ENTERPRISE IT SECURITY

VOL.1 NO.2 ISSUE 2/2011(2)

Hardening a Network Router

Take Pain Out of a Value Chain

Is scanning of computer networks dangerous?

PCI DSS at a Glance

PCI Audit – The Road To Compliance

NETWORK SECURITY

ENTERPRISE IT SECURITY

Publisher:
Paweł Marciniak

Editor in Chief:
Ewa Dudzic
ewa.dudzic@enterpriseitsecuritymag.com

Managing Editor:
Kinga Połyńczuk
kinga.polynczuk@software.com.pl

Art Director:
Marcin Ziółkowski
Graphics & Design Studio
www.gdstudio.pl

Production Director:
Andrzej Kuca
andrzej.kuca@software.com.pl

Marketing:
Kinga Połyńczuk
kinga.polynczuk@software.com.pl

Editorial Office:
Software Press
www.enterpriseitsecuritymag.com

Enterprise Advisory Board:
Rishi Narang, CEH www.wtfuzz.com

Beta Testers:
Aby Rao, Manu Zacharia, Jose L. Herrera

Proofreaders:
Aby Rao, Manu Zacharia, Jose L. Herrera

Publisher:
Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1

Phone: 1 917 338 3631

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.

DISCLAIMER!
The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

This time we have decided to focus on two topics: Network Security and PCI Auditing. Both of them are related to the latest events. By analyzing PlayStation Network breach, we can consider the ways of preventing this kind of data leaks in the future.

„Take Pain Out of The Value Chain" written by Simon Walker shows the importance of providing security. This article can be found on pages 6-9.

After familiarizing with this article, you can move to pages 10-12 where Dave Naples describes good practices of hardening a router.

Dhanjajay Garg shows some techniques of scanning and probing a network on pages 14-17.
On pages 18-21 a scanning tool – Angry IP Scanner – is described by its creator, Anton Keks. The next article, written by Rebecca Wynn, presents features of security auditing tool, Nipper.

The main ideas of PCI Audit and PCI DSS Standard are shown in two articles: „PCI Audit – The Road to Compliance" written by Ben Ben Aderet, and „PCI DSS at a Glance" by Dimitris Ergazakis.

We also highly recommend reading the other articles. I hope that you will find the magazine's content useful and spend some pleasant time reading Enterprise IT Security magazine.

Enjoy reading!
Best regards,
Kinga Połyńczuk & Enterprise IT Security
Magazine Team

ENTERPRISE IT SECURITY

Content issue 02/2011

NETWORK SECURITY

06 Take Pain Out of The Value Chain
Simon Walker
[…] the recent PlayStation Network incident shows, a critical part of security is the level of strategic focus on security. In an ideal world, security would be designed into products – but all too often this doesn't happen. In part, this is a result of the fact that considerations such as time-to-market are often deemed more important. However, the reality is that poor risk management can often significantly subtract from the value of an offering to customers. Hence, it's just bad business to skimp on security risk assessment.

10 Hardening a Network Router
Dave Naples
Since a router is traditionally installed at the perimeter of a network, it plays an important role in security. The best implementation of a router with regard to security is to use it simply as a single component of aa larger defense-in-depth security structure. This implementation allows a router to focus on what it was designed to do – route packets – rather than on security-specific concerns, such as intrusion detection/prevention, or as a firewall.

14 Networking Reconnaissance – Probing & Scanning
Dhananjay Garg
Identifying the IP address space of the target network is the first step. After gaining access to an IP address space, gathering details for a successful penetration into the target network is the next logical step. To do so, a penetrator performs network scanning to check the level of security that is implemented on the target network. Both attackers and security consultants usually use ICMP, TCP and UDP scanning to gain useful insights about the version of network services running on the host machine.

18 Is scanning of computer networks dangerous?
Anton Keks
Thanks to the recent activity of mass-media on the subject (that popularized the wrong term for a cracker – a 'hacker'), nowadays every educated person more or less understands the reasons and goals that stand behind malicious cracking: curiosity, stealing of information, making damage, showing self-importance to the world, etc. But why do administrators need to scan their own networks?

22 Network Infrastructure Parser – Nipper – An Introduction
Rebecca Wynn
Short for Network Infrastructure Parser, Nipper is an open source network devices security auditing tool. One benefit of being open source is that it's free. Previously known as Cisco Parse, Nipper Command Line Tool isn't flashy or pretty, but it is very functional, easy to install, easy to use, and it does exactly what it says it will do. It works with many different types of network devices, not just Cisco.

PCI AUDIT?

26 PCI Audit – The Road To Compliance
Ben Ben Aderet
When facing with a compliancy project and organization may sometimes find itself at a lost. The lost feeling might be intensified when getting unclear deadlines and requirements by the local acquiring banks. However, not all challenges for meeting compliancy are external.

30 **PCI DSS at a Glance**
Dimitris Ergazakis
[...] the Payment Card Industry Data Security Standard (PCI DSS) was developed providing a detailed set of security best practices. PCI DSS is neither just a standard nor a regulation per se, even though there are state laws in the USA that are already in effect to force components of the PCI DSS into law. Essentially, PCI DSS is a contractual agreement between card associations, the merchant banks, and the merchants.

ATTACKS & RECOVERY

36 **WikiLeaks, Compliance and Global Competitiveness – Reasons to Review Your DLP Strategy**
John Dasher
While data breaches can't be eliminated completely, organizations can greatly reduce the risks associated with confidential data leaving their organizations. Organizations are looking for a way to monitor the movement of sensitive information and stop users from emailing sensitive documents, printing, copying information to removable devices or posting via instant messages. All these things (and many more) can be controlled and monitored using Data Loss Prevention (DLP) solutions.

38 **Virtual Crime in The Real World**
Sian Haynes, Peter Burden
However, the digital world isn't as safe as it first seems. The alluring world may provide comfort and flexibility to the user's needs but it is just as dangerous if not more so than the real world today. The dangers in the real world seem threatening because they can endanger you physically, mentally and in the worst scenario can terminate your life. Although cybercrime does not come in the form of bullets or knives it can be just as deadly when your life is still at risk.

CLOUD COMPUTING

40 **Examining Aspects of Cloud Security and Risk**
Jon Shende
These days when we hear the term "Cloud Computing" there is an understanding that we are speaking about a flexible, cost-effective, and proven delivery platform that is being utilized or will be utilized to provide IT services over the Internet. As end users or researchers of all things "Cloud" we expect to hear about how quickly processes, applications, and services can be provisioned, deployed and scaled, as needed, regardless of users' physical locations.

42 **Cloud Computing Offers Hope For All**
Roger Strukhoff
The term springs up from the traditional view of the Internet as a cloud in representations of IT architectures and infrastructures. With cloud computing, applications and processing power seemingly fall from the heavens (i.e., the cloud), and data is stored there as well.
This point of view makes people nervous, from IT management to the C-Suite. How secure is this information? What guarantee do I have that my data is not being shared with others?

TECH CORNER

44 **Mobile Phones Operating Systems Forensics**
Peter Burden
According to several technical reviews the top 5 operating systems on the market at the moment (ranging from 1 – 5) are: Linux & Windows, RIM, Apple, Android, and Symbian. Now I know what the latest technical reviews say, I can now examine the mobile phones myself and generate my own review. The mobile phone operating systems that I have selected to be examined include: RIM, Apple iOS and Android, this will allow me to perform a case study on which one is the most secure dependant on how easy it was to access the information and how the operating system is set out.

Take Pain Out of the Value Chain

From a young age, we're told that it is important to learn from our mistakes – although it is even better to learn from other peoples' ones. Yet, week after week we see headlines about data loss and hacking incidents – are enterprises just careless, or is there a systematic failure at play? The Verizon 2010 Data Breach Investigations report highlighted a number of key steps organisations should take in order to reduce their risk of data compromise, but often don't. In outline, these included the elimination of unnecessary data, ensuring essential controls were in place (and verifying that this was so), testing and reviewing web applications, auditing user activity, filtering outbound traffic, and actively monitoring event logs. All sensible stuff, as far as it goes. The report goes on to emphasise that the majority of reported data losses were the result of external agents, although often aided, directly or indirectly, by insiders or business partners.

However, reports of this nature can be misleading; as the recent PlayStation Network incident shows, a critical part of security is the level of strategic focus on security. In an ideal world, security would be designed into products – but all too often this doesn't happen. In part, this is a result of the fact that considerations such as time-to-market are often deemed more important. However, the reality is that poor risk management can often significantly subtract from the value of an offering to customers. Hence, it's just bad business to skimp on security risk assessment.

It is not possible to protect an enterprise against every eventuality – but unless the real implications of security failures are realised, then management run the risk of making decisions based on very imperfect information. If security professionals are unable to convincingly articulate this, there is a problem. Security professionals may need to look beyond the confines of their profession to find the right tools and approaches to make headway in educating their organisation's senior leadership. As Einstein asserted, a good definition of madness is doing the same thing but expecting different results.

The PlayStation Network

Sony's PlayStation Network service has a clear customer proposition. Its prime attractions rest in the open architecture, a ready supply of downloadable games to purchase, and the ability to interact with other gamers. Ease of access to services tends to mean quick authentication and seamless payment, which means that user details, including card details are stored somewhere easily accessible. Where you have such data stored, you have something worth stealing. Secondly, if you're releasing a product for the young and technology literate, which needs to be globally accessible, you're also mapping quite neatly onto the demographic who are often keenest to attempt breaking technology. The presence of a ready-made community means that there is a shared interest in learning about any holes in the defences – both for legitimate purposes and for nefarious ones.

None of these are particularly obscure facts, so what can have gone wrong?

Sony's value chain

Initial suggestions from Sony that the incident was orchestrated by hacktivist group Anonymous have since been dismissed by the group. Anonymous were quick to issue a denial of this accusation (and notably were themselves apparently the victim of an "insider" attack a few days later. This seems to have been an attempt by Sony to excuse the incident and is in any case an irrelevance: the root causes of the incident were endemic, not a result of the actions of external influences.

The 'value chain' is a model that describes the activities of a firm within a specific industry, and consists of primary activities, and support activities. In Sony's case the former would include research, development, manufacture, marketing and sales, and after-sales service. Support activities would traditionally include organisational infrastructure elements – the internal IT, HR, and other functions which span the primary productive ones. Each element has costs, and adds (or subtracts) value from the end result.

Poor risk management sucks value out of products

There is a hoary management maxim that the things that are measured are the things that matter. There can be a temptation to excise those functions deemed as cost centres, rather than adding value. Does penetration testing generate revenue? However, this risks ignoring the downstream effects. If, for example, non-functional requirements don't include security, because it's "too difficult", or there is insufficient appreciation of the threat environment for a product, because senior leadership don't want to hear about it, then developers are on a losing wicket.

Ineffective risk assessment and treatment up front therefore devalues downstream activity. Developers may have been pushed to "deliver" a product with little or no built-in security, either because that is how their task was defined, or because they simply lacked the training. If delivery was time pressured, then there may have been little scope for robust security testing.

With what result? Developers may get stick for neglecting holes in code, IT Operations are dressed down for not patching – but if no-one makes it clear that's important, why should they bother?

Black swans are still swans

CloudNine Communications was one of Britain's earliest internet service providers. It had been in business for six years. It was voted ISP Review ISP of the Year 2000 and was listed in the Top 10 rated UK ISP's) from October 2000 through to January 2002. Its core offerings were email services and software, web site hosting and it was one of the first SaaS providers. Formed in 1996, it had approximately 30,000 business customers.

In January 2002, it was subject to a Distributed Denial of Service attack. A denial-of-service attack causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computer resources of the target. CloudNine had recognised the risk of a DDOS attack, but had deemed the cost of countermeasures to be prohibitive, relative to the risk. It was therefore the first known instance of a company being "hacked out of business".

As a consequence, the management were forced to sell the business to a competitor, Zetnet. Of course, we now recognise DDOS attacks as a real feature of the "bad hat's" arsenal. But even in 2002, it was not an unknown phenomenon.

It would be easy to dismiss incidents as being simply rooted in incompetence - this is simplistic and not very helpful. While it may not be possible to prepare for every eventuality, it is possible to plan to handle them – this is surely the point of effective risk management.

Some useful economics

Externalities can be defined as costs and benefits which are not naturally captured in the pricing of the activities to which they attach. This may also pertain where the costs and benefits of an activity are felt by different parties, resulting in a misalignment of incentives, as argued by Anderson and Moore (Anderson 2006). This results in the oversupply of goods and services where there are negative externalities, such as pollution, or undersupply, where there are positive externalities, as would be argued to be the case where information security is concerned.

There are a number of problems with trying to base business cases on the data in data breach surveys, however well researched these are. Firstly, they are only ever partial – it is artificial to classify the only data loss events being those that are detected. This would exclude all those instances of data leaving an organisation in people's heads, on print media, and so on. In this sense, they are never going to be as comprehensive a data set as, for example, the data available to insurance actuaries. When calculating whether what price will render a life insurance policy profitable, they have access to literally hundreds of year's worth of verifiable data regarding life expectancy. The richness of this data set lends itself to a high degree of predictive accuracy.

This highlights a second problem regarding the usefulness of available data. It is only retrospective – no-one has data on the loss events that are going to happen. Moreover, forecasting is difficult on a number of levels. The rate of technological change means that there is a constant stream of zero-day attack opportunities. As seems to have been the case in the PSN hack, a further key variable is technology within the specific context of an organisation – if your IT team aren't encouraged to patch, enterprise security will always be behind the curve of the technically possible, for instance. Moreover, sophisticated attacks may use a number of different vulnerabilities in combination. A great example of this is the Stuxnet attack, which exploited not only blind spots in anti-virus, but also lack of physical control on ports, and a low level of technical security awareness among the target user population.

Accounting for garbage

It is into the gap created by these variables that an effective enterprise risk function fits. But as we have seen, there are practical limits to the credibility of taking an "actuarial" approach to building the case for information security .It may therefore be

Table 1.

Tier	Description	Content
0	"Usual costs"	Direct and indirect costs which would be associated with an activity using a conventional accounting approach, including both revenue and capital expenditure.
1	"Hidden costs"	Additional costs usually found in overheads/general accounts. These would include regulatory management systems, and monitoring costs, both revenue and capital in nature.
2	"Liability costs"	These costs would not be incurred in the present period in a conventional accounting sense. These would emerge dependent on other events, for example changes in legislation, and their likelihood can only be estimated. Examples might include fines and other regulatory costs.
3	"Less tangible benefits"	Costs and benefits that are likely to arise from improved security management. These costs and benefits could include the effect of goodwill arising from a project; changed attitudes of suppliers, customers, and employees.
4	"Environmentally focussed benefits"	Costs that would be incurred if a security focussed approach was taken in a project can be estimated. Costs to ensure that a project has a net positive effect on information security could be estimated. These values would be informed by estimates of the industry and social impacts and alternatives.

useful to draw lessons, where possible, from innovative models used in other areas where externalities are a significant factor. One good example would be waste management – at an abstract level, it displays many commonalities with information security. For example:

Neither is generally thought of as a revenue generating activity

Both are display classic characteristics of public goods, with free rider problems and undersupply unless provided by a centralised authority (e.g. municipal governments for waste management and driven by central government legislation for information security)

In both cases, failure to supply has negative effects, but these are difficult to accurately quantify in advance

Comparative data exists on consequence, but is incomplete and its applicability would be open to challenge. For example, ineffective sewerage resulted in cholera outbreaks in 19th century London, but the only way of modelling the probability and effect of a major sanitary failing, other things being equal, in 21st century would be theoretical.

The State of Florida uses a full cost accounting approach for its solid waste management. Full Cost Accounting is a systematic approach for identifying, summing, and reporting the actual costs of an activity. It takes into account past and future outlays, overhead (oversight and support services) costs, and operating costs. In this respect, it can be seen to overcome the objection to ROSI that it is unrealistic to fixate on capital expenditure over revenue expenditure when considering information security expenditure.

Bebbington and Thomson (Bebbington 1996) lay out a series of layers of cost to be considered in a Full Cost Accounting model. These are laid out, in a form adapted for information security, in the table below (Table 1).

A cost/benefit model that excludes Tier 4 would not be a full accounting model – rather only “fuller” than ISACA’s ROSI. Working through the tiers systematically would enable an organisation to produce a holistic picture of the costs and benefits of its information security expenditure.

