ISBN: 978-1-59327-385-9).**
**Price: $39.95, 208pgs, paperback.**

As we know only too well, a very large percentage of the security vulnerabilities that hackers and cyber-criminals exploit derive from inadequate coding. Even simple errors in software can provide an opening that can lead to denial of service crashes, shell access, privilege escalation and a host of other exploits.

The bad guys spend days and weeks poring over code – often disassembled from executables – to find weak spots. Of course, white-hat security researchers and specialists do the same. One of them is Tobias Klein, founder of NESO Security Labs. And in this book he shares with us what he does, how he works and what he finds.

This is not theoretical: the bulk of the book contains seven case studies of vulnerabilities in real-world software discovered by Klein. Not only does he explain, in detail, how he uncovered the flaws, he also tells us how the software vendors reacted. And for those inclined to think only of the Microsoft Windows platform when it comes to vulnerable software, it's worth noting that one of the flaws was in the iPhone OS (now iOS), another was a kernel bug in Apple's OS X, and yet another was a kernel bug in OpenSolaris.

Klein's preferred approach is static analysis of source or disassembled code, but he also touches on dynamic approaches such as fuzzing. The vulnerabilities he uncovers are the classics – NULL pointer dereferences, type conversion flaws and our old favourite, the buffer overflow.

After a brief overview of the technology – what debuggers and disassemblers are, a definition of memory errors and a few paragraphs about why EIP is important – the author gets straight into the case studies. Most date back several years – as far as 2007 – and the flaws have since been remedied by the vendors. But it's the principles and techniques that are important, rather than the vulnerabilities themselves.

As the book's title suggests, Klein has adopted a diary form, so each chapter is broken down into dated entries taking you along a chronological journey, starting with the moment the author first becomes interested in a specific issue. For example, when he learns that a friend has jailbroken his iPhone, Klein sees seizes this as an opportunity to explore iOS for flaws.

He takes us step-by-step through the process of searching the code for weak spots. In the case of the VLC media player, for example, he finds what he's looking for in the source code – an input stream variable contained in a struct in a demuxer. Then he shows how he traces the input data: in the same example, he looks for references to the struct and finds one in a function that uses a buffer with no bounds checking.

Next, Klein takes us through how he exploits the vulnerability. In the case of VLC, he does this by manipulating a TiVo movie file to overflow the vulnerable buffer. He was able to gain control of the value of EIP leading to the ability to execute arbitrary code. All through this process, and with the following six cases studies, we're provided with copious code samples, debugger and disassembler output and screenshots.

The next step is disclosure. Klein shares with us both the reasoning behind how he disclosed the vulnerabilities and the responses received. In some cases – the VLC one, for example – it took a couple of iterations before the problem was fixed. There's also some discussion about why anti-malware features, such as Windows' DEP and ASLR, often fail to work. Each chapter rounds off with lessons learned, and throughout there are useful footnotes pointing the reader to further information, mostly web-based.

To get the most out of this book, you'll need to be comfortable reading C code and know your way around tools such as IDA Pro. And you need to understand the key vulnerability types, although here Klein helps by providing descriptions of buffer overflows, NULL pointer dereferences, type conversion errors and Global Offset Table (GOT) overwrites in an appendix. Other appendices provide command cheat sheets for debuggers and a brief overview (with useful references) of mitigation techniques and technologies.

Some people may feel that something is missing from this book. Indeed, Klein says as much, and explains why. Although he describes how the vulnerabilities he found could be exploited, there is no full exploit code. Klein is based in Germany where so-called 'anti-hacker' laws forbid the sharing of such information (as well as outlawing what most security researchers and professionals regard as standard tools of their trade). This is an interesting example of how a too-widely drafted law can have a chilling effect on the experts who are seeking to resolve the very problems the law was meant to address.

Still, it's the journey that matters here, and Klein gives us a fascinating, technically detailed insight into how zero-day vulnerabilities are found. There's a good argument that this book should be made required reading for all programmers. The simple – and perhaps depressing – fact is that all of these vulnerabilities could have been easily avoided. Yes, that's easy to say when you're not a programmer under pressure to get the product shipped. But several lessons crop up again and again – always check input, validate return values, define proper error conditions and use mitigation technologies where available.

Aside from coders, this book will also be valuable to those on the path to becoming security professionals, particularly pen-testers developing the skills to spot and exploit weaknesses. And, in fact, it will provide a fascinating insight for anyone who wants to understand software insecurities and what can be done to fix them. Even if your technical skills aren't up to understanding every detail of the code presented, you'll be able to get the gist. And never again will you take the security of the software you use for granted.

# AMTSO: the test of time?

David Harley, ESET North America

David Harley

**The Anti-Malware Testing Standards Organisation (AMTSO) was formally founded in May 2008.[1] Since then, the organisation has generated some serious documentation and even, from time to time, managed some (often controversial) press coverage.[2,3] That in itself is something of an achievement, considering that the eyes of many journalists glaze over at the very mention of testing. They often don't perceive it as difficult or challenging: there is a whole school of quick-and-dirty product reviews in generalist computer magazines where non-specialists attempt some evaluation of detection performance.**

AMTSO's foundation was the result of many years of concern on the part of anti-malware vendors and some mainstream product testers – concern, that is, that many individuals and organisations offered (and continue to offer) comparative testing and product certification at such a low level of competence and accuracy, consistently underestimating the knowledge and resources required to perform a meaningful test.[4] The organisation originally announced its intention to provide a forum for discussion, to develop standards and best practices in testing, foster education and awareness, and to provide or at least encourage the provision of tools and resources.

## Aims and aspirations

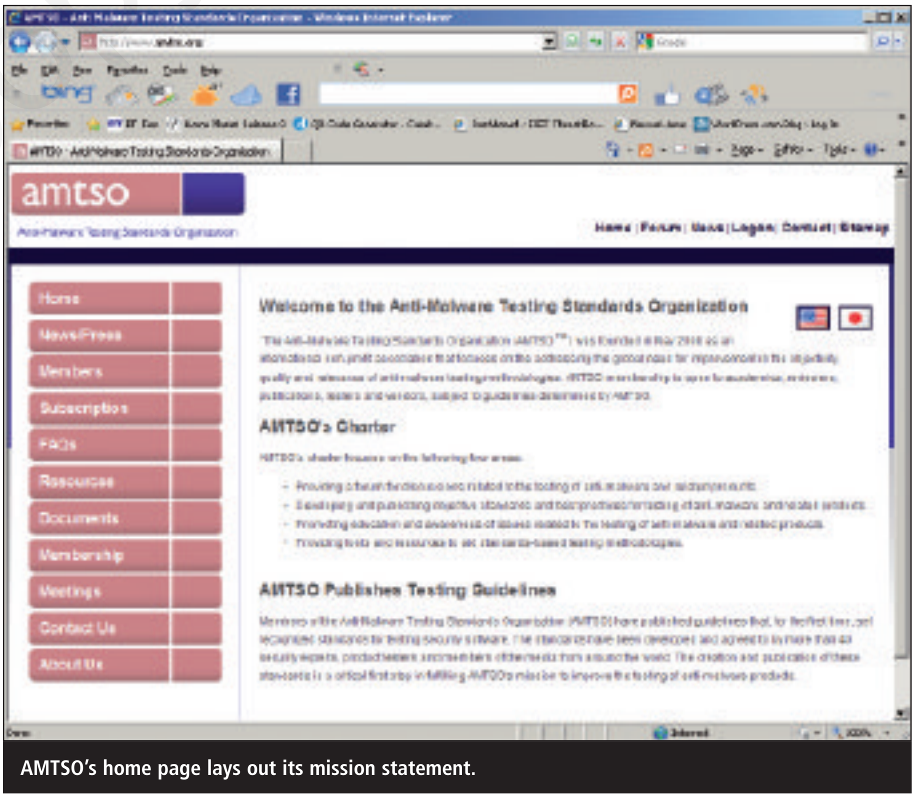
AMTSO's aim isn't always stated as clearly as it might be. But it can be put fairly simply, as per the mission statement on its own index page: it was intended to address the global need for improvement in the objectivity, quality and relevance of anti-malware testing methodologies.[5] This can be seen as largely focused on the issues of objectivity and impartiality, quality and relevance.

*"Too much testing – not all of it amateur – is about comparing apples to oranges"*

The objectivity and impartiality requirements mean that testing should be free (to the extent that this is possible) of hidden agendas and bias – from any source. The test audience is entitled to expect that the test is executed and documented in such a way as to promote that audience's best interests.

Quality and sound practice mean, essentially, recognition of the fact that testing *in general* is a discipline that requires technical knowledge and experience. Testing of software adds a further layer of complexity, and the testing of anti-malware products requires understanding of the complexities of malware and anti-malware technology that is largely restricted to experts and specialists.

Relevance to and consistency with avowed testing aims is at least as important as the other considerations, and that means something far more complex than statistical accuracy – though that itself is rarely achieved. Too much testing – not all of it amateur – is about comparing apples to oranges or even melons to raisins – trying to compare products that aren't intended to work in the same way.[6] Even where products have largely comparable base functionality, as is the case with most commercial anti-malware, out-of-the-box testing is not a level playing field unless all that's being tested is out-of-the-box configuration. Even then, reviews based on out-of-the-box testing are all too likely to reflect the prejudices of the tester better than the overall capabilities of the products, or even of their detection capability.



Welcome to the Anti-Malware Testing Standards Organization

[illegible]

AMTSO's Charter

[illegible]

AMTSO Publishes Testing Guidelines

[illegible]

AMTSO's home page lays out its mission statement.

## Protection and self-protection

AMTSO, as it was originally founded, was important because it pooled knowledge from both the security industry and the security testing industry, giving each the opportunity to learn from the other. Working together, they could implement a functional system of checks and balances where excessive self-interest could be controlled by a community that was more than an AV pressure group keeping the testers in line. However, much of the coverage the organisation has received is hostile. That in itself is not all bad: if everyone loved it, it would probably mean it had been ineffective at raising standards without knuckling under to vested interests. But most of that hostility is inspired by the assumption that AMTSO is, in fact, an AV pressure group. That's understandable, given that a high proportion of its members have, from the beginning, been representatives of AV companies. Journalist Kevin Townsend once asked, "Is AMTSO the anti-malware industry looking after itself? (It seems to be almost entirely composed of anti-malware companies and anti-malware testing companies; with little if any input from users.)"[7]

***"No-one believes that the anti-malware vendors aren't interested in their own bottom line ... many people assume that the AV industry is the ultimate in cynical exploitation of Fear, Uncertainty and Doubt"***

Naturally there's an element of self-protection. All testing hurts products that get bad reviews. But poor testing isn't only a problem because of the problems it creates for products that do badly: the industry isn't so self-protective and co-operative that it tries to look after the weaker products in its market sector. Testing that hurts good products while promoting not-so-good products is not just irrelevant and bad for the sales figures of the misevaluated product. It's much worse for customers who put their trust in a product that gives less protection than a test suggests.

Of course, no-one believes that the anti-malware vendors aren't interested in their own bottom line.[8] In fact, many people (including quite a few journalists) assume that the AV industry is the ultimate in cynical exploitation of Fear, Uncertainty and Doubt. And, in fact, most AV marketing is based on consumers' fear of negative consequences if they don't use security products – though that doesn't necessarily make the security industry any more exploitative than the pharmaceutical industry or even the agricultural industry.

The unusually pronounced dislike and distrust of the anti-virus industry is too complex to consider adequately in a paragraph or even a single article.[9] However, two significant yet inconsistent factors are in play: on one hand, the industry is assumed to fabricate psychological dependence by exaggerating the need for its services; yet on the other hand it is lambasted for failing to meet that need by eliminating the malware problem.

***"The acceptance by testers of practices agreed by a community of vendors and testers doesn't, in principle, work to the advantage of any one vendor"***

"Testing is changing whether vendors like it or not," as one journalist put it.[10] As a matter of fact, vendors *do* like it: they've been advocating better testing for a long time and complaining bitterly about generally low standards in that area.[11] While vendors sometimes have a somewhat self-interested interpretation of what constitutes 'good testing' in the context of tests in which they have participated (willingly or otherwise), the industry as a whole has some pretty clear and more-or-less impartial views on what constitutes good practice in testing. After all, the acceptance by testers of practices agreed by a community of vendors and testers doesn't, in principle, work to the advantage of any one vendor.

## Not all practice makes perfect

So what constitutes good practice? Actually, it's probably easier to define bad practice: at any rate, bad practice can certainly embrace some or all of these well-known and well-documented methodological approaches, though not every technique that's guaranteed to raise the hackles of vendors (and many testers) is included here:[12]

- Sample sets picked up somewhere on the Internet, or out of the tester's own mailbox, and possibly 'validated' by his or her own favourite scanner (preferably one that came free), or by submitting samples to VirusTotal and assuming that anything detected by any scanner is malicious.[13] Unfortunately, these forms of pseudo-validation do not necessarily eliminate the possibility of false positives, inappropriate detection of garbage files and so on, and a sound test cannot be based on invalid samples.[14]
- Samples supplied by the company that publishes one of the products under test (strangely enough, those products usually do rather well).
- Simulated malware. In general, the security industry considers a detection of malware that isn't malware as a false positive, though there are exceptions, of which the most obvious is the EICAR test file.[15] However, the naming of that file is misleading: the test file was never designed for product detection testing, but rather as a tool for checking that an anti-virus product is installed and capable of detecting real malware. There have been many attempts over the years to evaluate detection performance using modified versions of the EICAR test file, tending to finish up with something that is neither the EICAR test file, nor malware, nor a realistic simulation of malware.[16]
- Kit-generated or self-created malware which may or may not be valid – 'valid' meaning code that is both malicious and capable of being executed.[17]

## Creationism and testing

The use of unequivocally 'black hat' malware kits poses a number of technical and methodological problems. However, the use of self-created 'malware' adds difficulties closely related to those that accompany the use of simulations.

Malice, by legal definition, includes some element of evil intent.[18] Since security software is normally intended to detect malicious software rather than simulated malware, the tester's aim is presumably to simulate malice by including some equivocally malicious payload or other component that 'should be' detected. This approach presents considerable technical and philosophical problems, though the presence of genuinely self-replicating (viral) behaviour is an example – possibly the only example – of a behaviour that is almost always considered to incorporate malicious intent. However, there are ethical and legal issues that accompany even controlled replication that, combined with other technical and ethical issues, render custom-created test malware practically useless. The anti-malware industry hates newly-created or modified malware with a passion and for a variety of reasons, but the most pressing from a technical standpoint is that when testers create or modify malware, there's a good chance that the finished article isn't malware as the industry defines it.

***"While the intentions of many testers may have been honourable, misconceived approaches invariably generate problems and controversy"***

Of course, testers don't have to conform to the anti-malware industry's definitions of what malware really is, but the question that must then be asked is whether and why the industry should conform to a maverick tester's view of what should be detected.

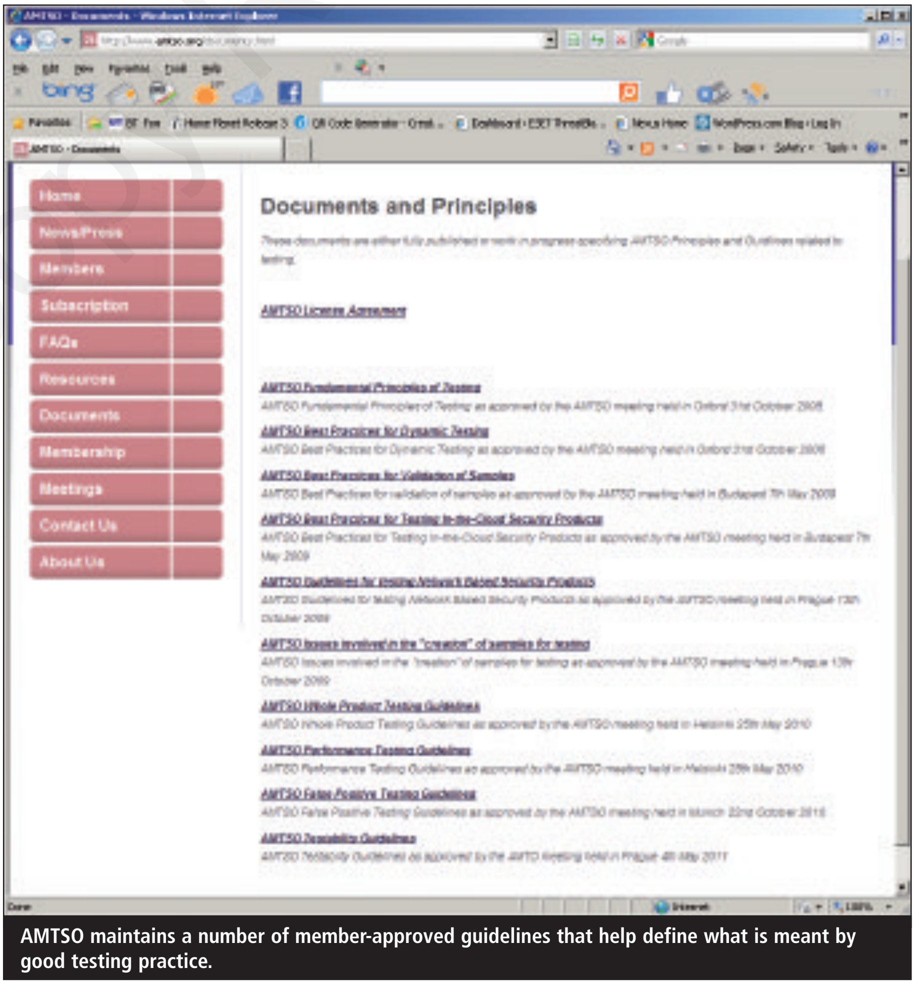
Until AMTSO, the AV industry wasn't very good at telling testers (or the public) what sort of tests it *did* consider legitimate.[19] While the intentions of many testers may have been honourable – though it's not unknown for tests to be inspired by hidden agendas that have little to do with the common good – misconceived approaches like the above invariably generate problems and controversy, and may be totally inappropriate, misleading, and open to abuse. There have been occasional concerted efforts to respond to a particularly inappropriate test, but the overall impression in the public mind was of a peevish anti-virus industry that didn't like the way testing was carried out but was reluctant to provide feedback more positive than "If you have to ask how to test, you aren't qualified".[20] There's some truth in that, of course, since asking for help is by definition an admission that the tester perceives a need for improvement. But this attitude doesn't help people who are genuinely interested in improving their testing. Even worse, it leaves the field open to those whose apparent self-confidence may not be matched by their competence.

## Practice and principles

When AMTSO started to answer the question, it was accused of telling testers how to test. As indeed it did, in a sense: even before the organisation was formally constituted, the vendors and testers who were primarily responsible for its formation were trying to move testing away from simplistic static testing towards more accurate (but more resource-intensive) dynamic, whole-product testing.[21,22,23]

AMTSO's 'Fundamental Principles of Testing', and its growing collection of AMTSO-generated and membership-approved guideline documents, represent an important milestone in the maturation of the anti-malware industry, offering genuine high-level guidance on what is meant by good testing practice. The nine fundamental principles of testing as defined by AMTSO are as follows:[24]

1. Testing must not endanger the public.
2. Testing must be unbiased.
3. Testing should be reasonably open and transparent.
4. The effectiveness and performance of anti-malware products must be measured in a balanced way.
5. Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.
6. The testing methodology must be consistent with the testing purpose.



Documents and Principles

These documents are either fully published or work in progress specifying AMTSO Principles and Guidelines related to testing.

AMTSO License Agreement

AMTSO Fundamental Principles of Testing
AMTSO Fundamental Principles of Testing as approved by the AMTSO meeting held in Oxford 31st October 2008

AMTSO Best Practices for Dynamic Testing
AMTSO Best Practices for Dynamic Testing as approved by the AMTSO meeting held in Oxford 31st October 2008

AMTSO Best Practices for Validation of Samples
AMTSO Best Practices for validation of samples as approved by the AMTSO meeting held in Budapest 7th May 2009

AMTSO Best Practices for Testing In-the-Cloud Security Products
AMTSO Best Practices for Testing In-the-Cloud Security Products as approved by the AMTSO meeting held in Budapest 7th May 2009

AMTSO Guidelines for testing Network Based Security Products
AMTSO Guidelines for testing Network Based Security Products as approved by the AMTSO meeting held in Prague 13th October 2009

AMTSO Issues involved in the "creation" of samples for testing
AMTSO Issues involved in the "creation" of samples for testing as approved by the AMTSO meeting held in Prague 13th October 2009

AMTSO Whole Product Testing Guidelines
AMTSO Whole Product Testing Guidelines as approved by the AMTSO meeting held in Helsinki 25th May 2010

AMTSO Performance Testing Guidelines
AMTSO Performance Testing Guidelines as approved by the AMTSO meeting held in Helsinki 25th May 2010

AMTSO False Positive Testing Guidelines
AMTSO False Positive Testing Guidelines as approved by the AMTSO meeting held in Munich 22nd October 2010

AMTSO Testability Guidelines
AMTSO Testability Guidelines as approved by the AMTO meeting held in Prague 4th May 2011

AMTSO maintains a number of member-approved guidelines that help define what is meant by good testing practice.

7. The conclusions of a test must be based on the test results.
8. Test results should be statistically valid.
9. Vendors, testers and publishers must have an active contact point for testing-related correspondence.

While it may seem hard to argue with such high-level statements, application of these principles to tests that actually exist in the real world has proved challenging.

## Watching the watchers

One of AMTSO's early initiatives was to add analysis and review of current testing to its list of objectives. It made valiant attempts to meet that objective but generated so much controversy that the whole process, essentially based on evaluating conformance with the nine principles, is now undergoing exhaustive review.[25] How did it go so wrong?