The Association for Chartered Certified Accountants (ACCA) is an international professional certification body for accountants, with over 140,000 members around the world. The ACCA (Bebbington 2001) define a number of steps that would be required to deploy this model in an environmental context. Adapted for information security, these would be:

1. Define the cost objective- for example, a new project or process. This is critical – in particular the end-to-end extent of an activity – failure to do this would result in incomplete consideration of costs and benefits.
2. Specify the scope of analysis – this serves to determine what sub-set of all possible externalities are to be considered. Moreover, this would be important in identifying the various layers of externality – these might include, for example, regulatory impacts. It would not be useful to try to include all conceivable externalities (e.g. impact on competitors); rather, only those externalities which can be directly identified with a particular project or activity should be included.
3. Identify and measure external impact – this requires an explicit link to be made between the cost objective and the externalities which arise from it. This requires the gathering of data on both the cost objective itself and the identified externalities. The first set can largely be drawn from boundary transactions – i.e. where there is a consumption or movement of resources resulting in a monetary transaction. With regard to externalities, there is a less exact and more variegated set of data which could be drawn on – for example, secondary data sets. In the UK these include reported costs of incidents from the latest PWC/BERR reports and historical fines under the Data Protection Act from the Information Commissioners Office. Although this information set has obvious drawbacks, it has the benefit of being publicly available.
4. Cost external impact (e.g. monetisation of the externalities). In many respects, this is the most problematic stage – for example, it would be dependent on a convincing scope having been identified earlier in the process. As was identified through the survey, this often the area regarded as most subjective and subject to challenge, as it will tend to be “story dependent”.

This therefore produces a theoretical model for a full cost analysis would be a summation of costs from Tier 0 to Tier 4. However, this still leaves the problem of the uncertainty of assertions about probability, and the relative balance between costs and benefits. This rather suggests the need to apply both prudence, and an adaptive management approach. In other words, the calculations should articulate clear assumptions about facts (e.g. the economic climate, which has an impact on the overall level of criminality), and should be expressed in a flexible way (i.e. “best case”, “medium” and “worst case”). This would allow conscious decisions about confidence levels, and would provide a clear rationale for revisions if specific assumptions are proven incorrect. Furthermore, it would allow for improved confidence in decisions over time, both from a psychological perspective and by providing internal benchmarks which can be refined over time. This is something that ROSI notably does not do, as a specific application of it will only ever be “generally in line with events” or “not aligned”. Turning this into a model for determining the return on a particular activity would therefore produce:

$$\text{Return} = \frac{(A + B + C) + (D + E + (F \times \text{probability of } F))}{(D + E + (F \times \text{probability of } F))}$$

Where:
A is the direct benefit of the activity/project (as per Tier 0)
B is less tangible benefits (as per Tier 3)
C is positive network effects (as per Tier 4)
D is Tier 0 costs
E is Tier 1 costs
F is the cost of contingent liabilities (as per Tier 2).

Haste to market: repent at leisure

There is no easy answer for the formulation of business cases for information security. That’s not to say that information doesn’t make sense from an economic point-of-view – it just means that, as a profession, we need to think more broadly about how we structure the approach , and think creatively about how to apply lessons from elsewhere. It took accountants (probably the third oldest profession) several thousand years to come up with double-entry book keeping and then agree on uniform standards. Hopefully, information security can manage to reach this point somewhat sooner – and security professionals should apply some pressure on industry bodies, the ISF for instance, to make it so.

Once a consumer product is in the hands of the end user, it's too late. Sony took the decision to take the PlayStation network down upon discovering the breach. As an organisation, Sony have a buffer whereby they can afford to take the network down for days, even weeks with manageable revenue loss. Is this a luxury most businesses could afford? Or have you a robust business continuity plan in place?

Is there enough time given to allow thorough system testing? Many companies tend to skim on this part by releasing 'beta' code and allowing their customers to report bugs. What about penetration testing? Whilst this omitting may be convenient and cheap, it's not always the right thing to do.

Lastly, consider the long term impact of security failures – if PSN was not secure, what other Sony products, services, or infrastructure are now being inspected with interest ? And what happens when all those consumers come to making their next technology purchasing decision? Were time-to-market considerations really worth driving a suboptimal product to market quickly, compared to the cost and time or managing the risk in the first place?

Getting it right – it's all sell, sell, sell

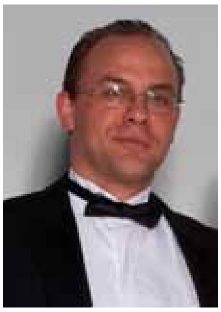
Getting security risk assessment of products should be simple – even though as we know, in real life it may not be the case. Part of this may be because security professionals are more used to "doing" than "selling" – a sweeping generalization of course, but one to which there is more than a grain of truth. In an ideal world we would work towards embedding sound security assessment practice; in reality we need to make sound security practices something people want to buy in to. Some key points are:

Sell a security as part of the value of the product – after all, there are plenty of case studies to point to now

Sell the idea to the organisation's project management function – after all, getting security right early saves pain, delay, and expense later on

Sell yourself. Be approachable. Do the right people know how to contact you ? Make your findings an easy read. Whether you like it or not, the most important people who read your report may not be very technically minded – so if they can't understand what you're telling them, that's a big problem.

None of this should give cause to security professionals to feel smug – if organisations feel that we are merely an occasionally necessary evil, then we have a problem. We do well to remember that classic triad of people, process, and technology; although the first may be the most intractable, it should not be ignored or sidelined in favour of emphasis on technology. After all, it is the mentality of an organisation's leadership which is one of the biggest influencing factors on organisational behaviour. It's all about the value add – and part of that is delivering security at speed, at the right time, and articulated in a manner meaningful to people at the top table.



SIMON WALKER

Simon Walker has over eleven year's experience in security and technology risk assessment, across the financial sector, government, and a number of other sectors, and was formerly a member of the UK Government's CESG Listed Advisor Scheme (CLAS). He is currently completing an MBA, and is Chief Strategy Officer of Quantainia, a boutique security consulting firm (www.quantainia.com)

Bibliography

- Bebbington, J. G., R.; Hibbitt, C.; Kirk, E. (2001) Full Cost Accounting: An Agenda for Action
- Bebbington, J. T., I. (1996). Business Conceptions of Sustainability and the Implications for Accountancy. London, Association of Chartered Certified Accountants.
- Reuters, "How CloudNine Wound Up In Hell", 02/01/02 Retrieved from 15/09/2010 from http://www.wired.com/techbiz/media/news/2002/02/50171

Hardening a Network Router

A router functions at the OSI (Open Systems Interconnection) network layer to direct the flow of network packets using headers and routing tables to determine the direction each packet should be sent. Specific protocols are used for communications and for selecting the best path between hosts or networks. The basic functions of a router include packet forwarding, sharing routing information with adjacent routers, packet filtering, network address translation (NAT), and encrypting or decrypting packets as in the case of virtual private networks (VPNs).

Since a router is traditionally installed at the perimeter of a network, it plays an important role in security. The best implementation of a router with regard to security is to use it simply as a single component of a larger defense-in-depth security structure. This implementation allows a router to focus on what it was designed to do – route packets – rather than on security-specific concerns, such as intrusion detection/prevention, or as a firewall. However, in very small networks, this is not always possible. Sometimes routers must perform multiple functions, including that of a single perimeter security solution in addition to routing packets. A router's ability to be flexible enough to fill this need is an excellent example of the value routers can bring to an organization. In certain environments, a router may be effective as a perimeter security device on its own. This requires a properly configured router to provide a solid foundation of perimeter defense. This scenario makes it even more important to apply defense-in-depth principles behind the router, such as NAT and host-based solutions. The practice of implementing a single line of network perimeter defense is an undesirable practice since an attacker only needs to exploit one defense layer before an entire network becomes vulnerable to compromise.

Why should we harden routers?

The strategy behind hardening routers is to eliminate one source of vulnerabilities on the network, thereby reducing overall risk. By closing unneeded ports on the router, vulnerabilities are removed because if an attacker cannot connect to a device, that device cannot be attacked. In addition, removing vulnerable services prevents an attacker from exploiting certain weaknesses since they are no longer available. Using a router as a filtering device employing NAT or using access control lists (ACLs) to filter external scans and effectively hiding internal hosts will greatly impact the effort on reducing visible hosts to potential attackers.

Statistics show that attackers still rely heavily on misconfigurations and functional vulnerabilities when targeting network infrastructure equipment. Vulnerabilities in open network services, such as a service with a memory corruption vulnerability, tend to be the primary entry targets for attackers. It is highly recommended to manually disable all services that are not being used on a router.

Router attacks and vulnerabilities

Similar to typical computer systems, routers contain a number of common innate vulnerabilities, many of which depend on the specific configuration. Conceptually, a router is created with three separate operational planes – the management plane, the control plane, and the data plane. Administration, configuration, and the state of the router are organized by the management plane. The control plane ensures that monitoring, routing table updates, and the dynamic operations of the router are properly handled. The data plane controls the forwarding of packets onto the attached network(s). To maintain a secure router, threats to each of these planes must be considered because exploitation of any one plane can easily lead to all planes becoming compromised.

Attacks on routers may include unauthorized access, session hijacking, denial of service (DoS), eavesdropping, as well as information theft. Several techniques of attack used against routers are password guessing, routing protocol attacks, IP fragmentation attacks, and attacks against specific vulnerable services. In the case of password guessing, most networking devices come with a preconfigured default username and password. It is up to the administrator to change the default settings to use more secure credentials. Many Cisco routers use the default username and password of *admin/admin*. It would not take an attacker long to break this username/password combination, especially since these credentials are well-known and highly published.

Methods of hardening routers

Security best practices suggest disabling any unnecessary services. Many services that use UDP are not frequently used for legitimate purposes on modern networks, but they are commonly used to launch denial of service (DoS) as well as other attacks. Cisco recommends disabling the TCP and UDP small services, which include *echo, discard*, *daytime*, and *chargen*. These services are located on TCP/UDP ports 7, 9, 13, and 19 respectively. All of these services are now outdated. They were once used in UNIX environments to provide information such as date and time, connectivity testing, and to generate a stream of characters. If left open, hackers can use these services to their advantage. For example, the chargen service (TCP or UDP port 19) can permit an attacker to send a flood of traffic directed at this port, effectively causing a Fraggle DoS attack. The below commands can be used to disable these services:

```
Router(config)#no service tcp-small-servers
Router(config)#no service udp-small-servers
```

The Finger service (TCP port 79) is also an old UNIX application that was used to determine who was logged into a device. Today, the same information can be provided from many other sources, diminishing the need for Finger. When the Finger command is used on a Cisco router, the router responds with the output from the show users command. This output could allow an attacker to see the current users logged onto the router as well as being able to acquire valid user identification credentials. The Finger service had a programming error in an earlier version of the service that facilitated the infection of the password cracking Internet worm of 1988. The Finger protocol can also reveal detailed user information such as login names, phone numbers, last login, etc. Probably the most famous cracker to date, Kevin Mitnick, also used Finger as one of his targeted services when he attacked Shimomura's network in 1994. The best option is to disable the Finger service using the command below:

```
Router(config)#no ip finger
```

Telnet is considered insecure because all communications conducted under it are completed in clear text. Numerous attacks are known to capture the traffic of a Telnet session with a packet sniffer, permitting the attacker to view the information contained in the session. The captured information may include such sensitive data as the device configuration, passwords, usernames, IP addresses, etc. Telnet should be disabled and the more secure service – the Secure Shell (SSH) protocol – should be used in its place. SSH operates on TCP port 22 and provides strong authentication and encryption of the session.

```
Router(config)#crypto key generate rsa general-keys modulus
   [360-4096]
Router(config)#ip ssh time-out 60
Router(config)#ip ssh authentication-retries 3
Router(config)#ip ssh version 2
Router(config)#line vty 0 15
Router(config-line)#transport input ssh
Router(config-line)#login local
```

The HTTP server protocol is supported on all newer Cisco IOS (Internetwork Operating System) releases to provide a Web interface for device administration. A very common router vulnerability is present when the HTTP server service is enabled. Attackers have discovered numerous methods of exploiting it to gain unauthorized access. Several of the weaknesses in the HTTP server include passwords being revealed in plain-text, and the requirement that administrators log on at full (level 15) privilege. Another HTTP exploit involves an attacker taking advantage of the HTTP authentication vulnerability. This exploit can allow a remote user to gain full administrative access to a router. Careful consideration should be given to the use of HTTP on a router and, unless it is used in conjunction with a secure authentication method such as AAA (AAA refers to Authentication, Authorization, and Accounting), it should be disabled. An additional HTTP hardening measure includes configuring access control lists to limit HTTP router management access to specific hosts.

Cisco routers and many other network hosts utilize the Network Time Protocol (NTP) to synchronize all the time-of-day clocks with a remote time server or other reliable time source. It is good practice to synchronize the time on all network devices down to the second if possible. Network time stamps assist administrators with recognizing problems such as lost connections, network crashes, buffer overflows, and missing packets. NTP also helps with network forensics investigations since time synchronization can affect log file accuracy, auditing precision, network fault diagnosis and recovery, as well as file time stamps. If NTP is employed on a network, the router can be configured with specific trusted addresses for the time source. Additionally, NTP authentication should be used whenever possible. However, if NTP is not needed on a network, it is important to disable this service to remove the vulnerabilities it presents.

The Cisco Discovery Protocol (CDP) is a data link layer protocol used to discover information about neighboring Cisco devices. CDP can show the Cisco IOS software version, network layer addresses, and the platform type of any neighboring Cisco devices. This information is not encrypted and CDP does not offer any mechanisms for authentication between devices. A malicious attacker can connect a rogue router or switch to a network and obtain information about the network devices. In addition, a router using an IOS version earlier than 12.2(3) may crash or reboot if battered with a flood of CDP frames by an attacker. CDP is enabled by default on Cisco routers and can be disabled globally or on specific interfaces. The recommended practice is to disable CDP to prevent router information from being transmitted to untrusted hosts.

If the Simple Network Management Protocol (SNMP) is needed on a router, the more secure SNMP version 2 should be used. Version 2 provides support for MD 5 (Message Digest 5) authentication rather than the clear text community string as used in version 1. If version 1 must be used due to compatibility restrictions, administrators should ensure the default "public" and "private" community strings are changed to community strings that are much more difficult to guess. Standard IP access lists can also be implemented to limit the router's SNMP access to specific network hosts.

Routing protocol security

Routing and routing protocols can raise several important security concerns. Routing security should be considered a high priority to prevent unauthorized access to network resources, to protect critical data, and to prevent network failures and service interruptions. Unprotected routers make painless targets for skilled attackers that can falsify routing update packets and corrupt the route tables. This attack can allow the attacker to reroute network traffic in any direction desired. The best way to prevent this type of attack is to implement only static routes. This is a very effective solution for smaller networks. However, static routes can create an administrative nightmare for administrators managing medium to large networks.

The use of routing protocols that can implement authentication is a better solution for larger networks. An important rule when employing dynamic routing protocols such as Routing Information Protocol (RIP; versions 1 and 2), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), Border Gateway Protocol (BGP), and Enhanced Interior Gateway Protocol (EIGRP) is to configure the protocols to ensure they are implemented in a secure fashion. These routing protocols can become an easily exploited security hole if due care is not taken. For example, several routing protocols include numbering schemes (such as an autonomous system [AS] number or area number) providing several specific details of the network that are transmitted in plain-text and easily captured by an attacker. To help prevent this security issue, administrators can implement route authentication. The process of route authentication includes the use of a secret keyword that is hashed with MD 5 and is used with all routing updates. The routing protocols that support this feature include RIPv2, OSPF, EIGRP, IS-IS, and BGP. Another method of securing dynamic routing protocols is to prevent tampering of the routing tables. This can be done by blocking updates from untrusted networks. To accomplish this task on a Cisco router, the command `passive interface [interface]` can be applied to the appropriate interface configuration.

AutoSecure

To automatically secure a router with the recommended security settings, an administrator can use the Cisco AutoSecure feature. When using full mode, AutoSecure will automatically apply more than 80 commands to a router to configure additional security features. AutoSecure will lock down the management plane services, the data plane services, firewall services, login functions, NTP, SSH, and TCP services. This feature may be useful for easy security implementation on a Cisco router, but it is only available on Cisco IOS Release 12.3(8)T and above. The AutoSecure feature can be run in full mode, noninteractive mode, or only for select services. Full mode will prompt the administrator with questions concerning how to secure the router. Noninteractive mode allows the router to automatically apply the recommended commands to the configuration. Another option is to specify the management plane, data plane, NTP service, etc. to apply the proper commands to the router in order to secure only the desired service or plane.

Conclusion

Many variables contribute to a router's vulnerability to threats, including outdated software, misconfigurations, unnecessary/unused ports and services left enabled, weak or default passwords, and insecure protocols. Network and security administrators may not always be aware of the best practices to follow or which ports, services, software, etc. are the most secure. By following the approach of this article, administrators should gain a better understanding of how to increase the security of a network router. This logical approach to remediating vulnerabilities can help secure an organization's network and reduce its overall IT risk. The general approach outlined in this article apply equally well to a number of network hosts. For instance, disabling or removing unnecessary services, using the latest software, and maintaining updates is applicable to virtually all hosts. The devices on a network that may benefit from this include additional network routers and switches (from Cisco or any other vendors), servers, virtual machines, and workstations.

DAVE NAPLES

Dave is a senior network security analyst for a major printing company in Houston, Texas. Dave has twenty years of professional experience in the information technology field, working for such organizations as the U.S. Navy, NASA, United Airlines, AT&T, and the University of Texas. Dave's past positions include working as a network operations manager, network engineer, and network analyst. He holds an M.S. degree in Information Assurance, a B.S. in Information Technology, as well as the CCNA and CCNA Security certifications.

References

- Antoine, V., Bongiorni, R., Borza, A., Bosmajian, P., Deusterhaus, D., Dransfield, M., … Ziring, N. (2005, December 15). Router security configuration guide. Fort Meade, MD: National Security Agency.
- Basta, A., & Halton, W. (2008). *Computer security and penetration testing*. Boston: Course Technology.
- Bhaiji, Y. (2008). *Network security technologies and solutions (CCIE professional development series).* Indianapolis, IN: Cisco Press
- Cisco Systems (2008). Cisco guide to harden Cisco IOS devices. Retrieved from http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml
- Cole, E. (2010). Security 401: SANS security essentials bootcamp style. Bethesda, MD: The SANS Institute.
- Deal, R. A. (2005). *Cisco router firewall security.* Indianapolis, IN: Cisco Press.
- EC Council (2010). *Computer forensics: Investigating network intrusions and cybercrime*. Clifton Park, NY: Cengage Learning.
- EC Council (2011). *Penetration testing: Security analysis*. Clifton Park, NY: Cengage Learning.
- Hucaby, D., McQuerry, S., & Whitaker, A. (2010). *Cisco router configuration handbook* (2nd ed.). Indianapolis, IN: Cisco Press.
- Lewis, W. (2006). *Switching basics and intermediate routing: CCNA 3 companion guide*. Indianapolis, IN: Cisco Press.
- Lindner, F. (2009, July 26). *Cisco IOS router exploitation: A map of the problem space*. Retrieved from http://www.recurity-labs.com
- Northcutt, S., Zeltser, L., Winters, S., Frederick, K. K., & Ritchey, R. W. (2003). Inside network perimeter security. Indianapolis, IN: New Riders.
- Roland, J. F. (2004). *CCSP self-study: Securing Cisco IOS networks* (SECUR). Indianapolis, IN: Cisco Press.
- Smith, P. G. (2005). *Linux network security.* Hingham, MA: Charles River Media.
- Stevens, W. R. (1994). *TCP/IP illustrated: The protocols*. Reading, MA: Addison Wesley Longman.
- Whitaker, A, & Newman, D. P. (2006). *Penetration testing and network defense.* Indianapolis, IN: Cisco Press.

SECURE NINJA
THE PATH OF THE DIGITAL WARRIOR BEGINS HERE
Save $500 on select Boot Camps.
Offer ends June 30, 2011.
Mention Code: NinjaQuest

Networking Reconnaissance

Probing & Scanning

The contents of this article are only meant for education, information and reference purposes. The author or editor won't be liable to any person for the consequences suffered as a result of any action taken or not taken on the basis of the contents of this article.

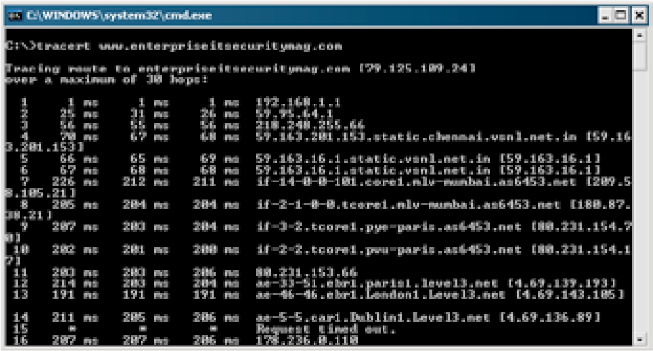
Identifying the IP address space of the target network is the first step. After gaining access to an IP address space, gathering details for a successful penetration into the target network is the next logical step. To do so, a penetrator performs network scanning to check the level of security that is implemented on the target network. Both attackers and security consultants usually use ICMP, TCP and UDP scanning to gain useful insights about the version of network services running on the host machine.

ICMP Scanning

Internet Control Message Protocol (ICMP) is the de factor protocol that is used to relay data transfer errors over networks. Attackers often use ICMP error messages to produce a road map of the network. A lot of information about the target machine can be determined using the Type and Code values found in ICMP error messages. The following table of error messages is useful:

Type	Name	Importance
3	Destination Unreachable	Network / Host / Protocol / Port unreachable, host precedence violation, precedence cutoff and communication administratively prohibited are all types of this error msg.
8	Echo Request	To determine whether or not the host is alive and the amount of time taken by a packet to travel from source to the destination.
13	Time Stamp	To determine the target host system time information.
17	Address Mask Request	To determine the subnet mask used by the target system.

Traceroute



```
C:\>tracert www.enterpriseitsecuritymag.com

Tracing route to enterpriseitsecuritymag.com [79.125.109.24]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  192.168.1.1
  2    25 ms    31 ms    26 ms  59.95.64.1
  3    56 ms    55 ms    56 ms  218.248.255.66
  4    70 ms    67 ms    68 ms  59.163.201.153.static.chennai.vsnl.net.in [59.16
3.201.153]
  5    66 ms    65 ms    69 ms  59.163.16.1.static.vsnl.net.in [59.163.16.1]
  6    67 ms    68 ms    68 ms  59.163.16.1.static.vsnl.net.in [59.163.16.1]
  7   226 ms   212 ms   211 ms  if-14-0-0-101.core1.mlv-mumbai.as6453.net [209.5
8.105.21]
  8   205 ms   204 ms   204 ms  if-2-1-0-0.tcore1.mlv-mumbai.as6453.net [180.87.
38.21]
  9   207 ms   203 ms   204 ms  if-3-2.tcore1.pye-paris.as6453.net [80.231.154.7
0]
 10   202 ms   201 ms   200 ms  if-2-2.tcore1.pvu-paris.as6453.net [80.231.154.1
7]
 11   203 ms   203 ms   206 ms  80.231.153.66
 12   214 ms   203 ms   204 ms  ae-33-51.ebr1.paris1.level3.net [4.69.139.193]
 13   191 ms   191 ms   191 ms  ae-46-46.ebr1.London1.Level3.net [4.69.143.105]

 14   211 ms   205 ms   206 ms  ae-5-5.car1.Dublin1.Level3.net [4.69.136.89]
 15     *        *        *     Request timed out.
 16   207 ms   207 ms   206 ms  178.236.0.110
```

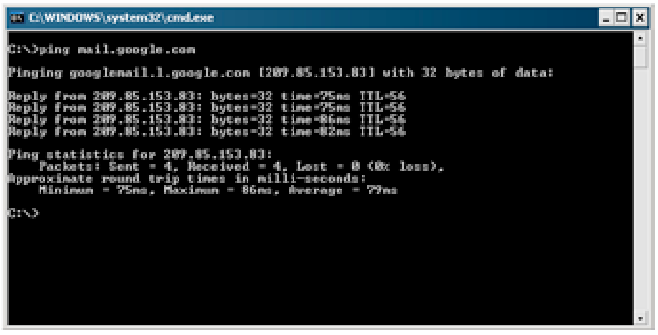
The traceroute command can be executed using the Windows based command prompt tool. The network path between the source and destination systems of each router crossed can be mapped using traceroute. A request timed out or request failed in a traceroute query is because of filtering by the router or due to a slow link speed. The command used here is: tracert www.enterpriseitsecuritymag.com

Other good third party tools for trace routing:

- Visual Traceroute (URL: www.visualroute.visualware.com)
- 3D Traceroute (URL: www.d3tr.de)

Ping

The ping tool sends an ICMP request to calculate the round trip time by storing the time at which it sends the echo request in the data portion of the ICMP message. It subtracts this value from the current time when the reply is returned. The command used



```
C:\>ping mail.google.com

Pinging googlemail.l.google.com [209.85.153.83] with 32 bytes of data:

Reply from 209.85.153.83: bytes=32 time=75ms TTL=56
Reply from 209.85.153.83: bytes=32 time=75ms TTL=56
Reply from 209.85.153.83: bytes=32 time=86ms TTL=56
Reply from 209.85.153.83: bytes=32 time=82ms TTL=56

Ping statistics for 209.85.153.83:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 75ms, Maximum = 86ms, Average = 79ms

C:\>
```

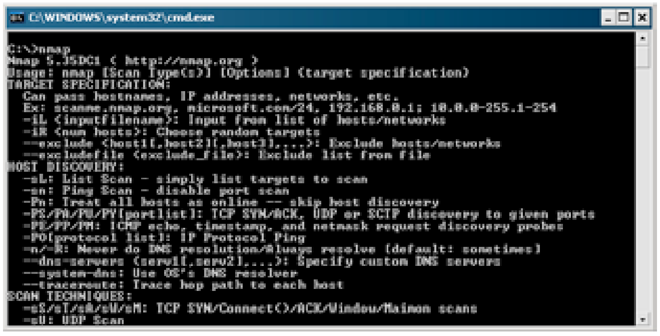
here is: ping mail.google.com. IP address can also be used instead of web address.

Other good third party tools for ping sweeping:

- WS_Ping ProPack (URL: www.whatsupgold.com/products/tools/ws_ping-propack)
- Send ICMP Nasty Garbage (SING) (URL: http://sourceforge.net/projects/sing)

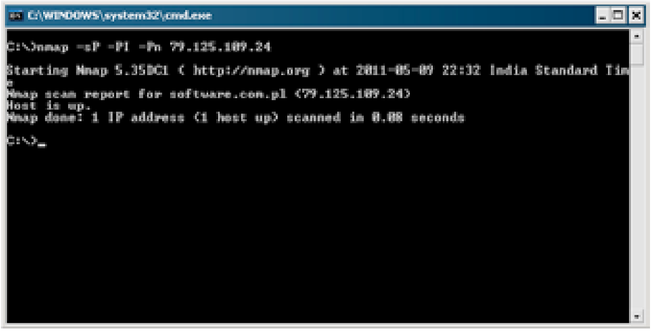
Although ping command is good, it is not made for advanced purposes. Tools like SING or WS_Ping ProPack are more often used to send ICMP packets because they enable users to send and receive spoofed packets. These advanced third party tools have satisfactorily replaced the ping command for many users.

NMap



```
C:\>nmap
Nmap 5.35DC1 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
```

NMap is an advanced tool for network reconnaissance. The tool can be downloaded from URL: www.insecure.org/nmap. After installing this tool, you'll be able to execute ping, ICMP echo / timestamp / netmask request, OS detection and even traceroute. In command prompt when you type nmap and press ENTER then you will get the list of all executable commands in nmap.

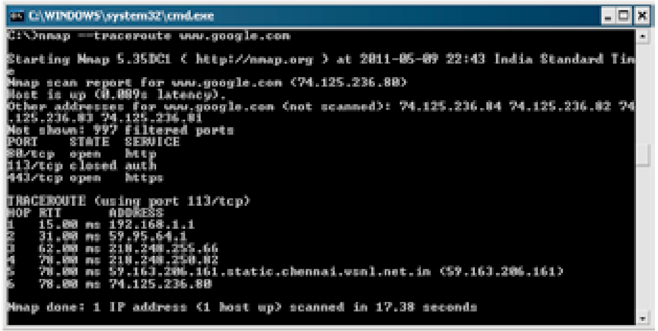


```
C:\>nmap -sP -PI -Pn 79.125.109.24

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-09 22:32 India Standard Tim
e
Nmap scan report for software.com.pl (79.125.109.24)
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds

C:\>_
```

You can perform ping sweeping on Nmap by executing the command: nmap -sP -PI -Pn 79.125.109.24

Output:

- Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-09 22:32
- Nmap scan report for software.com.pl (79.125.109.24)
- Host is up.
- Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds



```
C:\>nmap --traceroute www.google.com

Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-09 22:43 India Standard Tim
e
Nmap scan report for www.google.com (74.125.236.80)
Host is up (0.089s latency).
Other addresses for www.google.com (not scanned): 74.125.236.84 74.125.236.82 74
.125.236.83 74.125.236.81
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed auth
443/tcp open   https

TRACEROUTE (using port 113/tcp)
HOP RTT      ADDRESS
1   15.00 ms 192.168.1.1
2   31.00 ms 59.95.64.1
3   62.00 ms 218.248.255.66
4   78.00 ms 218.248.250.82
5   78.00 ms 59.163.206.161.static.chennai.vsnl.net.in (59.163.206.161)
6   78.00 ms 74.125.236.80

Nmap done: 1 IP address (1 host up) scanned in 17.38 seconds
```

Nmap traceroute command example: nmap --traceroute www.google.com

Output:

- Starting Nmap 5.35DC1 (http://nmap.org) at 2011-05-09 22:43
- Nmap scan report for www.google.com (74.125.236.80)
- Host is up (0.089s latency).
- Other addresses for www.google.com (not scanned): 74.125.236.84 74.125.236.82 74.125.236.83 74.125.236.81
- Not shown: 997 filtered ports
- PORT STATE SERVICE
- 80/tcp open http
- 113/tcp closed auth
- 443/tcp open https
- TRACEROUTE (using port 113/tcp)
- HOP RTT ADDRESS

1 15.00 ms 192.168.1.1
2 31.00 ms 59.95.64.1
3 62.00 ms 218.248.255.66
4 78.00 ms 218.248.250.82
5 78.00 ms 59.163.206.161.static.chennai.vsnl.net.in (59.163.206.161)
6 78.00 ms 74.125.236.80
Nmap done: 1 IP address (1 host up) scanned in 17.38 seconds

TCP Port Scanning

A list of open ports and services running on the remote host can be determined by port scanning the target system. Port scanning is among the oldest of techniques for information gathering and is always the first step by an attacker who is planning to break into a remote system.

TCP Connect Port Scanning

In TCP connect port scan a full three-way handshake is established. A system administrator on the remote system can easily determine that a port scan is tried on his / her system. TCP connect port scanning is fast, simple and accurate, but can easily be detected and traced. It is done in three steps:

- SYN (synchronize) flag is sent to each port on the remote system by the client.

- If the port is open, the remote system replies with an ACK (acknowledgement) as well as a SYN flag in a TCP packet. If the port is close, the remote system replies with an RST (reset) flag.
- ACK flag is then sent to the host by the client.

Nmap command for TCP connect port scan: nmap -sT -T 5 74.125.236.82

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-09 23:59
Nmap scan report for 74.125.236.82
Host is up (0.0011s latency).
Not shown: 988 filtered ports
PORT    STATE SERVICE
21/tcp  open  ftp
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
119/tcp open  nntp
143/tcp open  imap
443/tcp open  https
465/tcp open  smtps
563/tcp open  snews
587/tcp open  submission
993/tcp open  imaps
995/tcp open  pop3s
Nmap done: 1 IP address (1 host up) scanned in 33.13 seconds
```

TCP SYN Scanning

TCP SYN scanning was developed because TCP connect port scanning is easily detectable. In this only the first TCP packet containing the SYN flag and establishing a half TCP connection. TCP SYN scanning is fast, easy, accurate and harder to trace but is not stealthy and can easily be blocked. It is done in two steps:

- A TCP packet with a SYN flag is sent to the remote system by the port scanner.
- The remote system replies with a SYN/ACK (port is in listening state) or RST/ACK (port is not listening) packet.
- Nmap command for TCP SYN port scan: nmap -sS -T 5 74.125.236.82

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-10 00:17
Nmap scan report for 74.125.236.82
Host is up (0.088s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
80/tcp  open   http
113/tcp closed auth
443/tcp open   https
Nmap done: 1 IP address (1 host up) scanned in 13.39 seconds
```

TCP / FIN Scanning

In this type of port scan, a FIN packet is sent to the target port and if the port does not respond then the port is open else if the port is close then it will reply with a RST packet. FIN scan was primarily designed for UNIX systems, thus, other OS respond to FIN packets sent to open ports with an RST packet.