One major contributing factor is that the inevitable tension between the interests of vendor marketing and tester marketing resulted in some undesirably self-interested pressure on both sides. This caused some testers to take a more arms-length position or withdraw entirely.

***"Large testing organisations with a consumer focus often make a point of not engaging face to face with the manufacturers whose products are under test, for fear of undue influence"***

The introduction of a second-tier subscriber model in addition to the first-tier membership model allowed them a trade-off.[26] While subscribers have less influence on the directions AMTSO takes, they still have input, it costs them less, they're under less pressure to conform to AMTSO recommendations for good practice that they consider unrealistic, and they're less susceptible to pressure from vendors trying to negotiate better test results by using AMTSO as a threat. Of course, a somewhat similar trade-off is available to vendors, but the withdrawal of a vendor has less impact (positive or negative) on AMTSO's image than the withdrawal of a tester.

## Where did all the testers go?

There have been energetic attempts to recruit a wider range of organisations with a security testing remit, but with very little success. Some have not considered the advantages of membership sufficient to justify the cost, and others have declined to join an organisation largely made up of the companies they test and with an insufficiency of testers. The latter view is more than a chicken/egg paradox.[27] Large testing organisations with a consumer focus often make a point of not engaging face-to-face with the manufacturers whose products are under test, for fear of undue influence.

Unfortunately, there is a practical problem with this principled stand: you don't have to be an engineer to test a washing machine or even a digital SLR – though in the latter case it helps to know more than a little about photography – and you don't need to be a programmer to compare word processors. But the very nature of the security industry and the threatscape it tries to address and mitigate suggests that this aloofness doesn't work to the advantage of the customer. Even a comparative test of editing software is likely to be influenced by the tester's subjective understanding of what a product 'should' do, and a journalist's requirements and expectations are likely to be quite different from those of a home user, an academic, a lawyer and so on. Outsourcing testing to a testing specialist may be one way round this objection, but in practice, organisations that take this route often make use of an organisation whose expertise and contacts are not necessarily in malware/anti-malware technology.

## Testing the testers

Some testers have expressed a fear that AMTSO will compromise their ability to provide good testing. But the use of the word 'standards' in the organisation's name does it no favours here.

AMTSO does not and should not prescribe testing methodologies: rather, it provides guidance at varying levels of technical sophistication, put together and approved by people with considerable expertise in complementary aspects of testing and the technology under test. After all, it's hard to argue with transparency, relevance and lack of bias.

AMTSO doesn't set standards in a formal sense, like BSI or ISO, and does not say who is or isn't allowed to test.[28] Perhaps someone should, but a body controlling the certification of testers shouldn't be controlled itself by any single sector – not the academic community, the testing organisations, the anti-malware industry or their customers.[29] And the generation of true standards requires a collaborative effort across a wide range of stakeholders, perhaps under the umbrella of an impartial group such as IEEE.

***"Vendors may not feel (or resent that) they need testers, but tests are, for better or worse, part of the marketing ecology"***

Someone should be holding testers and reviewers to account for the accuracy of their testing and conclusions, but at this time, AMTSO does not seem to have the credibility to address the issue by virtue of its review analysis process, at least in its current (suspended) form. Sadly, it seems inevitable that AMTSO will have to do some serious PR, polishing its image rather than its core processes, before it can usefully address that objective, even if it can mitigate conflicts between the two main groups that constitute its membership.[30] It needs to do this not only to mitigate the poor image that the AV industry has in general, but also in order to persuade testing organisations that they can work with the AV industry without being subjected (or being seen as being subjected) to inappropriate pressure.

## Breaking down mistrust

Security product testing and security software publishing are two sides of the same coin (no currency pun intended). But they are industries, and their aims are not totally compatible. Testers need AV to evaluate, so that they can sell their results. Vendors may not feel (or resent) that they need testers, but tests are, for better or worse, part of the marketing ecology: furthermore, good testing gives vendors feedback on how they're doing in terms of popularity, effectiveness etc. Actually, so does bad testing, but in that instance it's not always useful feedback. Both industries have to watch their bottom line, and each has an impact on the other's financial viability.

The establishment of AMTSO gave testers that already had a good working relationship with the industry a chance to maintain and build on those links and also offered a chance to break down the mistrust between the industry and testers that don't have such links.[31] Sadly, neither industry has taken full advantage of that opportunity.[32] It would be a pity if the organisation didn't raise its game in that respect. However, an equal priority should be given to widening the range of informational and educational resources offered not only to testers, but also to the general public – not only adding to such content, but by maintaining the currency of the resources already there.

## About the author

*David Harley, senior research fellow at ESET North America (http://blog.eset.com), has researched and written about security since 1989. His background is in social and computer science and systems and security administration. He is a director of the Anti-Malware Testing Standards Organisation (AMTSO), and CEO of Small Blue-Green World and AVIEN. His books include 'Viruses Revealed' and the 'AVIEN Malware Defense Guide'. He is a Fellow of the BCS Institute, and also holds qualifications in security management, service management and security auditing. There's more information about him at: http://en.wikipedia.org/wiki/david_harley.*

## Resources

- AMTSO Documents and Principles. Accessed 28 Nov 2011. http://amtso.org/documents.html.
- Gordon, Sarah. 'Are Virus Simulators Still A Good Idea?' Accessed 28 Nov 2011. www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJG-3WP2C4W-4&_user=10&_coverDate=09%2F30%2F1996&_rdoc=1&_fmt=high&_orig=search&_sort=d&_docanchor=&view=c&_searchStrId=1397764983&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=ce3def7e5f12cb12f560a468b02c761d.
- Harley, David. 'Untangling the Wheat from the Chaff in Comparative Anti-Virus Reviews'. Small Blue-Green World, 2007. Accessed 28 Nov 2011. www.eset.com/resources/white-papers/AV_comparative_guide.pdf.
- Kuo, Jimmy. 'Let Telemetry Be Your Guide'. Microsoft, 16 July 2009. http://blogs.technet.com/b/mmpc/archive/2009/07/16/let-telemetry-be-your-guide-a-proposal-for-security-tests.aspx.
- Vrabec, Jan. 'Generalist Anti-Malware Product Testing'. ESET, 25 Jan 2010. Accessed 28 Nov 2011. www.eset.com/blog/2010/01/25/generalist-anti-malware-product-testing.

## References

1. AMTSO. 'Security Software Industry Takes First Steps Towards Forming Anti-Malware Testing Standards Organisation'. AMTSO, 4 Feb 2008. Accessed 28 Nov. http://amtso.org/amtso-formation-press-release.html.
2. Harley, David. 'Antivirus Testing and AMTSO: Has anything changed?' AMTSO, 2010. Accessed 28 Nov 2011. www.amtso.org/uploads/cfet2010-anti-virus-testing-and-amtso.pdf.
3. AMTSO. 'AMTSO in the Media'. AMTSO, 2 Jun 2010. Accessed 28 Nov 2011. http://amtso.wordpress.com/amtso-in-the-media/.
4. Tanner, Sarah. 'A Reader's Guide to Reviews'. Virus News International, November 1993: 40-41, 48.
5. Anti-Malware Testing Standards Organisation. Accessed 28 Nov 2011. www.amtso.org/.
6. Harley, David. 'Making Sense of Anti-Malware Comparative Testing'. Information Security Technical Report, 2009. Accessed 28 Nov 2011. http://dx.doi.org/10.1016/j.istr.2009.03.002.
7. Townsend, Kevin. 'AMTSO: a serious attempt to clean up anti-malware testing; or just a great big con?' 15 Jun 2010. Accessed 28 Nov 2011. http://kevtownsend.wordpress.com/2010/06/15/amtso-a-serious-attempt-to-clean-up-anti-malware-testing-or-just-a-great-big-con/.
8. Townsend, Kevin. 'Anti-Malware Testing Standards Organisation: a dissenting view'. 27 June 2010. Accessed 28 Nov 2011. https://kevtownsend.wordpress.com/2010/06/27/antimalware-testing-standards-organisation-a-dissentingview/.
9. Harley, David. 'I'm OK You're Not OK'. Virus Bulletin, November 2006. Accessed 28 Nov 2011. www.virusbtn.com/virusbulletin/archive/2006/11/vb200611-OK.
10. Finley, Klint. 'Antivirus Product Testing is Changing, Whether Vendors Like it or Not'. ReadWrite Enterprise, 25 Jun 2010. Accessed 28 Nov 2011. www.readwriteweb.com/enterprise/2010/06/antivirus-product-testing-changing.php.
11. Wells, Joe et al. 'Open Letter'. Cybersoft,, 2000. Accessed 28 Nov 2011. http://cybersoft.com/whitepapers/paper_details.php?content=cs008.
12. Harley, David; Lee, Andrew. 'Testing, Testing: Anti-Malware Evaluation for the Enterprise'. AVAR Conference, 2007. Accessed 28 Nov 2011. www.eset.com/resources/white-papers/Testing_Testing.pdf 2007.
13. Harley, David; Canto Julio. 'Man, Myth, Malware and Multiscanning'. Cybercrime Forensics Education & Training Conference, September 2011.
14. Košinár, Peter; Malcho, Juraj; Marko, Richard; Harley, David. 'AV Testing Exposed'. Virus Bulletin Conference, 2010. Accessed 28 Nov 2011. http://go.eset.com/us/resources/white-papers/Kosinar-etal-VB2010.pdf.
15. Harley, David; Myers, Lysa; Willems, Eddy. 'Test Files and Product Evaluation: the Case for and against Malware Simulation'. AVAR Conference, 2011. Accessed 28 Nov 2011. http://go.eset.com/us/resources/white-papers/AVAR-EICAR-2010.pdf.
16. Willems Eddy. 'EICAR 2010: Rainy Days in Paris'. Virus Bulletin, June 2010.
17. AMTSO. 'Issues Involved In The "Creation" Of Samples For Testing'. AMTSO, 13 Oct 2009. Accessed 28

Nov 2011. www.amtso.org/amtso---download---issues-involved-in-the-creation-of-samples-for-testing.html.

18. Malice (legal term). Accessed 28 Nov 2011. http://en.wikipedia.org/wiki/Malice_(legal_term).

19. Harley, David. 'AMTSOlutely Fabulous'. Virus Bulletin, April 2010: 11-12. Accessed 28 Nov 2011. http://amtso.org/uploads/vb_amsto_article_jan_2010.pdf.

20. Harley, David; Bridwell, Larry. 'Daze Of Whine And Neuroses (But Testing Is FINE)'. Virus Bulletin Conference, Sep 2011. Accessed 28 Nov 2011. www.virusbtn.com/pdf/conference_slides/2011/Harley-Bridwell-VB2011.pdf.

21. CARO. Workshop Presentation Slides. F-Prot, 2007. Accessed 28 Nov 2011. www.f-prot.com/workshop2007/presentations.html.