Nmap command for TCP/FIN port scan: nmap -sF -T 5 74.125.236.82

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-10 00:50
Nmap scan report for 74.125.236.82
Host is up (0.084s latency).
Not shown: 999 open|filtered ports
PORT    STATE  SERVICE
113/tcp closed auth
Nmap done: 1 IP address (1 host up) scanned in 8.56 seconds
```

TCP NULL Scanning

In this type of port scanning, a NULL packet (all flags are turned off) is sent to the host system. If the port is open then it will have no idea about what to do with it and so replies with an error message or discards it. If the port is close then it'll reply with a RST packet. This scanning method works effectively on UNIX based systems.

Nmap command for TCP/FIN port scan: nmap -sN -T 5 74.125.236.82

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-10 00:52
Nmap scan report for 74.125.236.82
Host is up (0.078s latency).
All 1000 scanned ports on 74.125.236.82 are open|filtered
Nmap done: 1 IP address (1 host up) scanned in 63.81 seconds
```

TCP XMAS Tree Scanning

TCP XMAS tree scanning is opposite of TCP NULL scanning. Here, a packet with all flags turned on is sent to the host system. If the port is open then it'll reply with an error message else if the port is closed then it replies with a RST packet. This scanning method works effectively on UNIX based systems.

Nmap command for TCP/FIN port scan: nmap -sX -T 5 74.125.236.82

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-10 01:08
Nmap scan report for 74.125.236.82
Host is up (0.086s latency).
Not shown: 999 open|filtered ports
PORT    STATE  SERVICE
113/tcp closed auth
Nmap done: 1 IP address (1 host up) scanned in 11.47 seconds
```

Tcp port scanning

UDP is a connectionless protocol and in UDP port scanning, a UDP packet is sent to all 65535 UDP ports. If the remote port is closed, then the server replies with "ICMP destination port unreachable" messages else if the port is open, then no such error message is generated because of the nature of UDP.

NMap is capable of UDP port scanning using the command: nmap -sU -T 5 74.125.236.82.

Output:

```
Starting Nmap 5.35DC1 ( http://nmap.org ) at 2011-05-14 07:17
Nmap scan report for 74.125.236.82
Host is up (0.065s latency).
Not shown: 998 open|filtered ports
PORT      STATE    SERVICE
138/udp   filtered netbios-dgm
33459/udp closed   unknown
Nmap done: 1 IP address (1 host up) scanned in 35.89 seconds
```

UDP port scanning in not always accurate because if the target host has installed a firewall filter for all the ICMP messages that go out of the network then most UDP port scanning tools will generate inaccurate results.

Port Scanning Tools

1. **Strobe:** It is a UNIX based tool meant for only TCP port scanning. This tool is fast and efficient but it cannot perform UDP port scanning. This tool is developed in C by Julian Assange.
   Download URL: ftp://ftp.internat.freebsd.org/pub/FreeBSD/ports/i386/packages-8-current/security/strobe-1.06.tbz
2. **Netcat:** Netcat, also known as TCP/IP Swiss Army Knife is a simple UNIX based tool that provides TCP and UDP port scanning.
   Download URL: http://sourceforge.net/projects/nc110/files/
3. **SuperScan:** It is a Windows based TCP / UDP port scanner that has variety of other utilities like traceroute, hostname lookup, whois and ping. You can specify any IP range for performing port / ping scans.
   Download URL: http://www.softpedia.com/get/Network-Tools/Network-IP-Scanner/SuperScan.shtml
4. **Hping:** hping is a command line oriented TCP/IP/ICMP/UDP packet analyzer. It can perform OS fingerprinting, firewall testing, trace routing, network fragmentation testing and many more. It is available for a variety of OS's like Linux, BSD, Solaris, Windows and MacOS.
   Download URL: http://www.hping.org/download.php
5. **ipEye:** It is a Windows based port scanner that is developed by Arne Vidstrom. It uses the Windows command prompt to launch variety of scans like SYN, FIN, NULL and XMAS.
   Download URL: http://www.net-security.org/dl/software/ipeye.exe

Countermeasures against Port Scanning

The difficulty in preventing port scanning of your system is that you cannot disable ports like HTTP, TCP or UDP as they are used by your client base. The least you can do to prevent port scanning is block or disable all ports that are of no use or where no daemon is running. This will reduce the possible number of entry points that lead to your critical system information. This countermeasure should especially be practiced on Windows based systems as by default there are many ports that are open on them.

Active monitoring of your system is another method by which you can prevent successful port scanning. This includes installing firewall or sniffing tools that monitors and maintains logs of all port scanning attempts. These logs can help you trace the users who are port scanning your system.

Countermeasure Tools for Port Scanning

1. **Scanlogd:** It is an Intrusion Detection System (IDS) which can be used to detect TCP port scans. This tool is ideally a UNIX based but can also be used on Windows based systems using the libnids and libpcap libraries. The Windows version of this tool is contributed by Michael Davis.
   Download URL: http://www.openwall.com/scanlogd/
2. **NukeNabber:** It is windows based tool that listens to the TCP and UDP port scans. This tool is designed to let you trace an attacker and can monitor 50 ports simultaneously.
   Download URL: http://majorgeeks.com/NukeNabber_d607.html
3. **BlackICE:** BlackICE is an IDS as well as firewall protection system. It's like a hacker's antivirus for your system because it enables you to detect the attack, tells you about the vulnerability and blocks the vulnerable port. This tool doesn't hog up on your system resources and can even be used to detect viruses on your hard disk.
   Download URL: http://download.cnet.com/BlackICE-PC-Protection/3000-2092_4-10040175.html

FTP Port Scanning

FTP port scanning is a method by which a malicious user connects to a FTP service on a particular system and then uses that FTP server to port scan any other system. This method is fast, easy and it offers anonymity to the user using it, but can easily be prevented by the system admin. A properly configured system can easily prevent FTP port scanning.

Countermeasures against Network Reconnaissance

Network scanning is one of the most time proven techniques for information gathering. You can't stop anyone from scanning your network, simply because that would affect your site's traffic. However you can make the work of malicious users difficult by implementing certain countermeasures.

- ICMP error messages are most dangerous of all the messages that can be received by the malicious users. Block or filter all ICMP error messages out of our network so that UDP or half TCP scanning become impossible. This will force the users to go with full TCP connect port scan leading to easy trace.
- Configure your firewall such that it can handle fragmented data. This will prevent attacks like tear drop. Also, port scanners have a peculiar speed of scanning a network for open ports. Configuring your firewall to detect fast port scans will lead to dropping of all packets from the source IP address for some time.
- Configure firewall such that FTP port scanning is not possible. It is always recommended that you install the latest patches for your firewall to ensure maximum security against any loop holes that are found by the manufacturer.
- The filtering mechanism on routers and firewall should be implemented in such a way that accessing your network without passing through the firewall is not possible.
- Scanners usually try to send many packets to several destination ports simultaneously in a quick time. Using this as signature pattern intrusion detection systems can be designed to obstruct the attack.
- Sending spoofed ICMP error messages to the malicious users is also a good method for concealing the real ICMP error messages.
- Penetrate your network regularly yourself or call a penetration tester to do it for you. This exercise will make you realize the vulnerabilities that are in your system. Professional penetration testers are always equipped with latest tools and techniques for penetrating a network in such a way that most system admins fail to realize.

DHANANJAY D. GARG

The author is an information security enthusiast who is based in India. He likes working on projects related to information security. As a freelance writer, he often writes on various topics related to computer sciences and can be contacted at dhananjaydgarg1989@gmail.com.

Is scanning of computer networks dangerous?

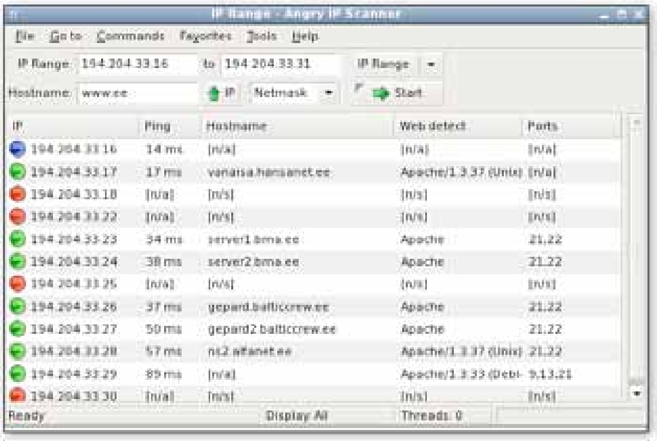
Scanning of computer networks (searching for addresses with known properties) is a practice that is often used by both network administrators and crackers. Although it is widely accepted that activity of the latter is often illegal, most of the time they depend on exactly the same tools that can be used for perfectly legitimate network administration – just like a kitchen knife can be used maliciously.

Thanks to the recent activity of mass-media on the subject (that popularized the wrong term for a cracker – a 'hacker'), nowadays every educated person more or less understands the reasons and goals that stand behind malicious cracking: curiosity, stealing of information, making damage, showing self-importance to the world, etc. But why do administrators need to scan their own networks? There are plenty of answers: to check status of computers and various network devices (are they up or down), find spare addresses in statically-addressed networks, monitor the usage of server-type or P2P applications, make inventory of available hardware and software, check for recently discovered holes in order to patch them, and much more things that are even difficult to foresee.

One widely-used open-source and cross-platform network scanner is Angry IP Scanner, written and maintained by the author of this article. As a rule, almost all such programs are open-source, because they are developed with the collaboration of many people without having any commercial goals. Secure networks are possible only with the help of open-source systems and tools, possibly reviewed by thousands of independent experts and crackers alike. In this article we will see how is this program's scanning component built and what are its working principles.

Features

Will begin with the definition of an IP address. IP means nothing more complex than the Internet Protocol. Nowadays, thanks to the Internet, TCP/IP is the most widely spread network protocol that over the years has replaced many other LAN and WAN protocols – it is now used in the majority of networks not even directly connected to the Internet. An IP address is the unique identifier of a network interface in the network. Most of the world still uses the older IPv4 version of the protocol, that limits the address space to 32 bits, making the maximum number of directly addressable nodes to be less than 4 billion, which will soon not be enough for current Earth's population of over 6 billion and the increasing usage of computers and mobile devices. In order to fix the problem, IPv6 was introduced at the end of the previous decade, that among other features provides a much broader address space of 128 bits. However, the usage of CIDR (classless inter-domain routing, that gave us "/24" network size notation, as opposed to the early "classful" Internet) and NAT (network address translation) are now helping to survive with the exhaustion of the IPv4 address space, and therefore is slowing down the adoption of IPv6. Until now, there are only a few ISPs worldwide supporting IPv6 and a relatively small number of early adopters, bridging their IPv6 networks to IPv4. Angry IP Scanner



IP Range: 194.204.33.16 to 194.204.33.31

Hostname: www.ee

IP	Ping	Hostname	Web detect	Ports
194.204.33.16	14 ms	[n/a]	[n/a]	[n/a]
194.204.33.17	17 ms	vanaisa.hansanet.ee	Apache/1.3.37 (Unix)	[n/a]
194.204.33.18	[n/a]	[n/s]	[n/s]	[n/s]
194.204.33.22	[n/a]	[n/s]	[n/s]	[n/s]
194.204.33.23	34 ms	server1.bma.ee	Apache	21,22
194.204.33.24	38 ms	server2.bma.ee	Apache	21,22
194.204.33.25	[n/a]	[n/s]	[n/s]	[n/s]
194.204.33.26	37 ms	gepard.balticcrew.ee	Apache	21,22
194.204.33.27	50 ms	gepard2.balticcrew.ee	Apache	21,22
194.204.33.28	57 ms	ns2.alfanet.ee	Apache/1.3.37 (Unix)	21,22
194.204.33.29	89 ms	[n/a]	Apache/1.3.33 (Debi-	9,13,21
194.204.33.30	[n/a]	[n/s]	[n/s]	[n/s]

Ready Display All Threads: 0

Angry IP Scanner's main window

was designed with IPv6 in mind, but the present user interface supports IPv4 only, as it is currently more useful.

Now what does an IP scanner able to do? As a rule, user provides a list of IP addresses to a scanner with the goal of sequentially probing all of them and gathering interesting information about each address as well as overall statistics. The gathered information may include the following:

- if the host is up (responding) or down (not responding)
- average roundtrip time (of IP packets to the destination address and back) – the same value as shown by the ping program
- TTL (time to live) field value from the IP packet header, which can be used to find out the rough distance to the destination address (in number of routers the packet has traveled)
- host and domain name (by using a DNS reverse lookup)
- versions of particular services running on the host (e.g., "Apache 2.0.32 (Linux 2.6.9)" in case of a web server)
- open (responding) and filtered TCP and UDP port numbers
- ... and much more

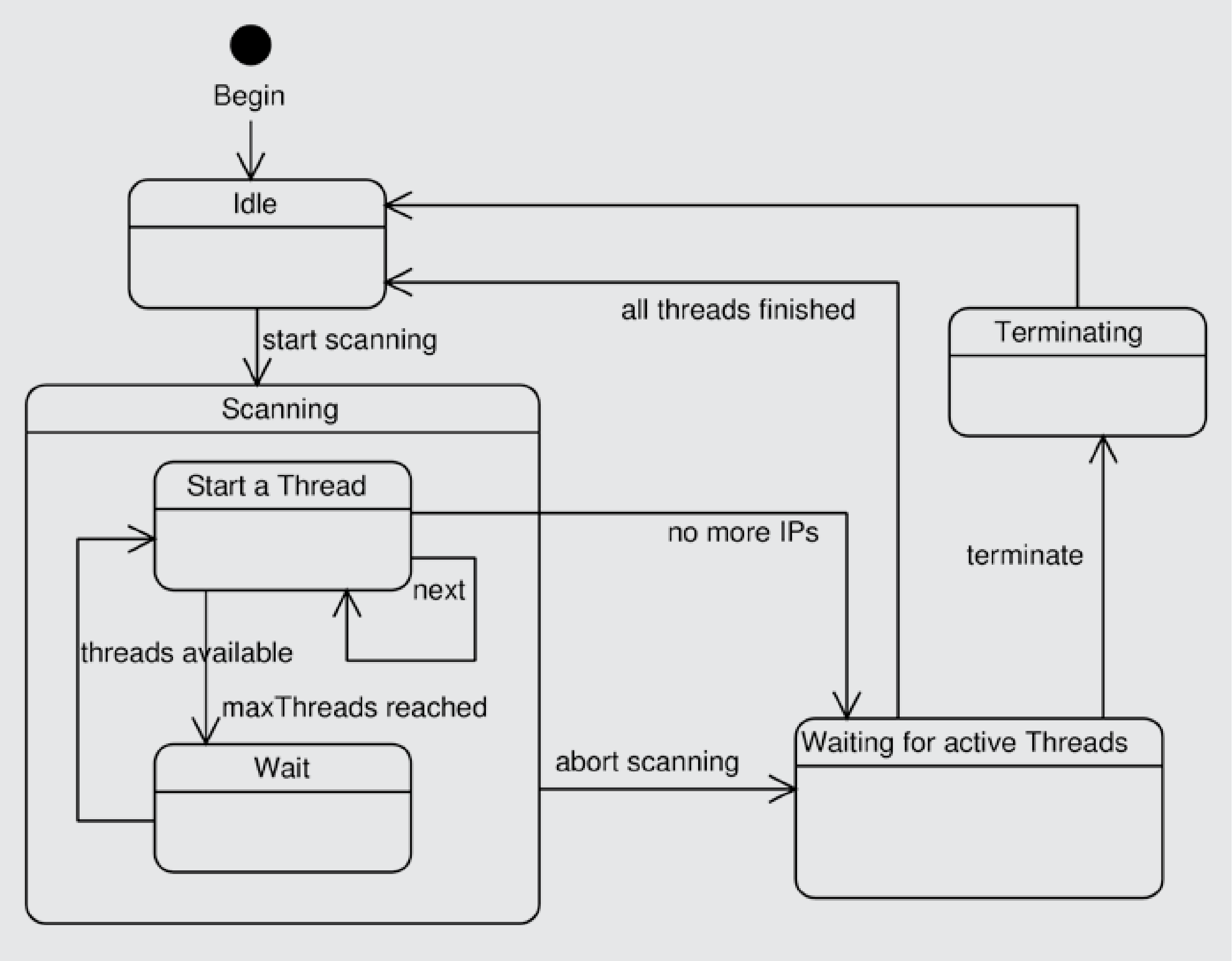
The list of addresses for scanning is most often provided as a range, with specified starting and ending addresses, or as a network, with specified network address and corresponding netmask. Other options are also possible, e.g. loading from a file or generation of random addresses according to some particular rules. Angry IP Scanner has several different modules for generation of IP addresses called feeders. Additional feeders can be added with the help of plugins.

Scanning component

Angry IP Scanner's scanning component is implemented as a Mediator pattern, which routes messages between the user interface, generator of IP addresses (feeder), and information retrieving modules (fetchers), generating events for other components. This ensures that all components of the program are loosely coupled and therefore reusable and interchangeable.

The scanning component itself is very abstract – it knows nothing about what information is being collected. Information is gathered with the help of fetchers that are selected by the user. Angry IP Scanner contains a number of built-in fetchers (e.g. mentioned above), but additional third-party fetchers can be used with the help of plugins. This ensures very good scanning flexibility and extensibility of the program – each user can have very different and non-standard needs, especially if the user is an administrator of a large network.

During scanning, the scanning component is controlling states (see the state diagram below). In the scanning state it iterates IP addresses provided by fetcher and gives control to fetchers in order to do the actual scanning.



State diagram of scanning component

All this would be very slow without doing most of the work in parallel.

Helpful threads

The easiest and most reliable way to make code run in parallel is the usage of threads, because in this case the operation system is dealing with all the complexity of task switching and scheduling, making programming a lot easier. The OS can even run several threads really in parallel if the machine has several CPUs, which is another great advantage over manual parallelizing. The programmer must only take care of proper synchronization.

But let's assume that the machine has only one CPU. Then, as opposed to microprocessor systems, threads cannot just magically increase the performance, especially in the case, when each thread needs 100% of processor time, which would result in performance degradation due to too frequent context switching compared to sequential program.

Fortunately, this problem is very improbable in case of scanning of networks: networks are generally much slower than the processor. Consequently, time consumed on processing of each packet is mostly spent on waiting for the second party's response, allowing the processor do deal with other jobs, which can include sending and waiting for other packets at the same time, resulting in much shorter total time required to process many packets compared to the sum of each packet's individual processing times.

Without threads it is also possible to process multiple packets simultaneously with the help of asynchronous sockets. In some way they can even perform slightly better, however if any complex processing of the results is in place and invocation of third-party plugins that send completely different and unrelated packets out all make the thread usage more reliable and much easier in terms of programming. Thanks to threads, the code of each fetcher or plugin can be linear, eliminating the need to think about what other fetchers are sending or receiving at the same time. It is well accepted that good design and simplicity of the code in programming are often much more important than slight performance improvements, because quality (working software) and lower costs of maintenance are very desirable in any case. Moreover, the easier it is to write a plugin, the more third-party plugins will be written, affecting the end users positively.

Unfortunately, there is a practical limit to the number of threads used for scanning. The limit is reached when context switching starts taking a considerable amount of processor time instead of doing the actual job. As different operating systems implement different switching and scheduling algorithms, maximum practical number of threads is different on different platforms even if running on the same hardware. Trials show that Microsoft operating systems are inferior in this respect to the free systems (e.g. Linux, *BSD), while older Windows versions (9X and ME) were not even able to process user events at the same number of threads that had no noticeable impact on Linux.

Because the maximum number of threads may be very different, Angry IP Scanner uses no more than 100 threads at a time by default. The user has the possibility to increase this number if their hardware and software allows that, or the opposite. Some latest combinations can even handle 500 scanning threads with no problems, however this number may be close to the situation when threads finish their jobs before the scanner is able to reach the limit by starting new ones. Another limitation may be due to instability of some network adapters or their drivers (especially wireless ones) – they just cannot process so many simultaneous connections or packets, so they start loosing them, rendering scanning results unreliable. The same problem sometimes is created artificially mostly on Windows platforms by rate limiting of connection attempts (Windows XP SP2 limits to 10 simultaneous connection attempts) with the goal of preventing scanning by worms that are unfortunately likely to get into the system.

Increasing scanning speed

The wish to make their tools better is very natural for humans. As scanning is a process that takes time, it is very natural to think about the ways to increase its speed. The delay of getting the information depends on scanning speed, and consequently the validity of the scanning results depends on it as well, because some networks can be very dynamic – especially dial-up and Wi-Fi networks. In some cases scanning speed can become even critical, e.g. when network administrator needs to localize all infected machines because of a zero-day worm or virus getting into the network. Also productivity should not be underrated – quick scanning makes administrator's job more effective, especially in case of large corporate networks.

Besides parallelizing, there are some more possibilities how to increase the scanning speed. The easiest way that is sometimes useful is the speed-accuracy compromise: the user can decrease various timeouts and the number of probes done (in case of pinging, for example). This will increase the probability of missing some hosts or ports, but the results are returned much more quickly. This can be useful in very crowded networks for getting of statistics.

A little bit smarter development of the above-mentioned idea are adaptive timeouts. The principle is in measuring of the average roundtrip time of packets in either the whole network or to the particular host and then using the value as a timeout for sending of the following packets. This can dramatically increase port scanning speed in case the host is probed with ICMP echo (ping) packets first, especially in contemporary networks where there are many network- and even host-based firewalls blocking the packets, making most of the ports filtered (no reply is sent to the TCP SYN packets at all). This makes port scanning speed depend a lot on the length of timeout for each port (for how long we are waiting for the response), and the shorter the timeout is, the faster scanning becomes. That means the scanner must always select the shortest reliable timeout possible, during which most of the packets should have enough time for getting back. And this desired timeout can be different for each scanned host. However, if the timeout is too short, then scanner will not get any replies to most of the packets, considering that the ports are filtered, but actually the host just replies slower than expected. Angry IP Scanner measures the average roundtrip time (if possible), multiplies it by three and then uses that value as a timeout for port scanning. Even this simple solution speeds up scanning several times.

Another relatively easy idea is *thread pooling*. Although, creation of each thread is by no means cheaper than creation of a process (sometimes threads are even called "lightweight processes"), it still is a relatively complicated task, involving memory allocation, registration in different system tables, etc. Considering very high level of thread creation and their short-liveness, it is wiser to reuse them instead of destroying them continually. As the scanner needs to limit the maximum number of threads anyway, why not to use the same number for the size of thread pool? In this case, when any thread finishes scanning a host, it is put to sleep, marked as free, and is returned back to the pool. Then, in case there are more addresses to scan and some threads are available in the pool, they can be taken back and reused for scanning of other hosts. In some programming languages or libraries, implementations of *thread pools* are even already available and can be used without any additional effort from the programmer: for example, *ThreadPoolExecutor* in Java 1.5 (for older versions of Java, Doug Lea's util.concurrent library can be used), and ThreadPool in .NET.

Scanning under different Operating Systems

Even though Angry IP Scanner is a cross-platform application, there is no reason to hope that each platform is suitable as a scanning source equally well.

Having mentioned the weakness of older Windows operating systems related to threads, we must say that Windows versions based on the NT architecture are a lot better in this respect – their TCP/IP stack implementation is much better. However, starting from XP SP2, consumer versions of Windows became even worse for scanning than before because of some newly introduced limitations. Namely, Microsoft has started limiting the number of outgoing connections per minute, removed raw socket support from Windows XP that are needed for sending and receiving of ICMP packets as well as for performing of more sophisticated scanning tricks, etc. The official reason was to prevent the widely-spread Internet worms from doing scanning and DDoS (Distributed Denial of Service) attacks from the infected Windows machines, but there is some speculation that the real reason was to force more advanced users to use the more expensive Windows Server family of operating systems. According to Microsoft, Windows XP (and Vista) is made for regular users who do not need to scan their networks or do anything advanced with networking.

Open source operating systems (and even Mac OS X that has its kernel based on FreeBSD) for sure are much better suitable for network administrators, considering their security, out-of-the-box functionality, and even the price. Many of the advanced functionality has existed in them for decades, without compromising security and becoming the nest for all kinds of malware, that are ruining the reputation of Windows.

Having said that, Linux gives the users of Angry IP Scanner more features, higher scanning quality and speed. As a bonus, Linux users get a lot of other useful software for network monitoring that works only there.

In order to reduce confusion among the end-users on Windows platform, it was decided to implement some detection mechanism of the reliable values for maximum number of threads and different timeouts when starting Angry IP Scanner for the first time. It will either try to open a local port itself and try to aggressively scan it for a couple of seconds or ask the user for some host and port that they know is open and accessible and perform the test against it. Then it will set up the best values that work reliably on the given machine. Unfortunately, it will make scanning a lot slower on most newer Windows machines, but at least the scanning results will be reliable and trustful.

Safety

Many Angry IP Scanner users ask: how safe or legal is it to use such a program?

Fortunately, the short response is that it is both legal and safe, however with some exceptions.