22. Harley, David. 'Execution Context In Anti-Malware Testing'. EICAR Conference, 2009. Accessed 28 Nov 2011. http://smallbluegreenblog.wordpress.com/2009/05/15/execution-context-in-anti-malware-testing.

23. Muttik, Igor; Vignoles, James. 'Rebuilding Anti-Malware Testing for the Future'. Virus Bulletin Conference, 2008. Accessed 28 Nov 2011. http://downloadcenter.mcafee.com/products/mcafee-avert/whitepapers/muttikvignoles_vb2008.pdf.

24. AMTSO. 'Anti-Malware Testing Standards Organisation: Fundamental Principles of Testing". 31 Oct 2008. Accessed 28 Nov 2011. www.amtso.org/amtso---download---amtso-fundamental-principles-of-testing.html.

25. Harley, David; Bridwell, Larry. 'Daze Of Whine And Neuroses (But Testing Is FINE)'. Virus Bulletin Conference, 2011. Accessed 28 Nov 2011. www.amtso.org/uploads/cfet2010-antivirus-testing-and-amtso.pdf.

26. AMTSO. 'AMTSO Widens the Conversation of Anti-Malware Testing with New Subscription Option'. AMTSO, 25 Oct 2010. Accessed 28 Nov 2011. www.amtso.org/pr-20101025-amtsowidens-the-conversation-of-anti-malware-testingwith-new-subscription-option.html.

27. Chicken Or The Egg. Accessed 28 Nov 2011. http://en.wikipedia.org/wiki/Chicken_or_the_egg.

28. Harley, David. 'AMTSO not ISO'. AMTSO, 6 Jul 2010. Accessed 28 Nov 2011. http://amtso.wordpress.com/2010/07/06/amtso-not-iso-standards-and-accountability/.

29. Harley, David; Lee, Andrew. 'Who Will Test The Testers?' Virus Bulletin Conference Proceedings, 2008. Accessed 28 Nov 2011. www.eset.com/resources/white-papers/Harley-Lee-VB2008.pdf.

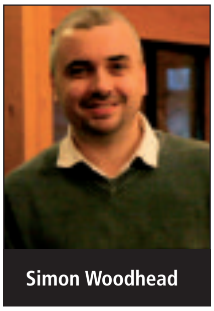
30. Lee, Andrew. 'The edge of reason(ableness): AV Testing and the new creation scientists'. AVIEN, 7 Jul 2010. Accessed 28 Nov 2011. http://avien.net/blog/?p=539.

31. AMTSO. Accessed 28 Nov 2011. www.amtso.org/quote-sheet.html.

32. Harley, David. 'Antivirus Testing and AMTSO: Has anything changed?'. Computer Forensics Education and Training, Sep 2011. Accessed 28 Nov 2011. www.amtso.org/uploads/cfet2010-antivirus-testing-and-amtso.pdf.

# Monitoring bad traffic with darknets

**Simon Woodhead, Simwood**


Simon Woodhead

**A common form of 'darknet' used by security researchers and analysts is a block of unused address space on a network. As the address-space is unused, and ideally has never been used, any traffic destined for this address-space is in some way improper. By monitoring traffic hitting the darknet we can build up a picture of aberrant traffic without the false positives that plague other technologies, particularly at scale.**

Only three explanations for such traffic are plausible:

- Misconfiguration
- Research networks
- Nefarious activity.

Although these three reasons are all possible, the analysis of traffic by those who operate darknets strongly suggests the majority of traffic fits into the last category – it is both improper and of malicious intent. We'll look closely at some real-world results, but in broad terms the various events that this wide-ranging category can contain include network scanning, malware probing for vulnerabilities and backscatter.

Although a darknet has multiple uses, and can be enhanced with various collectors, sniffers or detectors, its elegance lies in its simplicity and how easy it makes it to see bad traffic on a network in isolation without false positives.

## How it works

The key requirement for a darknet is some unused IP addressing. If you are seeking to monitor public Internet events, this will need to be routable public address space. This address space must not be used and should expect absolutely no traffic whatsoever. This is the fundamental requirement for your darknet.

You may find some advice urging you not to use bogons (unallocated public address space) and Martians (private addresses

| Rank | Country | Events | % |
|---|---|---|---|
| 1 | Russian Federation | 1,125,522 | 18.8 |
| 2 | China | 734,826 | 12.3 |
| 3 | US | 496,350 | 8.3 |
| 4 | Taiwan | 484,444 | 8.1 |
| 5 | UK | 332,993 | 5.6 |
| 6 | Brazil | 265,131 | 4.4 |
| 7 | Ukraine | 211,446 | 3.5 |
| 8 | Belarus | 168,435 | 2.8 |
| 9 | Italy | 146,100 | 2.4 |
| 10 | Romania | 131,977 | 2.2 |

Table 1: Top 10 source countries.

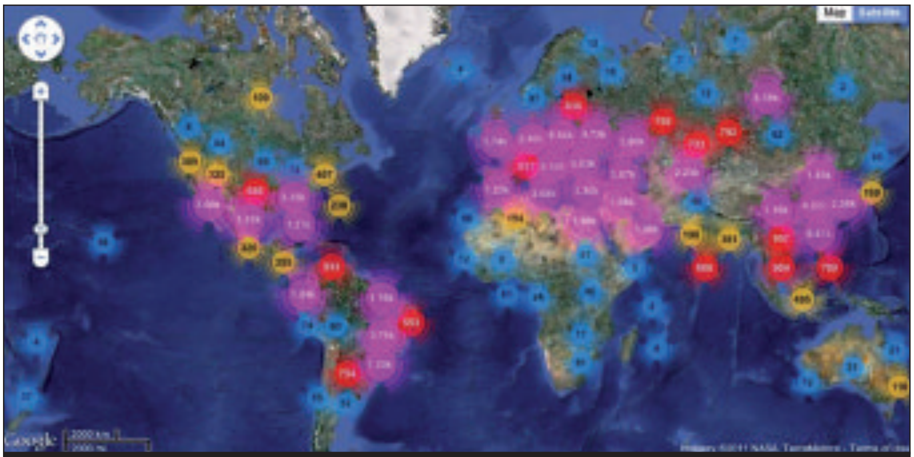


Figure 1: The origins of events hitting the Simwood darknet over a 24-hour period. Source: Simwood eSMS.

reserved for internal use) since they are avoided by many scanners and malware. The argument is that there is no ROI for malware since such space does not include vulnerable hosts. Other advice strongly disagrees with this: the use of such space will undoubtedly lessen the specifically targeted traffic, but experience tells us that most of the traffic the darknet will see is not targeted. The targeted traffic can be captured better using honeypots, and while malware may not seek to spread using Martians, given that malware is increasingly used as a proxy for other intrusion attempts, knowing what it is up to is helpful. In short, running a darknet on your internal network, implicitly therefore on private address space, can be incredibly insightful.

> ***"One guideline you should not deviate from is not to name your darknet. It doesn't exist, remember, so don't put it in your DNS, both forward and reverse"***

How much address space should you use? The easy answer is: as much or as little as you can spare. Analysis of the Simwood darknet shows that every single IP address within it receives traffic, and that holds true right down to a 60-minute window when perhaps one or two of the hundreds of addresses included may miss traffic. It is therefore perfectly acceptable for your darknet to just be a single IP address (/32), or perhaps a few /32s from several different blocks. By having more addresses you benefit from greater breadth of visibility and statistical significance. Certainly, if you're deploying an internal darknet then you can afford to allocate a large block of space and in this scenario a /24 would be an ideal minimum.

It is generally best to keep the darknet space in a VLAN or collision domain separate from other subnets in order to avoid contaminating it with legitimate traffic. That said, you may *want* to put it in the same collision domain as a legitimate system – one you consider vulnerable, for example. You trade the noise of legitimate traffic for the possibility of detecting nefarious traffic at a lower level. For example, you'll have the noise of ARP requests from legitimate equipment, but what if that legitimate equipment is only a single SQL Server that you can filter out? By separating the darknet completely, you'll never see Layer 2 traffic from a new improper host in that subnet; by having the darknet in the same subnet you will. Readers of this publication are sufficiently astute to know exactly what they're seeking to detect, so build your darknet how you choose, just be aware of the consequences of your decisions and stick to the guidance if in doubt.

Arguably, one guideline you should not deviate from is not to name your darknet. It doesn't exist, remember, so don't put it in your DNS, both forward and reverse: darknet.my.net might give the game away!

## Routing

What you do with this address space depends on your topology and certainly every public darknet does it differently. At the very least you will need to route it from an interface on an upstream router – remembering, of course, that none of the router interfaces should be in the darknet.

| Rank | ASN | Name | Country | Events | % |
|---|---|---|---|---|---|
| 1 | 4134 | Chinanet | China | 580,867 | 10.0 |
| 2 | 3462 | Data Communication Business Group | Taiwan | 408,945 | 7.0 |
| 3 | 31724 | Joint Stock Company Svyazist | Russian Federation | 333,646 | 5.7 |
| 4 | 29550 | Simply Transit | UK | 306,285 | 5.3 |
| 5 | 6697 | BELPAK | Belarus | 148,223 | 2.5 |
| 6 | 8402 | Corbina Telecom | Russian Federation | 119,975 | 2.1 |
| 7 | 27699 | DE SAO PAULO S/A – TELESP | Brazil | 92,590 | 1.6 |
| 8 | 44943 | Internet Service Provider 'RamNet' | Russian Federation | 87,228 | 1.5 |
| 9 | 13188 | Ukraine | Ukraine | 68,693 | 1.2 |
| 10 | 31200 | Novotelecom | Russian Federation | 62,564 | 1.1 |

Table 2: Top 10 source networks.

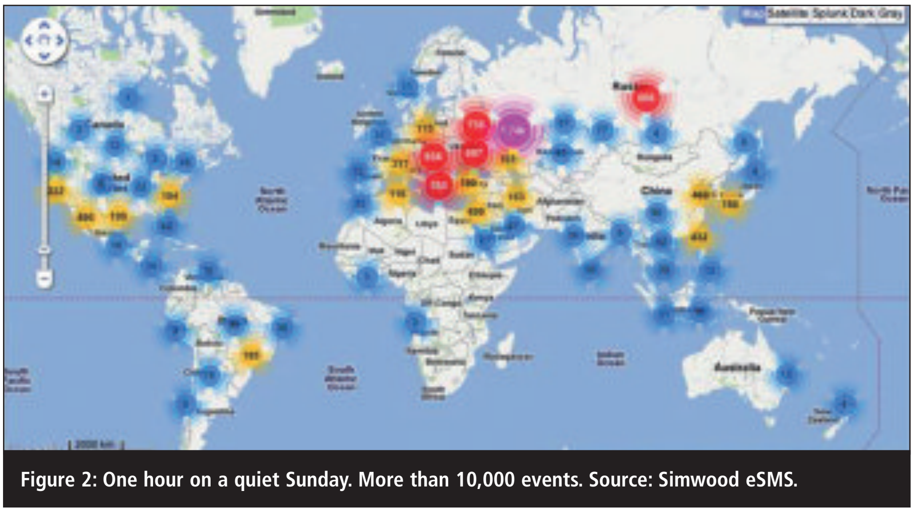


Figure 2: One hour on a quiet Sunday. More than 10,000 events. Source: Simwood eSMS.

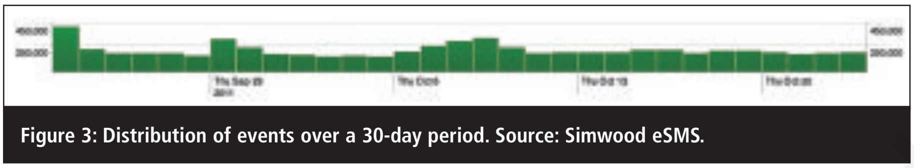


Figure 3: Distribution of events over a 30-day period. Source: Simwood eSMS.

One of the beauties of the rules of routing is that the most specific prefix wins, so it is perfectly feasible for you to have a production /24 on one interface, but statically route a specific /32 within it to another interface. Legitimate traffic goes one way, darknet traffic another, and to the outside world there is no difference. Of course, your router should be configured to protect itself and you probably want to configure it not to pass any outbound packets from the darknet, unless you're intending to proxy SYNs as below.

You are strongly recommended to route to another internal and dedicated router and blackhole the traffic there. As this is simply blackholing, it's perfectly feasible for this router to be a software-based solution or virtual machine. Keep in mind, though, that while this will need to share a subnet with the upstream router it should be outside the darknet space – there are no interfaces in the darknet address space.

It is interesting to note that because darknet traffic is actually routed:

- You can perform flow analysis on the upstream router and/or any switches in between. If you simply blackholed it on the first router this wouldn't be possible.
- You also have a Layer 2 path dedicated to the darknet into which you can insert any manner of sniffer or analyser you choose. The author's preferred approach here is to insert an IPS with firewall rules set to accept but log all traffic.

Another approach is to forgo the second router and instead build a darknet server. It will need two NICs, one for management and one for sniffing. The default route for this box should be the management NIC but, just as with the dual router solution, the upstream router should route traffic to the sniffer NIC, and on the server itself traffic to the darknet should be blackholed.

## A note on SYN proxy

You will be familiar with the fact that establishing a TCP connection requires a three-way handshake. The source sends a SYN, the host server sends a SYN-ACK and the source host responds with an ACK. The TCP socket connection is now established.

When there are no servers in your darknet you are really just seeing and logging SYNs. That is very useful, but with the benefit of real-world results, being able to log other states is also very useful. For example, the real-world results in Figure 2 show a substantial amount of traffic that is both mid-flow (sent assuming a socket which is not established) and backscatter (SYN-ACK in reply to a SYN not sent).

The only way to achieve this without running actual services in the darknet (by definition rendering it not a darknet) is to have something in the path acting as a SYN proxy. Thankfully, a good IPS will do exactly this as it is a key element of protection – it will respond to all SYNs and only when a socket is actually established will it establish a back-to-back socket with the actual server. In this way it protects from SYN floods (unlike a firewall) and only passes through established traffic (unlike NAT). Deploying an IPS in the path will give you this benefit if, of course, you want it. It is irrelevant for UDP, which has no handshake process as it is stateless.

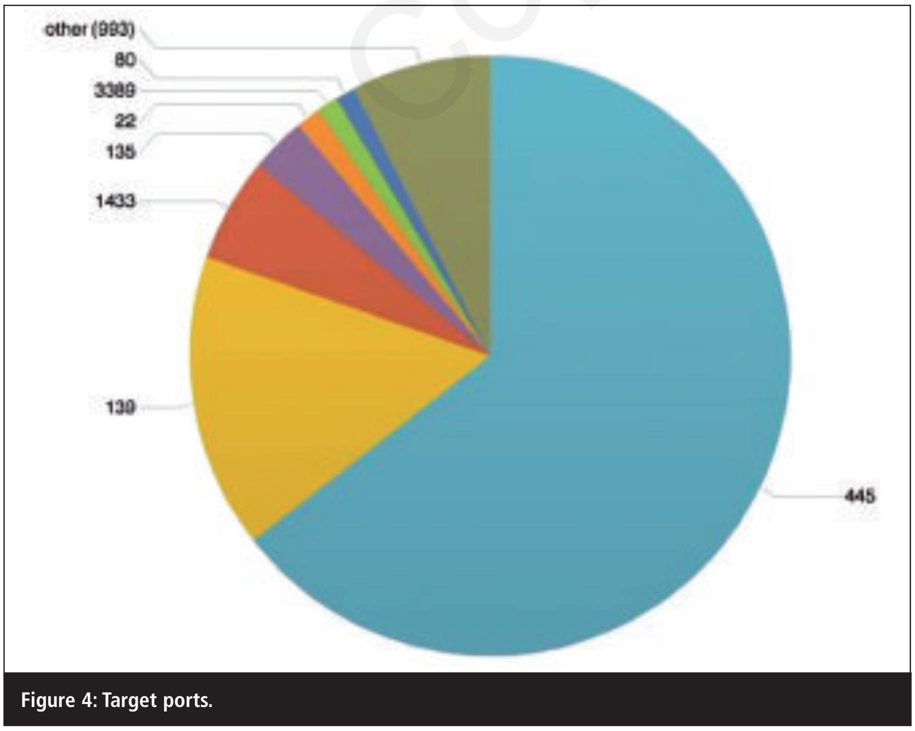


Figure 4: Target ports.

| Rank | Source IP address | Events | % |
|---|---|---|---|
| 1 | 117.41.183.44 | 377,679 | 6.2 |
| 2 | 92.48.118.200 | 303,162 | 5.0 |
| 3 | 61.222.28.50 | 232,667 | 3.8 |
| 4 | 202.57.57.156 | 44,312 | 0.7 |
| 5 | 60.191.222.112 | 37,481 | 0.6 |
| 6 | 80.87.240.41 | 33,165 | 0.5 |
| 7 | 178.22.249.10 | 19,367 | 0.3 |
| 8 | 12.35.109.36 | 17,700 | 0.3 |
| 9 | 202.57.57.143 | 16,255 | 0.3 |
| 10 | 60.191.222.174 | 15,824 | 0.3 |

Table 3: Top 10 source addresses.

| Days old | Quantity | % |
|---|---|---|
| 0-1 | 384,342 | 85.9 |
| 2 | 6,931 | 1.5 |
| 3 | 4,545 | 1.0 |
| 4 | 3,176 | 0.7 |
| 5 | 2,631 | 0.6 |
| 6 | 2,340 | 0.5 |
| 7 | 2,181 | 0.5 |
| 8 | 2,077 | 0.5 |
| 28 | 2,054 | 0.5 |

Table 4: Age of source IP addresses.

## Logging

If you were to follow an often favoured approach of inserting an IPS, you have all the logs you'll ever need. If, instead, you have built a darknet server you will need a means of capturing and logging traffic received on the sniffer NIC. For this there is a number of open source projects, but others who have gone this way have had good results with Argus, tcpdump and IP Filter.

## Analysis

Flow analysis from the first router may well be sufficient for you and you may not wish to analyse the actual logs. If you do, how you do so depends entirely on how they are generated. The above-mentioned open source packages have excellent companion analysis tools. Meanwhile, an IPS or firewall will generate syslog data that can then be analysed by a myriad tools. The analysis that follows is done using map-reduce against syslogs generated by an IPS.

Of course, the novelty of statistical analysis may quickly wear off and it is most likely you will want to answer specific questions. For example, you've heard of a new worm targeting port X and want to find out how much traffic your darknet is receiving. If you're running an internal darknet you'll be very interested in this as well, but more so in which workstation it is originating from so you can take steps to correct it. Similarly, are any workstations or external hosts scanning your network for certain services? You will find endless uses for your darknet once you have it in place and doubtless develop custom tools for answering your own specific questions.

## Real-world results

The following results are from an existing, large Internet-facing darknet, and using map-reduce, the data has been analysed over 30 days. In the analysis you will find reference to 'events.' An 'event' is an attempted TCP connection or a unique UDP source/destination address/port combination per hour. As UDP is stateless it is necessary to group it like this to avoid packet-level analysis but as a result it is possibly understated.

The key take-away figures from this analysis are this:

- Each IP address in the darknet sees on average one event per 109 seconds.
- Every single address in the darknet sees events over any time window down to 60 minutes.

One event per 109 seconds may not sound like much until you consider how many public-facing addresses your organisation may have. It equates to 1,097 per minute for a /21, 585 per second for a /16. In any event, these are all 'events' that should not be happening and any one of them could represent a breach, if successful, against production equipment. Our analysis is based on over 6 million events from more than 447,000 unique source addresses. So let's look at what conclusions we can draw from the tables.

Table 1 is largely self-explanatory. Note number 5, which is entirely represented by a single host on a single network. Otherwise, like much of Western Europe, the UK would not appear in the top 10.

In Table 2, the top 10 ISPs sourcing traffic represent 38% of traffic.

The key point to highlight in Table 3 is that the top 10 addresses account for less than 20% of traffic. It is also worth commenting that while historic analysis has suggested that as much as 60% of nefarious traffic originates from bogons, ISPs are doing a better job of not passing this kind of traffic as this analysis shows just 0.9% of traffic originating from bogons.

Table 4 shows that if you're considering using your darknet to power a block-list, you should think again. The vast majority of source addresses are under a day old. Doubtless though, the larger the darknet is, the older source addresses would be – that is, we'd be seeing the same source address in more places, ergo for longer.

Figure 4 shows that all ports visible are TCP and with the exception of port 22 (SSH) and port 80 (HTTP) they are entirely targeting Windows machines. As Table 5 indicates, your darknet will see protocols outside the big three, including some that don't necessarily exist.