Even though nowadays legal laws do not catch up with the fast development of the IT world, network scanning has existed for almost as long as the networks themselves, meaning that there was probably enough time to update the laws. Nevertheless, scanning itself remains perfectly legal, because in most cases it neither harms the scanned systems in any way nor provides any direct possibilities of breaking into them. Network scanning is even used by some popular network applications for automatic discovery of peers and similar functionality. Most countries' laws forbid getting illegal access to data, destroying, spoiling, modifying it, or reducing its usefulness or value in some other way. As a rule, the scanning results just provide the publicly available and freely obtainable information, collected and grouped together. However, this legality may not apply in case some more advanced stealth scanning techniques are used against a network you don't have any affiliation with.

As the topic of user's personal safety is covered: scanning in most cases is legal, then how about the more general safety – the safety of all the people? As was already mentioned before, nothing can be one hundred percent safe. On the other hand, the best tools for maintaining the security are the same ones that are used by those who we need to defend from. Only that way it is possible to understand how do crackers think and how do they work. Using the same tools as they do it is possible to check the network until it is too late because they managed to do it themselves.

Every serious network administrator knows that regular probing of own networks is a very good way for keeping it secure.

Background information

Angry IP Scanner is a well-known and very popular IP scanner. It is used in banks, government agencies (including in the USA), education networks, in many large and small companies as well as at homes all over the world.

Its first and very simple version was released in 1998. As its popularity grew, the development was continued. Recently, a preview of version 3.0 was released, which is a complete rewrite of the program in Java language with the goal to make it cross-platform.

During its existence, Angry IP Scanner was featured in many magazines, such as German PC Welt, Russian ComputerPress, British PC Advisor, put on hundreds of compilation CD-ROMs, as well as mentioned in some books on computer security.

At the time of writing this article, Google search returns about 460 000 results where Angry IP Scanner is mentioned, and this number even excludes different nicknames that users sometimes use, like "angryip". The official site is visited by an average of 5000 people every day and almost half of them download the program.

ANTON KEKS

is a software craftsman, co-founder of Codeborne, an agile software development company in Estonia, frequent speaker at conferences, and a lecturer in Tallinn Technical University. He is also a strong believer in open-source software and agile development methodologies, regular contributor to numerous open-source projects. During spare time he plays a guitar, rides a motorbike and travels to remote corners of the world.

Links

- Angry IP Scanner official page – http://www.angryip.org/
- Google search - http://www.google.com/search?q=angry+ip+scanner
- TCP/IP stack: http://en.wikipedia.org/wiki/Internet_protocol_suite
- IP protocol: http://en.wikipedia.org/wiki/Internet_Protocol
- Legal: http://www.asianlaws.org/cyberlaw/library/cc/ptscanning.htm

Network Infrastructure Parser – Nipper – An Introduction

Short for Network Infrastructure Parser, Nipper is an open source network devices security auditing tool. One benefit of being open source is that it's free. Previously known as Cisco Parse, Nipper Command Line Tool isn't flashy or pretty, but it is very functional, easy to install, easy to use, and it does exactly what it says it will do. It works with many different types of network devices, not just Cisco.

Here's a list of compatible network devices that Nipper can audit:

- Cisco Router (IOS)
- Cisco Catalyst (IOS)
- Cisco Catalyst (NMP)
- Cisco Catalyst (CatOS)
- Cisco Firewall (PIX)
- Cisco Firewall (ASA)
- Cisco Firewall (FWSM)
- Cisco Content Services Switch (CSS)
- Juniper ScreenOS Firewall
- Nortel Passport
- Nortel Ethernet Routing Switch
- Nortel Contivity
- Nortel Switched Firewall (CheckPoint)
- Nortel VPN Router
- Alteon Switched Firewall (CheckPoint)
- Bay Networks Accelar
- Checkpoint Firewall Module
- Checkpoint Management Module
- Checkpoint IP
- Nokia IP
- Crossbeam Firewall
- SonicWall SonicOS Firewall
- HP ProCurve Switch
- HP JetDirect Print Server
- 3Com SuperStack 3 Firewall
- 3Com 5500 Switch
- Extreme Networks Summit (ExtremeWare)
- Extreme Networks Alpine (ExtremeWare)
- Foundry BigIron Switch (IronWare)
- Foundry FastIron Switching Router (IronWare)
- Foundry NetIron Switching Router (IronWare)
- Fortinet FortiGate
- WatchGuard Firebox-X Edge

Network filtering audits include the following, all of which can be modified:

- Rule lists end with a deny all and log
- Rules allowing access from any source
- Rules allowing access from network sources
- Rules allowing access from any source port
- Rules allowing access to any destination
- Rules allowing access to destination networks
- Rules allowing access to any destination service
- Rules that do not log
- Deny rules that do not log
- Rules that are disabled
- Rules that reject rather than drop
- No bypass rules exist
- Default rules
- During a security audit Nipper can test passwords and connection timeouts, these can be configured from the command line.

The configurable options are:

- Timeout
- Minimum Password Length
- Passwords must contain upper case characters
- Passwords must contain lower case characters
- Passwords must contain numbers
- Passwords must contain special characters
- Passwords can contain upper or lower case characters

- Dictionary for testing against passwords

Nipper will decode Cisco type 7 passwords, other passwords can be output to a john-the-ripper file for further testing. Nipper includes support for a variety of different device types and gathers a lot of information whilst performing a security audit. However, nipper does not gather all information from a device configuration.

The following describes what information is used and what security issues nipper identifies.

IOS-Based Configuration Settings:

- Hostname
- IOS Version
- Timezone and offsets
- Authorative Time Source
- Service Password Encryption
- Minimum Password Length
- IP Source Routing
- Bootp
- Service Config
- TCP Keep Alives
- Cisco Express Forwarding
- Gratuitous ARP
- Classless Routing
- Domain Name
- Domain Lookup
- DNS Servers
- Enable Passwords
- Users
- Privileges
- Banner
- Telnet
- SSH
- HTTP
- Finger
- TCP / UDP Small Services
- NTP
- SNMP
- CDP
- PAD
- Logging
- Syslog
- Buffered Logging
- Terminal Logging
- FTP
- TACACS
- AAA
- BGP
- VRRP
- EIGRP
- RIP
- OSPF
- Routes
- Route Maps
- Keys and Key Chains
- Lines
- Interfaces
- VTP
- Switch Ports
- NAT (All types)
- ACL (All types)

IOS-Based Security Issues:

- Software Versions
- Dictionary-Based / Default Passwords
- Weak Passwords
- Auto-Configuration
- IP Directed Broadcasts
- BGP Route Dampening
- OSPF Authentication
- EIGRP Authentication
- RIP Authentication
- VRRP Authentication
- TCP Keep Alives
- Connection Timeouts
- AUX Port
- Source Routing
- Finger
- HTTP
- SNMP
- Telnet
- Redirects
- Access Lists
- uRPF Verification
- Switch Port Mode
- Switch Port Security
- Logging
- Proxy ARP
- SSH
- CDP
- Classless Routing
- Minimum Password Length
- Bootp
- TCP / UDP Small Servers
- IP Unreachables
- IP Mask Reply
- Enable Secret
- Password Encryption
- Banners
- Domain Lookup
- PAD
- MOP

PIX/ASA/FWSM-Based Configuration Settings:

- Hostname
- Domain Name
- Version
- Transparent Firewall
- Enable Password
- Users
- SSH
- Interfaces
- NAT / PAT
- Routing
- Access Control Lists
- ICMP Access
- Protocol Analysis
- Group Objects
- Name Mappings

PIX/ASA/FWSM-Based Security Issues:

- Connection Timeouts

- Access Control Lists
- SSH Protocol Version

CSS-Based Configuration Settings:

- Hostname (a little hack, recommend specifying)
- CSS Version
- FTP Server
- SNMP
- SSH Server
- Telnet Server
- Web Management Server
- Access Control Lists

CSS-Based Security Issues:

- SNMP
- Telnet
- Access Control Lists

CatOS/NMP-Based Configuration Settings:

- Hostname
- NMP Version
- Location
- Contact
- Core Files
- Syslog Files
- Idle Session Timeout
- Port Security Auto Configure
- Enable Passwords
- Login Passwords
- ICMP Redirects
- IP Unreachables
- IP Fragmentation
- CDP
- SNMP
- Permit Lists
- VLAN Configuration

CatOS/NMP-Based Security Issues:

- Dictionary-Based / Default Passwords
- Weak Passwords
- Connection Timeouts
- IP Redirects
- CDP
- IP Unreachables

ScreenOS-Based Configuration Settings:

- Hostname
- Administrative Settings
- Users
- Alerting
- Timeouts
- Authentication Server
- Admin Privileges
- SSH
- Interfaces
- Policies
- Name Lists

ScreenOS-Based Security Issues:

- Policies
- Connection Timeout
- Administrative HTTP Redirect
- Management IP Address

The output from Nipper can be in HTML, Latex, XML or Text formats. Furthermore, Nipper will reverse any Cisco type-7 passwords identified; all other encrypted passwords can be output to a John-the-Ripper file for further strength testing. By default, input is retrieved from standard input (stdin) and is output (in HTML format) to standard output (stdout).

How do you use Nipper?

1. First, download Nipper from SourceForge.net (http://sourceforge.net/projects/nipper/) or http://packetstormsecurity.org/search/files/?q=nipper%200.12 — it's available for Microsoft Windows, Apple Mac OS X and GNU/Linux systems. Extract it to a folder on our local PC; let's call it C:\nipper.
2. Next, obtain a text version of the router's configuration file. Telnet or SSH to the router, use the show running-configuration command, copy and paste the output into Notepad, and save it to your local PC in the aforementioned C:\nipper directory.
   Example on how to get the config of a Cisco Router:
   A. Log on to the device IOS or Console.
   B. Authenticate with your credentials.
   C. Type at the command line: show running config
   D. Copy the contents displayed.
   E. Open notepad (start -> run -> notepad)
   F. Paste the contents onto notepad and save it as . config
   Alternatively, you can use a TFTP server and copy the configuration to your local PC. For example, try using Tftpd32.exe. Use the copy running-configuration tftp command.
3. Once you have the running configuration that you want to audit on your PC, go to the Windows command prompt, and CD into the Nipper directory. Run the following:
   ```
   c:\nipper>nipper --ios-router--input=testrouterconfig.txt
                        --output=audit.html
   ```
   The system will immediately return you to the command prompt without providing any information. But don't worry — it worked.
4. Next, open a Web browser and enter this URL: c:\nipper\audit.html. This will take you to the security report that you just generated.

What does Nipper tell you?

Nipper provides security audit information such as:

- A software version that has vulnerabilities and the reference numbers for those vulnerabilities
- Recommendations to disable services that might cause others to be able to access the router
- Commands that you need to enable to secure the router

In your report, Nipper might tell you that you need to do the following:

- Upgrade the router's IOS needs to prevent vulnerability to a Telnet remote DoS attack and a TCP listener DoS attack.

- Configure the service tcp-keepalives-in command to help prevent a DoS attack.
- Configure timeouts on consoles to prevent anyone from gaining access to the router from a Telnet or console session.
- FTP and Telnet are enabled
- SSHv2 is being used instead of the more secure SSHv3
- Configure the HTTP service as secure with HTTPS, and enable authentication.
- Enable logging.

Nipper also provides a summary of the device's configuration — what services are turned on or off, status of the lines, status of the interfaces, DNS, time zone, and more.

Nipper One

I personally like to use Nipper One which has a GUI interface and is easy to use. You just point at the configuration file and a very friendly report is created. You can download it and try it for free https://www.titania-security.com/nipper/overview. After you install Nipper One, click on the NipperOne.exe file. You can either allow Nipper One to auto detect the device type or you can select it from the drop down..

Step two is selcting the configuration file to be tested which can be a text file (.txt) or conguration file (.config or .cgf) and selecting Go! You will need to add the 30 day free trial license key before the report will be generated.

There are additional setting that you can change to have the security report that will best suit your environment.

Nipper One has two files that you may want to review and use for security reporting and tracking. The first is the vuln2.db file which is in the resources folder. An easy way to review this file is to change the file extension from db to xml and open the xml file with Microsoft Excel. You will want to import it as an XML table.

Vuln2 Database in MS Excel

I use the database to easily correlate findings and create trend reports.

The second file you will want to look at is the nipper.ini file. It is used with the Nipper Command Line tool. You use this file if you want to add ports, set defaults, etc.

Conclusion

Using the Nipper Command Line Tool or the Nipper One GUI, security administrators and managers can quickly see the security posture of their routers, switches and firewalls. This allows the security issues to be addressed quickly. I have used these tools on routers, switches and even firewalls that are 6000 lines long. In each case, it quickly helped me to identify critical issues. What I like most almost about Nipper One compared to the Nipper Command Line Tool is that the reports that it generates are colored coded versus just a white and blue font html webpage. Nipper One uses a color coded system in the generated reports red – orange – yellow which makes presenting issues to management easier. It also allows me to quickly do analysis and create project plans. I have listed a few colored coded examples for you.

The impact section describes what an attacker could gain from exploiting the security issue. The impact of an issue is often defined by other configuration settings that could heighten the issue or partially mitigate it. For example, a weak password could be partially mitigated if the access gained from using it is restricted in some way. The impact is rated depending on the significance of the security threat.The ease section of each issue describes the knowledge, skill and physical access that would be required of an attacker in order to exploit it. The ease will describe if open source or commercially available tools are required for an attacker to exploit an issue. Additionally, the ease will note where an extended period of time is required to exploit the issue, such as cracking weak encryption ciphers. Each issue is rated upon how easily it can be exploited.

Each issue includes a recommendation section which describes what steps Nipper recommends should be taken in order to mitigate the issue. The recommendation will sometimes include various options, if several mitigating choices are available, and any relevant system commands.

Directly following the recommendation, the issue dependencies and other relevant issues are referenced. The dependency issues are those that when mitigated will eliminate the described issue. For example, if the Simple Network Management Protocol (SNMP) is disabled it no longer matters if a view has not been configured. The relevant issues are ones that can affect the impact or the ease that the issue can be exploited.

The recommendation includes a rating that indicates how easy an issue is to resolve.

The recommendation section is designed to assist in the mitigation of the security issues identified by collating the security issue recommendations into a single location.

REBECCA WYNN

Rebecca Wynn, MBA, CISSP, LPT, CIWSA, NSA/CNSS NSTISSI 4011-4016 is a Principal Security Engineer with NCI Information Systems, Inc. She has been on the Editorial Advisory Board for Enterprise I.T. Magazine since its inception.

References

The Titania web site (http://www.titania.co.uk) includes Nipper user documentation, device specific documentation, support forums, feature request and issue tracking system, updates, licensing information and more. Nipper is copyright Titania Limited.

PCI AUDIT

The Road To Compliance

Most of you probably have already heard about PCI DSS. It is the standard that was formed by the five major credit card brands back in 2004. This information security standard borrowed best practices from the payment brands' internal security programs to be unified under one coherent guideline which is called Payment Card Industry Data Security Standard.

The standard is now at its fourth reincarnation, version 2.0. The current version was preceded by version 1.0 which was published on December 2004; version 1.1 which was published on September 2006; version 1.2 which was published on October 2008 and version 2.0 which was published on October 2010.

Current version of the standard has more than 220 strict requirements. These requirements touch upon all major information security domains to include: network and infrastructure, configuration management, encryption and data protection, operating systems security, access rights, user identities, password management, physical security, audit management, security testing and policies and procedures.

The PCI standard and its enforcement issues are complex and have many facets. Starting with misrepresentation of some local acquiring banks of the global payment brands, through inadequate understanding of the standard by the enforcing parties and onward to corporate managements, which when kept in the dark are not quite sure how to bite this frog.

It has been known and it is still a known fact that acquiring banks across the globe (with the exception of the United States perhaps) are sometimes wary when trying to enforce the standard in their domestic environment. Moreover, it is even more complex when acquiring banks are required to enforce this standard and apply fines to some of its largest merchants that are typically responsible for generating a large percentage of those acquiring banks' revenue.

This article's purpose is to try and clear the fog and disperse the mist, if you'd like, so that corporate managements would be able to clearly see the path for compliance while identifying some of the obstacles, opportunities, challenges and projects that lie ahead.

Greatest Challenges for Meeting Compliancy

When facing with a compliancy project and organization may sometimes find itself at a lost. The lost feeling might be intensified when getting unclear deadlines and requirements by the local acquiring banks. However, not all challenges for meeting compliancy are external.

Firstly, most large corporations to include Banks, Retail chains, Telco companies, Insurance companies, eCommerce companies or any other merchant that deals with credit card information has a large cardholder data environment. This is mostly due to the fact that most organizations grew as time went by and so did their IT systems and applications. Therefore, it is not uncommon to find an organization that has web servers that inputs credit card information, internal database servers that store them, data warehouse application that stores and processes them, reporting applications that store and process them, clearing applications that transmit them, and antifraud applications that process and transmit them and so on.

It is to understand that the larger the cardholder data environment is, the more difficult it is to fully meet compliancy with PCI DSS. This is due to the fact that the standard requires changes to be made at all levels; stemming at the infrastructure level, operating system level, application level, network level, procedures level and so on. The wider the environment and the sample size are, the more difficult it is to meet PCI DSS requirements. For instance, not many organizations wish to undertake a security code review project on their core legacy applications that were written in COBOL.

It is also imperative to understand that PCI DSS is an annual and ongoing requirement. The larger the cardholder data environment is the harder and the more costly it is to maintain. Another main challenge when approaching a PCI DSS project is the fact that lack of full and total management approval is not always granted. In some organizations PCI DSS is perceived as a strategic goal and as a business enabler whereas in most organizations it is perceived as an unnecessary burden to be dealt with when it is absolutely necessary and not a minute sooner. This sometimes may lead to an unattainable deadline and subsequently to fines, penalties or other sanctions taken by the payment brands.

There are also those who wish that the local acquiring banks share the cost of becoming PCI DSS compliant. This article's writer would love to hear of such successful endeavors.

Third challenge that we may encounter when facing a PCI DSS compliancy project is the fact that the requirement to comply with PCI DSS may come in midyear, after budgetary framework has been decided upon and approved. This might delay any wishful attempts for PCI DSS compliancy until the next budget discussions set. This takes us back to the point on the domestic acquiring banks risk management programs. It is from personal experience alone and in this article's writer personal opinion that acquiring banks are sometimes digging their own graves. It has been demonstrated several times during the past years by acquiring banks that the requirements they stipulated to their merchants and service providers were those of minimal effort needed and not nearly adequate to allow these merchants and service providers' ample time and strategic planning for meeting with PCI DSS compliancy. For instance, if you are a large merchant that during the past two years has gotten used to getting quarterly letters politely asking you to complete an SAQ statement and to conduct quarterly scans and nothing more, imagine the shock when you suddenly get a letter requiring you to fully comply with PCI DSS and pass a PCI DSS audit by a certified QSA within a month.

Last challenge I will discuss within the confines of this article is the level of comprehension obtained by information security professionals in regards to this standard.

It is not uncommon by information security experts to misinterpret the standard. Most security professionals have some firm beliefs in regards to their own competency level at the various information security domains. As a result some will argue against some of the standard's requirements, some may design unneeded complex solutions or some might simply negate some basic requirements, thus misguiding the organization.

The simple, and to this writer's opinion, the only way for a successful PCI DSS project is to have a QSA on board during all crucial milestones in the decision making process and along the work plan's establishment process. Having a QSA on board will not only assure the organization that the road to compliance is clear, but it will also allow some transfer of responsibility and liability to another qualified factor.

Are there Magic Solutions?

The truthful answer is NO. That said, there are many best practices methods that allow a structured approach for a successful PCI DSS project and a successful audit. For instance, don't go out on a shopping frenzy of sexy technologies.

First, form an educated work plan to point exactly which technologies you need to support your business needs. DLP, NAC, SIEM/SOC, IDM, electronic vaults and more sounds really cool to have but they are not always necessary for meeting PCI DSS requirements, despite what some enthusiastic vendors might claim. All of these are excellent products to have and are very much needed in order to keep up a good security practice going on, but the choice whether to implement those or not shouldn't be only about PCI DSS but should derive from the organizational unified information security policies and business goals. Secondly, and before embarking on this voyage, choose your resources wisely and hire a QSA to partner up with you for the duration. Experienced QSA will guide the organization safely through risk based approach and will assist you in taking the right decisions.

Remember - compliance means that security becomes a fundamental perspective; therefore compliance should be maintained constantly. This realization needs to seep through all layers of the organization and to allow complete acceptance of this project and ample resources for dealing with the challenges that arise along the way.

Thirdly, make sure you guide the process and don't be guided by it or by external factors such as: exuberant vendors that are out to make a sale, local acquiring banks that only care about submitting nice and tidy excel sheets to their local payment brands or internal enthusiastic security staff that are harnessing the PCI DSS opportunity in order to promote other (and sometimes very important although not entirely PCI related) security agendas. Lastly, use the prioritized approach formal road map guide for managing your internal PCI DSS projects and to help you navigate the PCI DSS maze. The PCI SSC Prioritized approach presents a formal roadmap for managing the standard and its implementation the right way. It also directs the organization to work with risk base approach and addresses the most critical and burning issues first.

Scope Scope Scope (Reduction…)

PCI DSS is comprised of more than 200 requirements. Each and every requirement applies to each and every component that is included within the cardholder data environment. The math is simple – the more robust and complex your network AND the more you distribute credit card information among your IT systems and through network components, the more you grow in scope of PCI DSS audit. Try to do everything in your hands and reduce the business need to save credit card data, you can do it if you live by the motto "if you don't need it don't save it". Another way is to create network segmentation and to isolate the card holder data in separated, controlled and monitored environments.

In this writer's opinion, scope reduction workshops and discussions should be the first items on the discussion table whenever a PCI DSS compliancy projects sets off. It is imperative to gather the resources and skillful personnel from various business units and IT divisions in order to form an acceptable policy for cardholder data storage locations and transmission flows. For instance, you might discover that 6 first digits and last 4 digits plus another time stamp or transaction ID are sufficient for you to allow verifications, investigations and inquiries by your customers or merchants.

You might also discover that instead of storing full credit card number on your POS device you may only keep a salted hash value of your specific lists of cards (membership cards usually), for your local verification and authentication of the card. As salted hash values are not considered sensitive information by the PCI council's decree this might help you lessen the burden on your retail shops that have the main focus of ongoing operational work with minimal interference for the sake of all parties involve (no customer wants to have to wait too long in line).

Trends

In the spirit of scope reduction and magic solutions, we should consider the emerging trends that involve the PCI DSS and the payment industry as a whole.

Most trends as introduced by vendors or even by the payment brands have a twofold purpose – to minimize the burden on the merchant and to increase security level at the same time.

Tokenization

Tokenization is known as the practice of replacing the sensitive data in discussion, in our case – the PAN (Primary Account Number; usually 16 digits written on the face of the card) with another unique identifier which is not considered as sensitive.

Most tokenization products have two features that allow robustness and the ability to work in a cross platform environment.

The first is the ability to represent a replacement of the original string without affecting the data structure. This is achieved by generating a different 16 digits string that sometimes keeps the last four digits and first six digits. In any case this is mostly configurable.

The second important feature of most tokenization products is the external input form that allows all input of credit card information into a secured environment to begin with, thus negating the need to send sensitive data through a myriad of network components and participating applications. In many products this form can be integrated into any web based application and sometime to non-web applications as well.

EMV

The payment brands have announced an EMV rollout plan for various markets across the globe. EMV allows end to end encryption for the transaction from the moment the card is swiped and until the transaction is processed.

The introduction of end to end encryption with no decryption key along the process will also negate some if not many of the PCI DSS requirements. As this is not published yet by the PCI council, one can only speculate some less rigid requirements in chapter 3 that deals with encryption, chapter 10 that deals with auditing, chapter 6 that puts a large burden on most organizations and more. But again, at this point in time these are only speculations.

Secure Payment Devices

Although those types of solutions could not be used in all market segments, they are becoming increasingly popular among the retail chains. The reason being is simple and it is, of course, reduction of scope. When using a PTS device which has no connection to the network a retail chain might significantly reduce its PCI DSS burden. The same might be achieved by using tokenization services.

By properly implementing secure payment devices and organization might never send real PAN data through its IT environment.

Segmentation

The last trend or solution concept we will shortly discuss in this article is the issue of segmentation. It might be used for creating a minimal environment for credit card storage, processing or transmission.

Once properly established, an organization might realize that segmentation takes a lot of the burden off when implementing a PCI DSS compliance program.

How Do We Start?

Choose your help wisely. Whereas there are many excellent information security consultants out there, when it comes down to PCI you don't have to be the best security guy but rather you need to fully understand PCI DSS requirements.

Some companies that choose information security consultancy firms for helping with complying with PCI DSS find themselves tangled up after a few years of work only to find that the lead QSA of their current audit dismisses most baseline assumptions and integrated solutions already in place.

The PCI SSC recommends choosing a QSA to partner up with an organization that needs to meet PCI DSS compliancy for the entire process and not only for the audit. This way, the QSA shares some of the responsibility and will make sure you do not stray from the right path to compliance.

Pitfalls to Avoid

1. Tokenization does not make you compliant! You still need to implement all controls as required by the PCI DSS. If you plan your budget solely on tokenization solution you're in for a surprise as you will quickly learn that there is much more to do.
   Challenge every vendor that presents you with a magic box. Ask around, get recommendations, confer with colleagues and most importantly – authorized any solution with your QSA.
2. Encryption is not the only requirement in the standard. No, if you encrypt it does not mean you are compliant. There are still 219 more requirements you need to comply with.
3. No, you cannot choose not to encrypt your data just because you think it is hard or you think your access control system is unbreakable. It is not up to you to make that call and one solution that meets with a specific requirement cannot come instead of another requirement.
4. Purchasing an expensive suite of products will not make you compliant. You need to define your policies and make sure the products you purchase or integrate are in alignment with PCI DSS requirements.

Quick Wins

Start off with a business oriented Gap Analysis. Map all your data repositories and their corresponding business need. Identify all business processes that require credit card transaction, input, output, storage and transmission. Ask yourself and the relevant business owner whether some of the business processes can change to allow easier compliancy.

Use salted key hashed values for all matching functions for your customer's card.

Share your progress with your local acquiring banks. Ask for their advice and be transparent about the process.

Good luck in your PCI project!

The writer of this article is a QSA, PA QSA, CRISC qualified, and Co-Founder of GRSee Consulting, a QSA and PA QSA consulting group.

BEN BEN ADERET, QSA, PA QSA, CO-FOUNDER

With more than 12 years of experience in the field of information security as a consultant, project manager, product manager, group leader, and professional services manager, Ben is proud of his accomplishments with a number of financial, governmental, and Telco establishments in Israel as well as overseas. Before starting GRSee Consulting, Ben was a leading member in a small start-up company that produced GRC software applications and became known as the Professional Services division of GRSee Information Technologies. Ben is also highly skilled with UTM devices, routing technologies, and Firewall technologies.

GRSEE CONSULTING
Compliance . No Fuss

GRSee Consulting LTD

About us

GRSee Consulting is an innovative consulting firm with multifaceted expertise in all areas of information security including Governance, Risk Management, and Compliance.

GRSee is dedicated to the core values upon which the company was founded: to provide a high level of service that is professional, efficient, and prompt. All clients are greatly valued, and full customization of products can be designed in order to develop the best solution for every business need.

OUR Innovation

GRSee Consulting has developed a unique multi-regulation database to help businesses meet the various demands of regulators, legislators, and customers.

The company is proud to offer a complete range of consultancy services, plans for implementation, as well as full PCI Certification packages worldwide.

The Problem Businesses face

Despite the fact that information security has been a major concern for businesses for at least the last ten years, companies still find it difficult to stay current with the ever changing technology issues, new legislation, multi-regulations, and customer demands.

Even the best information security professional may find it quite difficult to keep up to date with the multi-regulations environment when attempting to understand which controls need to be met first, what risk factor is the most urgent for the business to deal with, which risk assessment to conduct at which time, and perhaps most importantly, how to govern the GRC process in an efficient manner.

GRSee Consulting Has the solution

By utilizing a multi-dimensional internal methodology, supported by tailor made professional services and software application tools, businesses are given the opportunity to view their organization on the whole as it navigates through the regulatory maze. Our team of experts will help you throughout every step of the process by using our own methodology for Governance, Risk management, and Compliance while keeping your precise business goals in focus at all times.

OUr Company and Market Status

Founded in 2009, GRSee has quickly risen to the top of its field and has gained recognition as the leading QSA and PA QSA in Israel. GRSee Consulting has established a diverse market presence since its inception, acquiring a long list of notable customers including Visa CAL, Yes Telecom, Mifaal Hapais, Ayalon Insurance, Retalix, Home Center, Bituach Yashir, AIG, Pelephone, Orbotech, Israir, Avis, and Sonol Petroleum, just to name a few. GRSee Consulting is proud to be perceived as the most professional Qualified Security Assessor and multi-regulatory consultant in Israel.

This level of success can be attributed to the MultiReg methodology that was developed by GRSee Consulting upon its foundation. All of our customers benefit from this unique approach when having to meet obligatory and non-binding regulations. The company is currently focused on enhancing the performance of this methodology within selected businesses, as well as expanding its services to selected companies in India.

The Grsee consulting Management TEAM

- **Ben Ben Aderet, QSA, PA QSA, Co-Founder** – With more than 12 years of experience in the field of information security as a consultant, project manager, product manager, group leader, and professional services manager, Ben is proud of his accomplishments with a number of financial, governmental, and Telco establishments in Israel as well as overseas. Before starting GRSee Consulting, Ben was a leading member in a small start-up company that produced GRC software applications and became known as the Professional Services division of GRSee Information Technologies. Ben is also highly skilled with UTM devices, routing technologies, and Firewall technologies.
- **Iftach Shapira, QSA, PA QSA, Co-Founder** – Iftach has more than 12 years of experience in the field of information security, of which, seven are in the areas of application security and secured architecture solutions. He is proud of his various accomplishments relating to complex architecture projects, as well as large scale security solutions. Iftach was the Chief Information Security Officer at Orbotech before co-founding GRSee Consulting. During this time he managed all daily information security activities as well as implemented state of the art technologies, completed internal audits, and oversaw SOX Compliancy projects. Iftach also worked as the head of Information Security for one of the top mobile and cellular communication companies in Israel, Pelephone, early in his career. This high level of skill and experience carries over today, as Iftach continues to specialize in security design and implementation, Microsoft development technologies, and secure architecture and design for a variety of software applications.

GRSee Consulting LTD.
www.grsee.co.il
Email: info@grsee.co.il
Tel: 972-52-3866591/972-54-2405700

PCI DSS at a Glance

In today's dynamic and continuously evolving business and IT environments, organisations strive to manage and respond to the ever increasing information security challenges. In the last decade however, an outburst of breaches has been recorded, the majority of which involved payment cards' data[1]. The breaches concern, not surprisingly enough, both card-present and card-not-present transactions.

In today's dynamic and continuously evolving business and IT environments, organisations strive to manage and respond to the ever increasing information security challenges. In the last decade however, an outburst of breaches has been recorded, the majority of which involved payment cards' data1. The breaches concern, not surprisingly enough, both card-present and card-not-present transactions.

In this context, the major payment brands, namely Visa International, MasterCard Worldwide, American Express, JCB and Discover Financial Services, formulated a strategic alliance and in 2004 launched the PCI Security Standards Council (PCI SSC) which is an open global forum for the on-going development, enhancement, storage, dissemination and implementation of security standards for account data protection. The mission of the PCI SSC is to enhance payment account security by fostering broad adoption of the PCI Security Standards[2]. While within the scope of the PCI SSC lies mainly the development and management of data security standards and related documents, the compliance tracking and enforcement of these standards lie with the payment brands which are also issuing several related mandates, including compliance deadlines.

PCI SSC identified the need to standardize security requirements on payment card transactions across all card brands since it was quite difficult or even daunting for merchants to become familiar with and adhere to different standards published by each individual payment brand. Moreover, as fraud losses were increasing, the card industry realised that the development and proliferation of consistent and well defined security standards was an absolute necessity. As a result the Payment Card Industry Data Security Standard (PCI DSS) was developed providing a detailed set of security best practices. PCI DSS is neither just a standard nor a regulation per se, even though there are state laws in the USA that are already in effect to force components of the PCI DSS into law[3]. Essentially, PCI DSS is a contractual agreement between card associations, the merchant banks, and the merchants.

Any entity wanting to accept credit or debit cards as a form of payment is required to contractually agree to comply with this standard and failure to comply can result in a variety of fines and, potentially, the loss of the right to accept payment cards at all. PCI DSS applies to merchants, processors, acquirers, issuers, and service providers. A service provider is a business entity directly involved in the processing, storage, transmission or switching of transaction data or cardholder data on behalf of other merchants or service providers. Service providers can be companies that provide services to merchants or other service providers or members that control or could impact the security of cardholder data. In the context of PCI a service provider could be a hosting provider, a managed security services provider, a payment gateway, a transaction processor, a payment application software developer, a call-centre or even a printing provider. The key to whether an entity needs to comply with the PCI DSS is whether they 'store, process, or transmit cardholder data' via any payment (acceptance) channel, including brick-and-mortar, mail, telephone, e-commerce.

PCI DSS is focusing on the protection of cardholder data, whether at store or in transit. Cardholder data include the debit, credit or pre-paid card Primary Account Number (PAN) alone or in conjunction with the expiration date, the cardholder name, or the service code. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment, they must be protected in accordance with all PCI DSS requirements except certain encryption requirements, which apply only to PAN. Sensitive Authentication Data are considered the Card Verification Values (CAV2/CVC2/CVV2/CID), PIN (Personal Identification Numbers) and PIN blocks, Track 1 and Track 2 Data (full magnetic stripe data or data equivalent on a chip). This type of data must not be stored post authorisation, even if encrypted[4].

Merchant Levels & Validation Requirements

Merchant and service provider levels are based on their annual transaction volume. The specific criteria for placement in merchant levels varies across the payment brands, however all merchants, regardless of level, must adhere to the PCI DSS requirements. The level into which a merchant or service provider is placed determines the PCI DSS compliance validation. The terms compliance and validation are not synonymous nor can they be used inter-changeably. Compliance is the process of implementing the security controls and policies required by the standard, while validation is the process of proving that an entity is compliant. Validation requirements might include an Annual On-Site Security Audit for Level 1 merchants (conducted by a Qualified Security Assessor), Annual Self-Assessment, and Quarterly Network Scans (performed by an Approved Scanning Vendor). It has to be noted that each payment brand has its own set of validation and reporting requirements. Besides the volume of annual transactions another criterion for placing a merchant to a certain level is whether they have suffered a security compromise.

Merchants Validation though Self-Assessment

The merchants' level is determined by the acquirer or directly by a payment brand in case the latter it is also an acquirer (e.g. AMEX). Resultantly, an organisation could be different levels

Table 1.

Level	American Express	Discover	JCB	MasterCard	Visa Inc.	Visa Europe
1	>2.5 million or deemed Level 1 by American Express	>6 million or deemed Level1 by Discover or required by another brand to validate and report as Level1	>1 million or compromised	>6million MasterCard & Maestro or compromised or deemed Level 1 by MasterCard or Visa	>6million (all channels) or global who deemed Level1 by any Visa region	>6million (all channels) or compromised
2	50,000 to 2.5 million	1 to 6 million or required by another brand to validate and report as Level2	<1 million	>1million and <= 6million MasterCard & Maestro Any merchant meeting the Level 2 criteria of Visa	1 to 6 million (all channels)	1 to 6million
3	<50,000	20,000 to 1 million card-not-present or required by another brand to validate and report as Level3	N/A	>20,000 and <= 1million MasterCard & Maestro e-commerce Any merchant meeting the Level 3 criteria of Visa	20,000 to 1 million Visa e-commerce	20,000 to 1million Visa e-commerce
4	N/A	All other merchants	N/A	All other merchants	<20,000 Visa e--commerce only and all other up to 1 million	<20,000 Visa e--commerce only and all other up to 1 million

Table 2.

Level	American Express	Discover	JCB	MasterCard	Visa
1	Annual onsite assessment by QSA or internal auditor * Quarterly ASV network scan	Annual onsite assessment by QSA or merchant's Internal auditor Quarterly ASV network scan	Annual onsite assessment by QSA Quarterly ASV network scans	Annual onsite assessment by QSA Quarterly network scan by ASV	Annual onsite assessment by QSA Quarterly network scans by ASV Attestation of Compliance form
2	EU ONLY : Annual SAQ Quarterly ASV network scan	Annual SAQ Quarterly ASV network scan	Annual SAQ Quarterly ASV network scan	Annual onsite assessment by QSA Quarterly network scan by ASV	Annual SAQ Quarterly network scan by ASV Attestation of Compliance form
3	EU ONLY : SAQ Quarterly ASV network scan (both recommended)	Annual SAQ Quarterly ASV network scan	N/A	Annual SAQ Quarterly network scan by ASV	Annual SAQ Quarterly network scan by ASV Visa Europe: either complete annual SAQ and quarterly network scans OR use PCI DSS certified Payment Service Providers for all payment processing, storage and transmission
4	N/A	Compliance Validation requirements determined by acquirer. Recommended validation: Annual SAQ Quarterly ASV network scan	N/A	Compliance Validation is at discretion of acquirer. To validate: Annual SAQ Quarterly ASV network scan	Annual SAQ Quarterly network scan by ASV recommended Compliance validation requirements set by acquirer

for different payment brands. Service providers' level can be determined by multiple entities. When involved in transaction authorisation, payment brands can easily tell by simply counting the number of transactions. When not involved in transaction authorisation their customer may dictate their level. A merchant's transaction volume is determined by each acquirer and is based on the aggregate number of transactions from a 'Doing Business As' (DBA), or a chain of stores (not a corporation that has several chains)[5] (Table 1).

The table below depicts Merchant Levels per payment brand (Table 2).