Table 6 is quite interesting and demonstrates the statistical significance

| Rank | Protocol | Events | % |
|---|---|---|---|
| 1 | TCP | 5,943,903 | 97.9 |
| 2 | UDP | 83,501 | 1.4 |
| 3 | ICMP | 40,939 | 0.7 |
| 4 | 67 | 1 | 0 |
| 5 | 31 | 1 | 0 |
| 6 | 253 | 1 | 0 |
| 7 | 218 | 1 | 0 |
| 8 | 153 | 1 | 0 |
| 9 | 131 | 1 | 0 |
| 10 | 122 | 1 | 0 |

Table 5: Top 10 protocols.

| Rank | Target IP addresses | Events | % |
|---|---|---|---|
| 1 | 1 | 343,778 | 76.7 |
| 2 | 2 | 46,418 | 10.4 |
| 3 | 3 | 17,314 | 3.9 |
| 4 | 4 | 9,294 | 2.1 |
| 5 | 5 | 6,158 | 1.4 |
| 6 | 6 | 4,502 | 1.0 |
| 7 | 7 | 3,262 | 0.7 |
| 8 | 8 | 2,590 | 0.6 |
| 9 | 9 | 2,044 | 0.5 |
| 10 | 10 | 1,636 | 0.4 |

Table 6: Target addresses per source IP.

| Rank | Protocol | Events | % |
|---|---|---|---|
| 1 | FWALL: Matched By Firewall | 3,160,621 | 52.1 |
| 2 | NETWK: TCP Connection With Missed Setup | 1,756,239 | 28.9 |
| 3 | DDOSA: SynFlood – Connection To Server That Fails Proxied Handshake | 976,807 | 16.1 |
| 4 | DDOSA: SynFlood – Connection From Malicious Source IP Address | 83,021 | 1.4 |
| 5 | DDOSA: SynFlood – Connection From Client That Fails Proxy Handshake | 65,489 | 1.1 |
| 6 | AAUPV: SunRpc mount operation | 17,981 | 0.3 |
| 7 | EXPLT: MSSQL Resolution Overflow 1 | 4,539 | 0.1 |
| 8 | EXPLT: UDP Frame Length Mismatch With IP Length-UDP Bomb | 1,208 | 0 |
| 9 | AAUPV: IP Frame Reserved Bits or ICMP Frame Unused Bits Set | 1,022 | 0 |
| 10 | NETWK: TCP Frame Contains Bad Sequence Number | 198 | 0 |

Table 7: IPS assessment.

achieved by having a larger darknet. While every address receives traffic, the data in the table show that most source IP addresses hit only one or two darknet addresses. If a darknet is small, you will either not see the traffic at all, or attribute a greater significance to it than is necessarily appropriate. What this analysis fails to show is the few source addresses that target lots of IP addresses; these are of interest as they characterise a different traffic profile that is scanning the network.

Table 7 shows the IPS's view of traffic passing through it. As it is configured to pass, but log, all traffic, the first entry represents 'normal' traffic – or as normal as traffic we shouldn't be getting can be. Item 2 shows traffic that is mid-flow – that is, purports to be for an established TCP socket when one is not established. As mentioned above, NAT would pass this straight through if it hit the right port. Items 3 and 5 show SYN events where the handshake fails – that is, we get a SYN, the IPS SYN-ACKs but there is no response. This is synonymous with a DDoS SYN flood or could be reconnaissance traffic. Item 4 shows traffic from addresses the IPS has taken upon itself to block based on past behaviour – for example, failed handshakes.

## Conclusions

Considering all of the above should lead us to view traffic hitting the darknet as having one of a few distinct profiles:

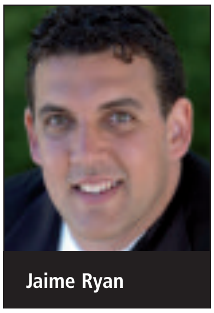
- Approximately 30% is backscatter – that is, replies to traffic you did not originate.
- Less than 20% is from an obviously spoofed source.
- Under 1% (but of significant interest) are sources scanning the network.
- Some 50% are targeting single specific vulnerabilities on 1-3 IP addresses.
- The vast majority are targeting Windows!

Keep in mind, though, this is traffic received on a dark area of the Internet which should receive no traffic at all.

### About the author

*Simon Woodhead is founder and managing director of Simwood eSMS. Simwood is a network service provider that offers a number of security products to help protect service providers and enterprise customers. It is pioneering a new approach to threat mitigation through IP reputation. Woodhead speaks regularly to industry on this topic, and the darknet and honeypots that Simwood operates provide valuable insight into the evolving threat landscape and feed directly into its security solutions. Woodhead can be contacted on simon.woodhead@simwood.com, and Simwood is at www.simwood.com or on Twitter @ simwoodesms.*

# Rethinking the ESB: building a secure bus with an SOA gateway



Jaime Ryan

**Jaime Ryan, Layer 7 Technologies**

**For years the Enterprise Service Bus (ESB) has been seen as a corporate integration and messaging backbone upon which application architectures are built. However, this concept must evolve to meet the requirements of today's corporate landscape, where IT boundaries are blurring, driven by the need to securely integrate with partners, cloud and mobile applications.**

Service Oriented Architecture (SOA) gateways were originally designed to provide edge security between enterprises exchanging data via web service standards such as Simple Object Access

Protocol (SOAP), Representational State Transfer (REST) and XML. They have now been brought inside the firewall to provide a more flexible solution to traditional integration requirements, and with an eye to future integration challenges over the Internet.

## Functional requirements

At its core, the ESB pattern represents a basic set of functional requirements used to integrate applications across an enterprise – mediation, transformation, routing, and so on. Unfortunately, the term has been conflated with vendor-specific product suites and application platforms, often leading enterprises toward insecure, overpriced, code-heavy architectures that ignore many of the pattern's non-functional requirements – security, performance and manageability.

In many cases, SOA gateways are a simpler alternative that meet each of these ESB requirements. They allow a lightweight deployment alternative to the oversized ESB approach and enable enterprises to be more agile and responsive to customer demands at a lower total cost of ownership.

SOA gateways were initially created to solve a different problem – how do you protect your internal applications when interfaces are being exposed to external partners and customers over HTTP and HTTPS protected only by IP firewalls? The solution was to include a hardware-based, application-aware appliance to provide protection from these new threats, specifically around XML-based attacks, message- and field-level data privacy and integrity, and interface abstraction. Specifications around WS-Security, and other web service-only standards such as SOAP and WSDL, were the primary focus.

> ***"SOA gateways treat security as a first-class citizen, by enforcing policies around message privacy, message integrity and access control"***

Once known simply as XML gateways, the name evolved as these interfaces diversified into the various protocols and message formats potentially present in modern service-oriented architecture. When companies began reusing these services internally, SOA gateways and appliances moved and evolved with them, providing the same basic functionality for internal app-to-app communication in various form factors. And that's when IT architects began to recognise the overlap between SOA gateways and ESB, and explore more sophisticated internal use cases.

## Modern attributes

Modern SOA gateways include all the attributes of a traditional ESB: standards-based endpoint abstraction, broad data and transport mediation capabilities, and dynamic, intelligent message routing. Traditional ESBs approach these requirements either through adapters or code. The first approach often results in 'death by adapter', trying to deal with hundreds of obscure, incompatible, additional-cost components that then have to be wired together uniquely for each point-to-point connection. The second approach results in application logic being written in the ESB itself, introducing tightly-coupled interfaces, long services engagements and serious security concerns.

SOA gateways, on the other hand, treat security as a first-class citizen, by enforcing policies around message privacy, message integrity and access control. They utilise a consistent configuration-driven interface to avoid the need for hordes of programmers and the potential introduction of additional security vulnerabilities. And they provide the scalability and manageability one would expect from enterprise-class architecture components.

This broad set of capabilities opens the door for many diverse use cases commonly deployed on an ESB:

- Any-to-any transformation functionality allows integration of legacy mainframe applications with modern service interfaces such as SOAP, REST and JSON.
- Application-awareness and comprehensive message inspection enable dynamic routing, SLA management and protocol bridging decisions based on transaction content.
- Integration with databases and flat-file formats allows message enrichment and custom data mappings.
- Connectivity to (or inclusion of) identity stores allows identity federation and credential token mapping.
- Runtime access to latency and throughput information allows business-level reporting and analytics.

The list goes on and on, but they all boil down to the same simple principle: an SOA gateway should quickly and securely get messages to the appropriate target, in the appropriate format, using the appropriate protocol.

## New requirements

Providing these functions while focusing on security and performance allows businesses to respond to new requirements for application integration, essentially expanding the traditional enterprise architecture beyond the four walls of the datacentre. This adds four important new capabilities to the ESB paradigm:

- **Cross-departmental:** connecting siloed divisions within the same enterprise, perhaps across geographical boundaries. Related applications running in separate environments can now communicate securely for cross-divisional integration.
- **B2B:** integrating with partners for enhanced processing capability and production of composite applications. These business-to-business interactions allow monetisation of internal applications or value-added mash-ups of varied functionality.
- **Cloud:** enabling hybrid cloud infrastructures through application replication to public platforms or integration with SaaS providers. High traffic volumes can now 'burst' to the cloud during industry-specific calendar events such as the tax season in April, the retail rush in November and December or new product introductions following industry tradeshows.
- **Mobile:** opening previously internal data and applications to mobile platforms for remote workforce initiatives or developer-based expansion of

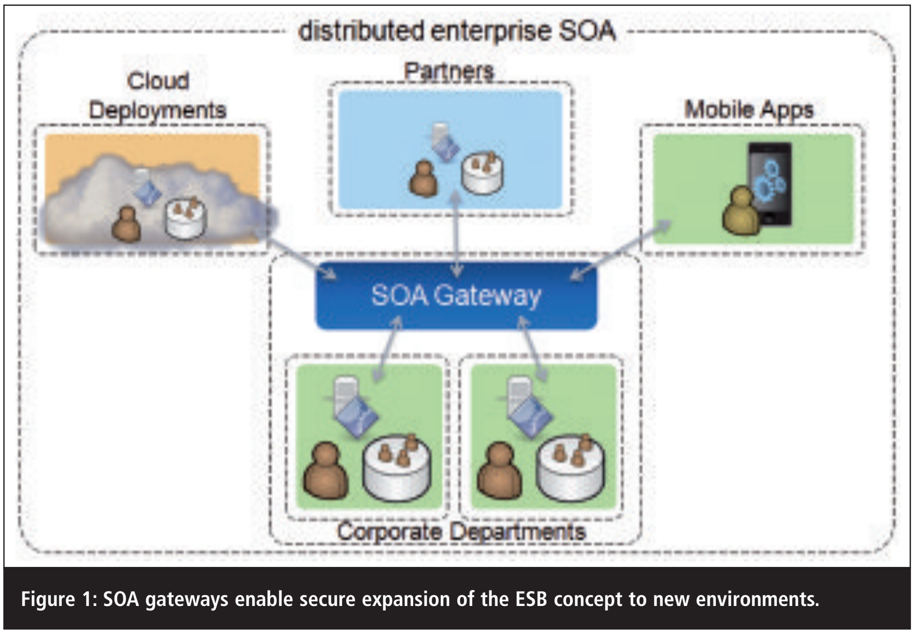


Figure 1: SOA gateways enable secure expansion of the ESB concept to new environments.

business reach. Service APIs can be exposed to apps built by internal developers or made public for home-grown development of apps for new platforms.

In each of these cases, potentially sensitive data is being exposed to a distributed group of new consumers, raising concerns about access control, privacy and network latency. SOA gateways solve these issues and enable an expansion of the traditional ESB role to fit modern IT requirements.

## Different implementations

Though the ESB replacement concept is the same for most SOA gateways, vendor implementations can be very different. Each vendor can provide a laundry list of its supported protocols and message formats. Each will take a unique approach to policy configuration and extensibility. Each will support slightly different encryption algorithms and access control mechanisms. Each will have various potential deployment methods and clustering strategies.

When considering an SOA gateway in an ESB scenario, the goal is to match up each of these capabilities with your particular requirements. Consider which of your current applications could be made more valuable by providing a robust, standards-based interface. Consider what data you'd like to expose, to whom and in what format. Then go through the various options and choose wisely. If you want to provide an OAuth-protected REST interface to a mainframe application accessed using Message Queue (MQ), then make sure the necessary formats and protocols are supported by your SOA gateway vendor. Support for these common ESB functions is what will probably make your decision much easier.

- In terms of protocols, what do you need beyond basic HTTP(S)?
- Are messaging protocols – MQ, Java Message Service (JMS), Enhanced Messaging Service (EMS) – a requirement? If so, do you use a particular flavour (vendor-specific JMS), and is it supported?
- Do you need file-based protocols such as FTP and NFS? If so, which secure versions and/or security options (FTPS, SFTP, NFSv4)?
- Do you need support for incoming (POP3, IMAP) or outgoing (SMTP) email?
- In terms of message formats, are XML-based options (XML, SOAP) sufficient?
- Do you need flat-file support? B2B formats such as EDI? Mainframe formats like COBOL Copybooks? Modern web-based formats such as JSON?
- What tools will you use to map between these formats?
- How is policy created on the gateway, using what interfaces?
- Is there a logical GUI that makes it clear what actions are taking place?
- Is there a Command Line Interface (CLI)?
- How about a services-based interface for programmatic access to gateway functions?
- On the security side, what incoming and outgoing credential types need to be supported, and is there an easy, standards-based way of mapping between them? What authentication and authorisation servers are supported? Does the gateway both support modern cryptographic algorithms and protect against common threats?

Requirements for security certifications or specialised hardware are common in many environments. Do you need PCI DSS compliance for handling credit card data, Security Technical Implementation Guide (STIG) vulnerability testing for a DoD environment or Common Criteria and FIPS certification for your secure computational platforms? Do you have a requirement for hardware-based storage of cryptographic keys? Considerations around placement of an ESB and integration into existing architectures carry over to SOA gateways acting in the same capacity. Some enterprises require a hardware gateway form factor when dealing with deployments that touch the DMZ, some deploy all internal applications on virtualisation software and others need their internal architecture to be replicable in a public cloud environment. These form factor choices will be of primary importance to your network and operations teams, along with clustering methodologies and integration with existing logging, monitoring and reporting. Auditing is of particular importance when dealing with secure transactions or industry compliance issues.

## Limitations

Understanding the limitations of SOA gateways is equally important. They're powerful and flexible, but are by no means a panacea. For example, though they generally provide workflow and logical message-processing capabilities, they are not Business Process Execution Language (BPEL) business orchestration engines that can manage all of your human interaction and long-running processes.

Though they can process batches of messages, they are neither a managed file transfer platform nor an Extract Transform Load (ETL) data warehousing tool. And though there is definitely some feature overlap with Web Application Firewalls (WAFs), SOA gateways don't generally fulfil all of those requirements; neither do WAFs come anywhere close to parity on non-HTML traffic.

The exact deployment model for an SOA gateway in an ESB role depends on the feature comparison exercise we just went through, and generally falls into one of three categories.

If these 'lightweight ESBs' meet all of your corporate requirements for application integration and SOA deployment, they can easily stand alone and fulfil the ESB pattern.

If, on the other hand, an existing ESB is meeting most of your application integration needs, then an SOA gateway can be deployed as a complement to provide value as an on- and off-ramp to that ESB. This 'ESB gateway' use case focuses on the gateway's strengths around security, high-performance transformation and edge-based protocol mediation.

***"SOA gateways combine the capabilities of a traditional ESB with security, agility and simplicity"***

The third option is most common in large enterprises that have grown through mergers and acquisitions and have a heterogeneous corporate IT landscape. In these cases, the SOA gateway can perform all of the ESB functions for those divisions without an existing infrastructure and can act as a bridge between other, more-entrenched technologies in the rest of the enterprise. It even enables extension of this secure architecture to applications deployed in public or private cloud environments. This 'Federated ESB' use case takes advantage of the true agility and flexibility of SOA gateways without requiring a rip-and-replace implementation.

SOA gateways combine the capabilities of a traditional ESB with security, agility and simplicity. They transform the archaic code-based challenge of application integration into a modern configuration and networking problem. They can be implemented as hardware, as VMs or in the cloud. They are Internet-ready, giving enterprises the immediate ability to support the extended enterprise, which increasingly encompasses partners, cloud and mobile.

In a modern corporate culture that demands we do more with less, they give you the capacity to respond to customer demands and provide new, secure interfaces to the data and applications that drive your business. SOA gateways truly are the cure for the common ESB.

## About the author

*Jaime Ryan is the partner solutions architect for Layer 7 Technologies, and has been building secure integration architectures as a developer, architect, consultant and author for the past 15 years. He is based in San Diego. Layer 7 Technologies helps enterprises secure and govern interactions between their organisation and the services they use in the cloud, across the Internet, and out to mobile devices. Layer 7 gives enterprises the ability to control identity, data security, SLA and visibility requirements for sharing application data and functionality across organisational boundaries.*

# A secure model for building e-learning systems

**Shadi R Masadeh, Nedal Turab, Farhan Obisat, Faculty of Information Technology, Applied Science University, Isra University, Arab Academy (AABFS), Amman, Jordan**

**E-learning involves the use of the Internet as a communications medium between instructors and students who are separated by physical distance.[1] Wireless networks have become very common in this environment, often replacing wired networks, in order to provide mobile access to educational systems and the Internet for students and staff. But these networks must be secured.**

In this article, we're proposing a model for a secure e-learning system designed to be implemented by computer centres at universities. It would provide faculties with a new learning approach that could be developed at later stages to provide a secured portal for educators to access instructional and exam materials. In addition, the computer centre is able to use a wireless network to connect to faculties and other organisations outside the university. This model employs a secured network that utilises the latest security technologies, including firewalls, OpenVPN and PGP.

A firewall is an appliance or software used to protect a network from unauthorised access from outside the network. It allows legitimate access to the network according to a set of predefined rules and policies. Firewalls are either packet filters or network layer devices: packet filter firewalls allow packets that match a set of established rules; network

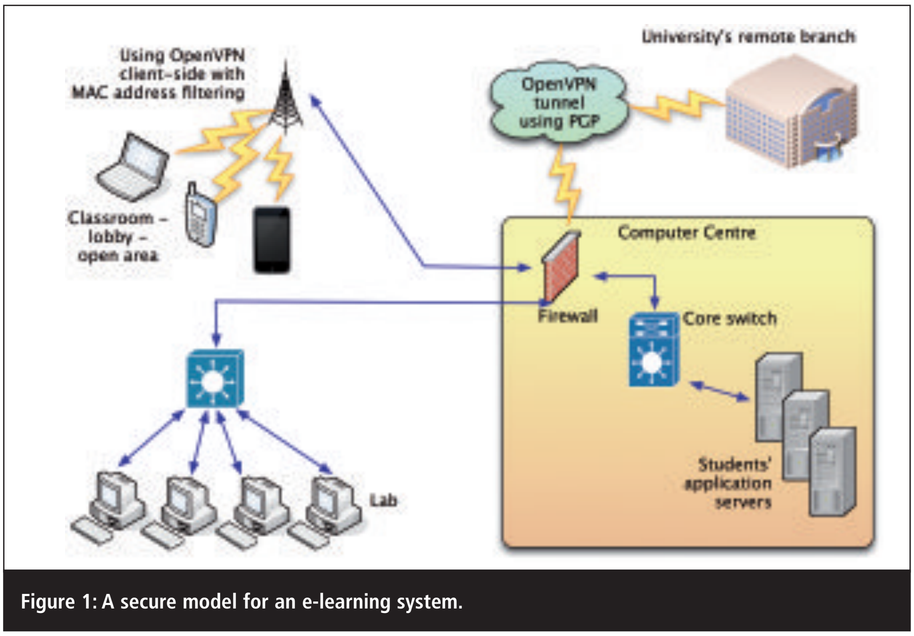

Using OpenVPN client-side with MAC address filtering
University's remote branch
OpenVPN tunnel using PGP
Classroom - lobby - open area
Computer Centre
Firewall
Core switch
Students' application servers
Lab

Figure 1: A secure model for an e-learning system.

layer firewalls generally fall into two subcategories – stateful and stateless. The former use state information to provide a context about active sessions in order to allow or deny packets. This context may include UDP or TCP port connections, source and destination IP addresses, and the lifetime of the connection.

Open Virtual Private Network (OpenVPN) is a free and open source software application that is used for site-to-site connection. It uses encryption (static key-based, using a range of key sizes, or certificate-based public key encryption), and the authentication features of Secure Socket Layer/Transport Layer Security (SSL/TLS).

Pretty Good Privacy (PGP) is a data encryption/decryption and authentication protocol and is often used for digital signing, and encrypting and decrypting texts, emails and files to enhance the security of email communications.[2]

## Related work

Many researchers have studied the security issues and countermeasures connected with e-learning systems from different points of view. E Kritzinger *et al* identified the key security issues and recommended using four pillars that should be put in place to enhance overall security.[3] These pillars are: ensuring e-learning security; creating e-learning security policies and procedures; the implementation of e-learning security countermeasures; and monitoring the e-learning security countermeasures. A Jalal *et al* described the security features of e-learning authentication and recommended the use of web applications.[4] They used the SKiP method to provide similar features to SSL. And they recommended using the RIPEMD-160 hash function, to provide security and authentication. Najwa Hayaati *et al* discussed how information security management is essential to ensure the security of the e-learning environment.[5] They suggested that the combination of ISM and information security technology can provide a more secure e-learning system. Farhan Obisat *et al* investigated the factors that influence the adoption of e-learning systems in Jordan, as well as surveying which aspects have not been tested yet in the domain literature.[6]

## The proposed system

A wireless system provides academic staff, employees and students with remote access to the faculty students' database files, the Internet and online e-learning courses. The main security issues that must be assured are the standard 'CIA' triad of Confidentiality, Integrity and Availability of the system data and resources. Therefore, the new security system must satisfy the following factors:

- Checking the e-learning application environment for any server-level vulnerabilities.
- Ensuring that roles and privilege levels are respected.
- Evaluating the use of cryptography for data at rest and in transit.
- Validating user input for malicious data that could result in loss of integrity or confidentiality of data.
- Anti-automation and end-user protection measures.

The proposed system is shown in Figure 1 and is made of the following components:

- All the PCs are connected to the access switches which in turn are connected to the core switch.
- All wireless devices (laptops, PDAs and tablet PCs) are connected to the access point that is connected to the core switch via access switches.
- Students' application servers in the computer centre are connected to the core switch and are considered as a highly secured area.
- The core switch and the entire network are protected by a firewall.
- The university is connected to the remote site using OpenVPN and PGP.

All the wireless connections to the access points are secured using OpenVPN on the client side with MAC address filtering in the access point, with encryption using Temporary Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). To ensure message integrity, a strong data integrity algorithm – the Michael Message Integrity Check (MIC) – is applied. The students' applications servers employ Active Directory to provide central authentication for the students, academic staff and wireless stations. In addition, Remote Authentication Dial-In User Service (Radius) can be used for this purpose.

The core switch is a very high speed, multi-layer device that provides switching, routing and intrusion prevention and is protected by external firewall services. The core switch connects all the switches distributed around the university buildings (access switches). Routing is necessary to provide inter-VLAN connections. The VLANs are used to separate different networks belonging to different faculties and departments for greater security and more efficient performance.

All the traffic to or from the university is controlled by the perimeter firewall to allow only legitimate access according to the predefined rules and security policy of the university.

The connection from the university to any remote site or branch is secured using OpenVPN and PGP.

IPSec VPNs are either too expensive or difficult to use. IPSec contains too many options to be configured. OpenVPN avoids the complexity of IPSec by using SSL/TLS protocols. OpenVPN has all the security features of VPN/SSL, which include: remote access; site-to-site remote access VPNs with load balancing; and wifi security. OpenVPN supports two authentication modes:[7]

- **Static key** – using a pre-shared static key that is generated and shared between both entities (peers) before the tunnel is started. This static key contains four independent keys: Hash-based Message Authentication Code (HMAC) send key; HMAC receive key; encrypt key; and decrypt key. Both peers use the same HMAC keys and the same encrypt/decrypt keys.
- **SSL/TLS** – the protocols are used with digital certificates for authentication and key exchange. Each side presents its own digital certificate. If the authentication succeeds, encryption/decryption and HMAC keys are randomly generated and exchanged over the SSL/TLS connection. Both sides have different HAMC and encrypt/decrypt keys.

PGP is a presentation layer protocol that is used to secure email messages. It supports many encryption algorithms, such as 3DES, AES, Blowfish, CAST and IDEA. PGP can operate using only one key for encryption and decryption. A key size of 128 bits is considered sufficient, but this mode of operation has a problem with shared key exchange.[8]

Another mode of operation is public key (asymmetric) encryption, where two keys are used: one public and the other private. At the sending end, the message is encrypted using the receiver's public key. The receiver decrypts using the private key. PGP uses a hybrid public key encryption method, incorporating both symmetric and asymmetric encryption methods as shown in Figure 2.

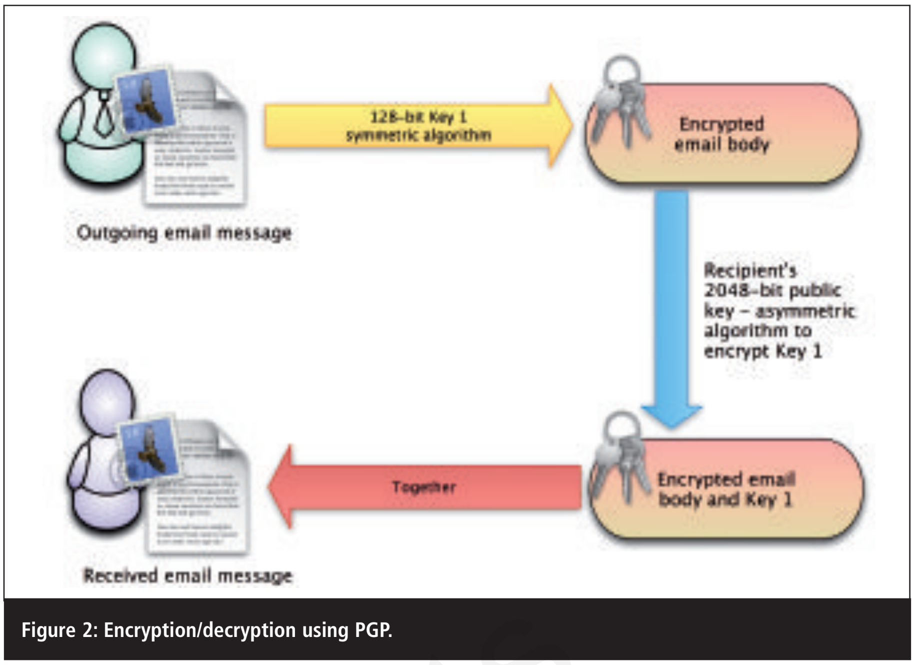


Figure 2: Encryption/decryption using PGP.

The combination of OpenVPN and PGP is as follows: use OpenVPN with SSL/TLS mode for tunnelling and second-layer encryption (using digital certificates and HMAC keys). PGP is used for encryption/decryption and key distribution using public and private key pairs using RSA.

## Conclusions

E-learning can involve a range of technologies, including CD-ROM, networks, intranets and the Internet. It can include text, video, audio, animation and virtual environments. It can be a very rich learning experience, providing a very high level of training. And it can incorporate many elements that make learning more interesting.

The aim of the proposed e-learning model outlined here is to give teachers and students the ability to gain secure mobile access to course materials and administrative tools, enabling the teaching staff to perform administrative functions from any location, manage coursework and collaborate more efficiently with colleagues. It will also allow them to distribute coursework or to provide online access to course materials, and to provide constant access to critical information via wireless networks. By accommodating the latest security technologies – such as firewalls, PGP and OpenVPN – this proposed model will help to enhance the security for the e-learning course content and the education process.

### Acknowledgement

The authors are grateful to the Applied Science Private University, Amman, Jordan, for the partial financial support granted to this research project (Grant no. DRGS-2011-34).

### About the authors

*Shadi R Masadeh received a BSc degree in CS and CIS from Philadelphia University, Jordan 2000 and an MSc in IT from*

*Continued on page 20...*

*Continued from page 19...*

*Al-Neelien University, Sudan 2003. His PhD in CIS is from the Arab Academy for Banking and Financial Sciences, Jordan. His research interests including e-learning security and WLAN security. He is currently an assistant professor in the CNS department at the Applied Science University, Jordan.*

*Nidal Turab received a BSc degree in communication engineering from the University of Garounis, Benghazi, Libya 1992 and an MSc in telecommunication engineering from the University of Jordan, Amman in 1996. His PhD in computer science is from the Polytechnic University of Bucharest, 2008. His research interests include WLAN security. He is an assistant professor at Isra University.*

*Farhan Obisat received a BSc degree in CS from Mu'tah University, Jordan and MSc and PhD degrees in CIS from the Arab Academy for Banking and Financial Sciences, Jordan. His research interests include building e-learning systems. He is an assistant professor at the Arab Academy for Banking and Financial Sciences.*

## References

1. Cooper. 'Anatomy of an On-Line Course'. THE Journal, 26, 49. Retrieved May 25, 1999 from INFOTRAC, SearchBank (Article# A53929573).
2. 'Pretty Good Privacy'. Wikipedia. Accessed Dec 2011. http://en.wikipedia.org/wiki/Pretty_Good_Privacy.
3. Kritzinger, E; von Solms, SH. 'E-learning: Incorporating Information Security Governance'. 2006. Accessed Dec 2011. www.informingscience.org/proceedings/InSITE2006/IISITKrit157.pdf.
4. A Jalal and Mian Ahmad Zeb. 'Security Enhancement for E-Learning Portal'. IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.3, 2008.
5. Najwa Hayaati, Mohd Alwi, Ip-Shing Fan. 'E-Learning and Information Security Management'. International Journal of Digital Society (IJDS), Volume 1, Issue 2, 2010.
6. Dr Farhan M Obisat; Dr Ghalib Saleh Saraireh. 'Factors affecting e-learning in the Middle East: Jordan school case study'. 2010.
7. Hosner, Charlie. 'OpenVPN and the SSL VPN Revolution'. SANS Institute, Aug 2004. Accessed Dec 2011. http://www.sans.org/reading_room/whitepapers/vpns/openvpn-ssl-vpn-revolution_1459.
8. Zhao, Zhong. 'PGP (Pretty Good Privacy) Introduction'. http://web.cs.dal.ca/~tt/ECMM6010/presentations/PGP.pdf.

## Resources

- IEEE802.11i – Local and metropolitan area networks. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
- 'Securing Wi-Fi Wireless Networks with today's technologies'. Wi-Fi Alliance, 6 Feb 2003. Accessed Dec 2011. ftp://ftp.im.must.edu.tw/download/wtlin/TCFST-80211/WPA/Whitepaper_Wi-Fi_Networks2-6-03.pdf.
- Landau, S. 'Data Encryption Standard (DES)'. Notices of the AMS, 2000.
- Wong, Jenne. 'Performance Investigation of Secure 802.11 Wireless LANS: Raising the security bar to which level?'. 2003. Accessed Dec 2011. www.cosc.canterbury.ac.nz/research/reports/MastTheses/2003/mast_0301.pdf.
- McCrea, F; Gay, RK; Bacon, R. 'Riding the big waves: A white paper on B2B e-learning industry'. Thomas Weisel Partners LLC, 2000.
- Urdan, TA; Weggen, CC. 'Corporate e-learning: exploring a new frontier'. WR Hambrecht, 2000.
- Tim L Wentling; Consuelo Waight; James Gallaher; Jason La Fleur; Christine Wang; Alaina Kanfer. 'E-learning – A Review of Literature'. Knowledge and Learning Systems Group, University of Illinois at Urbana-Champaign, 2000.
- Howell, SL. 'E-Learning and Paper Testing: Why the Gap?' Educause Quarterly, Number 4, 2003.
- Ashwin, A. 'E-Learning in Business and Economics'. In Teaching Business Education 14-19, Jephcote & Abbott (eds), David Fulton. 2005.
- Blum, K. 'Gender Differences in Asynchronous Learning in Higher Education: Learning Styles, Participation Barriers and Communication Patterns.' Journal of Asynchronous Learning Networks, 1999.

# EVENTS CALENDAR

January 30–February 4 2012
**SANS Monterey 2012**
Monterey, US
www.sans.org/info/85574

13–18 February 2012
**SANS Phoenix 2012**
Phoenix, US
www.sans.org/info/83779

20–23 February 2012
**HITBGSEC (Hack in the Box Global IT Security Conference)**
Mumbai, India
http://conference.hitb.org

27 February–March 2, 2012
**RSA Conference 2012**
San Francisco, California, US
www.rsaconference.com/events.htm

5–17 March 2012
**SANS Secure Singapore 2012**
Singapore
www.sans.org/info/83994

7–9 March 2012
**Military Cyber Security**
Washington DC, US
www.militarycybersecurity.com

12–13 March 2012
**European Smart Grid Cyber Security – Priority One, securing the digital infrastructure**
London, UK
www.smi-online.co.uk/2012smartgridprivacy25.asp

14–16 March 2012
**Black Hat Europe**
Amsterdam, The Netherlands
www.blackhat.com/html/bh-eu-12/bh-eu-12-home.html

24–26 April 2012
**Infosecurity Europe**
London UK
www.infosec.co.uk