Merchants Validation though Self-Assessment

Merchants eligible to complete an SAQ need to choose one of the five SAQ types based on the various methods they use to process payment cards. The table below describes briefly the different SAQ categories[6] (Table 3).

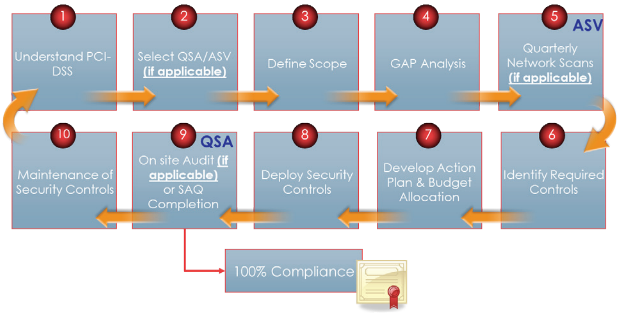
The SAQs are essentially subsets of the entirety of the PCI DSS standard requirements.

PCI DSS Goals & Requirements

The standard addresses a comprehensive list of information security aspects including operational, management, and technical control measures. It has six goals and 12 requirements which specify a framework for a secure payments environment (Table 4).

The Compliance Process

The diagram shown below depicts the major milestones an entity has to complete in order to achieve and maintain compliance.


1
Understand PCI-DSS
2
Select QSA/ASV (if applicable)
3
Define Scope
4
GAP Analysis
5
ASV
Quarterly Network Scans (if applicable)
6
Identify Required Controls
7
Develop Action Plan & Budget Allocation
8
Deploy Security Controls
9
QSA
On site Audit (if applicable) or SAQ Completion
10
Maintenance of Security Controls
100% Compliance

The Compliance Process

The diagram shown below depicts the major milestones an entity has to complete in order to achieve and maintain compliance.

The PCI SSC has developed a Prioritized Approach providing a roadmap of compliance activities based on risk associated with storing, processing, and / or transmitting cardholder data. The roadmap helps to prioritize efforts to achieve compliance, establish milestones, lowers the risk of cardholder data breaches sooner in the compliance process, and help acquiring banks objectively measure its compliance activities. The Prioritized Approach was developed after factoring data from actual breaches, and feedback from qualified security assessors, forensic investigators, and the PCI Security Standards Council Board of Advisors[7]. The six milestones of the approach are as follows:

- Milestone 1: If you don't need it, don't store it: Remove sensitive authentication data and limit data retention. If sensitive authentication data and other cardholder data had

Table 3.

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial- out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.

Table 4.

Goal	Requirement
Build and Maintain a Secure Network	Install and maintain a firewall configuration to protect cardholder data Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	Protect stored data Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	Use and regularly update anti-virus software Develop and maintain secure systems and applications
Implement Strong Access Control Measures	Restrict access to cardholder data by business need-to-know Assign a unique ID to each person with computer access Restrict physical access to cardholder data
Regularly Monitor and Test Networks	Track and monitor all access to network resources and cardholder data Regularly test security systems and processes
Maintain an Information Security Policy	Maintain a policy that addresses information security

not been stored, the effects of the compromise would have been greatly reduced.

- Milestone 2: Secure the perimeter: Protect the perimeter, internal, and wireless networks. This milestone targets a key area that represents the point of access for most compromises: vulnerabilities in networks or at wireless access points.
- Milestone 3: Secure applications: This milestone focuses on applications, as well as application processes and application servers, since application weaknesses are a key access point used to compromise systems and obtain access to cardholder data.
- Milestone 4: Control access to your systems: Protect CDE through monitoring and access control since this is the key method to detect access to your network (who, what, when and how).
- Milestone 5: Protect stored cardholder data: For those organizations that have analyzed their business processes and determined that they must store PAN, Milestone Five targets key protection mechanisms for that stored data.
- Milestone 6: Finalize remaining compliance efforts, and ensure all controls are in place: Complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment

Security practices and technical solutions

PCI DSS requirements refer to both procedural and technical controls, the distinct components of which can be summarised in the list below (Table 5).

A further analysis will be provided for some of the security practices and technical solutions required to meet the intent of the respective PCI DSS requirements.

Firewalling / UTM Solution: Firewalls operate as both a 1st level proactive countermeasure to protect from intrusions, by minimising the exposed services of protected systems, as well as a 2nd level countermeasure against the escalation of successful intrusions by controlling server-to-server communications. Additionally, firewalls nowadays are becoming “Unified Threat Management” systems, integrating functionalities, such as Network IPS, etc. and thus providing another “generic-level” of protection. In the context of PCI, firewalls that protect the cardholder environment should be configured in order to restrict connections between untrusted networks (e.g. internet) and any system components of the CDE. In that configuration context the firewall should limit inbound & outbound traffic only to that which is necessary for the cardholder data environment. In addition to that, all other inbound and outbound traffic should be specifically denied, for example by using an explicit “deny all” or an implicit deny after an allow statement.

Strictly speaking network segmentation is only a requirement in order to separate any untrusted external network, with the internal CDE, and internet facing CDE system components from other irrelevant internet facing information systems. In that context the standard requires that any database server(s) that store, process and transmit cardholder data should be installed in the internal network, which should be properly segregated from the DMZ.

Regardless the aforementioned, an alternative would be to proceed with an internal network segmentation project, in order to minimize the CDE scope. A proper segmentation strategy would entail:

- the identification of every CDE system component
- the discovery of the CDE required network traffic
- the identification of the user base that requires access to the CDE
- the aggregation of the above, in order to design the segmented CDE.

Table 5.

PCI DSS Control Components	
Change & Configuration Management	Vulnerability Management
Network Mapping	Web Application Security
Firewalling / UTM	Strong Authentication
Security Roles & Responsibilities	Physical Access Monitoring and Controlling
Security Operations	Media Handling
Endpoint Security	Security Monitoring & Log Management
Encryption	File Integrity Monitoring
Data Retention	Penetration Testing
Prohibited Data Storage	Security Policies & Procedures
Data Leak Prevention	Security Awareness
Identity & Access Management	Incidence Response
Key Management	Privileged Account Management
Patch Management	Secure Code Development

Furthermore, CDE reduction may be accomplished by removing cardholder data from information systems which do not need to process, transmit and / or store them. Finally, for any information system which has to communicate with system components of the CDE and therefore be part of it, but not for CHD processing, transmission or storing, the introduction of an intermediate system, such as a terminal server and / or an application middleware component, combined with the implementation of a CHD truncation solution, would effectively permit the information systems to continue their normal business operation, whilst are removed from the CDE.

The network should be segmented with the support of network stateful inspection firewalls and this fact may lead to "heavy" IP reengineering. A way to avoid this daunting task is the installation of contemporary layer 2 firewall(s), which is/are installed without an IP address, inline between two or more IP networks, in order to inspect, permit, prohibit and in general manage the transiting network traffic, in accordance with the predefined firewall ruleset and policy. Moreover, these firewall systems provide advanced IDS/IPS capabilities, satisfying this way the PCI DSS requirement 11.4.

Moreover, a wireless device (known or unknown) could pose a potential threat to the CDE. In that context perimeter firewalls should be installed and deny any traffic, allowing only that which is necessary for the cardholder data environment.

Critical Servers & Endpoint Security: Achieving total protection for the critical corporate severs is not a matter of a single solution deployment. A combination of specialised security controls is required for that purpose. Having said that, covering the server protection requirements of the CDE includes the following security solutions:

- Network IPS, providing the necessary protection to the corporate servers from network threats and attacks
- Advanced antimalware protection & Host IPS
- Full audit and control of changes and compliance monitoring

From an endpoint perspective, every PC accessing an enterprise network is a target for rapidly proliferating worms, penetration attacks, Trojan horses, spyware, and other exploits. The deployment of an advanced endpoint security solution safeguards the enterprise network from penetration by malicious code or targeted attacks with a combination of proactive protection for every network endpoint along with central policy management and enforcement. The security benefits for the internal network by the deployment of such solution are:

- Proactive endpoint security
- Assured access policy enforcement
- Easy and flexible central management
- Total access protection

The specific control plays the main role regarding endpoint security, as it centrally enforces and manages the appropriate desktop firewall rules and other client workstation controls in accordance to the defined internal network security policy-standard. Endpoint Security system secures all internal network endpoints by centrally managing proactive defences and enforcing policy compliance. It assures that a PC is running updated antivirus, has critical patches and service packs installed, has the latest versions of applications such as browsers and VPN clients, is not running any prohibited programs, and meets other trust criteria before it gains authorized access to the network.

Privileged Account Management: The purpose of implementing the specific security system in the internal network is the secure storage, distribution and use of the administration passwords by the IT administrators so that the privileged access to corporate IT resources is effectively controlled. More specifically the system should meet the following security requirements:

Enforcement of a strict security policy for the administration passwords confronting some major security issues such as:

- Use of same password from multiple administrators (password sharing)
- Use of the same password to multiple systems
- Lost or forgotten passwords etc.
- Central management and secure storage of the critical admin passwords into a special protected system instead of the administrator's workstations
- Secure distribution of the administration passwords to the authorized users, over encrypted connections
- Required authorization prior to the provision of an administration password (in combination with user authentication)
- Detailed logging of the password request procedure including the personal details of the user that the password was provided
- Automated change of the administration passwords on the selected systems in specific time intervals or after every usage

Web Application Security: Web applications are an excellent means to provide access to data; however, they are not risk-free. A Web-application firewall could be installed in front of any public facing web application, in order to filter and block non-essential & malicious traffic at the web application layer. The firewall protects custom Web application code against attacks such as SQL injection, cookie poisoning, parameter tampering, directory traversal, etc. The provided dynamic profiling automatically creates a dynamic positive security model of Web application usage dynamics and application structure, including URLs, http methods, parameters, hidden fields, cookies, session IDs, and response codes. As users interact with the application, the web firewall closely monitors their activities and compares them to the profile. Any attack attempt is detected and (optionally) blocked.

The PCI DSS requirement for reviewing applications or installing web-application firewalls is intended to greatly reduce the number of compromises on public-facing web applications that result in breaches of cardholder data.

Data Leak Prevention: One of the issues facing global companies is how to effectively share with, and allow the usage of confidential and proprietary information, by colleagues and trading partners, whilst remaining in control of the information, both internally and externally. To address this, well-governed companies have implemented the appropriate policies and procedures to comply with regulatory and business requirements. However, monitoring, auditing, and controlling of information usage - at the point of use, is the only way to protect, control and understand the usage of your proprietary information. Some basic tasks that need to be facilitated by a Data Leakage Prevention solution are the following:

- Detecting the information leakage and suspicious activity from PCs, Laptops and other endpoints without human intervention.

- Preventing data leakage by defining and enforcing endpoint security policies to selected endpoints.
- Producing the proper information for investigations assistance.

A data leak prevention solution may be employed to mask, log, encrypt and in general control how cardholder data is used by trusted end users. The data masking specifically provides a complete audit capability for all user activities as well as field level data masking or redaction. In addition to that the solution captures a concise audit trail of user interactions with applications and data and applies pre-defined rules in real-time to ensure that data use is appropriate. The DLP prevents data loss at the point of use, meaning the end-user's environment, as a result of "hard to detect" user actions such as: illicit copying to CD (or USB device), printing, network transfer, or the personal e-mailing of sensitive files and other data.

Security Event/Information Management System: Although many systems provide valuable information about the security state of the IT environment, they also provide a high volume of events and at the same time without consolidating, normalising and correlating them, we are not capable to obtain a holistic view of the security state. For this reason security event management systems that are able to consolidate logs from various sources, filter and correlate them, should be deployed, in order to acquire a holistic and of better value view of the security state of the monitored environment.

It must be noted that a SEM system is not a point-solution and must be regarded as a corporate-wide infrastructure. For this reason the selection of such a system should take into account the whole corporate IT environment. The deployment and configuration of these systems should follow the principles illustrated below:

- Ability to gather security-relevant events from a wide variety of sources and not only security systems, such as databases, web servers, etc.
- Ability to pre-filter data prior or upon gathering, in order to minimise network overheads and information overload, which would make difficult the analysis of the events.
- Ability to correlate events gathered in order to be able to minimise false positives and detect real security incidents.
- Hierarchal architecture, in order to be able to scale for large deployments, and thus to minimise network overheads and expand accordingly to business needs.

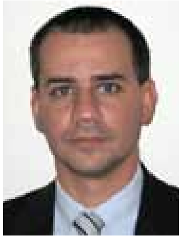
Configuration Audit & Control / File Integrity Monitoring: In short, configuration audit and control is the process of establishing that infrastructure components are maintained in a known and trusted state. This is done by ensuring all changes are detected and analysed to verify the change was authorized and the updated system still complies with organizational and regulatory standards. Defining IT configurations and identifying a process for change is insufficient for maintaining control of today's dynamic environments that are affected by interaction from a variety of sources. Patches are automatically installed, application upgrades occur, and users manually alter established system settings outside the bounds of a predetermined IT policy. IT and Security managers alike need to be certain their environments simultaneously maintain operational efficiency and conform to accepted compliance and security standards. Unfortunately, today's IT service stacks are too complex to manage by purely manual methods, and so a gap has been created between Change and Configuration Management requirements and IT operation's ability to meet those needs. Configuration Audit and Control fills this gap in IT enterprise management by providing the tools necessary to collect accurate configuration data, monitor change in real time, promptly remediate problems, and ensure a stable and productive IT service stack.

The control of user access on the critical systems can be significantly enhanced by the deployment of an advanced configuration audit and control mechanism which enables continuous monitoring of any changes performed on the critical servers at the OS, files system, database and application level, as well as to network and firewall devices, in the course of authorized user access session. The solution provides a single point of configuration audit and control across the enterprise. By maintaining configuration baselines for current and past versions, the solution can detect any change or nonconforming configuration for every system it monitors. When a change is detected, the system collects detailed change information, compares the change against known and authorized changes, and if unauthorized, notifies designated staff to initiate investigation.

Vulnerability Management: A vulnerability scanning solution may be used to discover, enumerate, analyse and evaluate known technical vulnerabilities in information systems, computer networks and applications. Internal vulnerability scanning should be conducted in a quarterly fashion and after any significant change in the CDE system components.

Remote Access: Remote access in the CDE system components should be provided to employees, administrators and third parties, via the employment of two factor authentication (e.g. something you have and something you know). An advanced two factor authentication solution is comprised from an infrastructure system and OTP tokens, that operating in concert; change automatically the remote access user's password every 60 seconds.

Advance remote access technologies have been developed allowing for the extension of an organisation's internal infrastructure to the Internet by utilising VPN technologies such as IPSec, SSL VPN, L2TP over IPSec etc. Each technology provides the required security and features depending on the nature of the remote connection.



MR DIMITRIS ERGAZAKIS

Has been working in the IT field for more than eleven years, specifically in the fields of IT auditing & Risk Consulting with Deloitte & Touché, ERP Implementation with LogicDIS and Information Security with ENCODE SA, where he currently serves as a Manager in the Security Strategy Services Practice.

He holds a M.Sc. in Analysis, Design & Management of Information Systems from the London School of Economics and a B.Sc. in Applied Informatics from the University of Macedonia, Greece. He also holds numerous professional certifications, namely: PMP, CISSP, CISA, CISM, CGEIT, PCI DSS Qualified Security Assessor (QSA), ISO27001 Lead Auditor and ITIL Foundation Certificate in IT Service Management.

[1] *Verizon Business: 2009 Data Breach Investigations Report*
[2] *https://www.pcisecuritystandards.org/*
[3] *http://www.pcicomplianceguide.org/security-tips-20090227-pci-compliance-law.php*
[4] *Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Ver 2.0, Oct 2010*
[5] *PCI SSC – QSA Certification Training*
[6] *Payment Card Industry (PCI) Data Security Standard, Self-Assessment Questionnaire Instructions and Guidelines, Ver 2.0, Oct. 2010*
[7] *PCI SSC – The Prioritized Approach to Pursue PCI DSS Compliance*

WikiLeaks, Compliance and Global Competitiveness

Reasons to Review Your DLP Strategy

WikiLeaks has dominated the news recently with its threats to expose confidential documents from some of the world's major corporations. Many businesses are seriously evaluating their data protection strategies, and security vendors are seeing a huge increase in requests for risk assessments.

The recent data leaks publicized by WikiLeaks and others often evoke a response along the lines of, "I need not worry. My company does not handle government cables or diplomatic documents. I'm not a high-profile company, and am not a WikiLeaks target." This view misses the point. WikiLeaks is broadly relevant not because a particular company might be a "target", but rather, because of how the leak occurred.

WikiLeaks was a result of a privileged insider copying data that they had legitimate access to as part of their job. All companies have such insiders, regardless of their product or service. In fact, studies show that the overwhelming source of data loss is in fact insiders. People on your payroll. Wearing your badge. More often than not, these data losses are not malicious, but a result of negligence. After all, security is someone else's job.

While data breaches can't be eliminated completely, organizations can greatly reduce the risks associated with confidential data leaving their organizations. Organizations are looking for a way to monitor the movement of sensitive information and stop users from emailing sensitive documents, printing, copying information to removable devices or posting via instant messages. All these things (and many more) can be controlled and monitored using Data Loss Prevention (DLP) solutions.

Software installed on users' machines can monitor and protect them from accidentally leaking information; being able to affirm a user's intention to share confidential data prior to allowing it to be sent. There are also appliances that can be installed on the network that record and classify everything that goes over the Internet, and there are devices that can mine stored structured and unstructured data so organizations can search and discover where data is kept.

Traditionally, an organization would need to have up-front knowledge about the data and its use, so that IT could look for communications anomalies. But this approach is fundamentally flawed, as it requires organizations to anticipate, in advance, where and how the data loss will take place – something that is nearly impossible except in the simplest cases of credit card data or Social Security numbers (which should never leave). Technology can now allow organizations to answer, after the fact, questions such as these as well as help an organization define business processes that can then be enforced through solutions. Once the anomalies have been found, they can be remediated using technologies such as encryption, enterprise digital rights management, user education, or requiring manager approval.

Mobility continues to empower and enable workforces to accomplish more than ever, and this trend is only increasing. Simultaneously, social media channels are of growing interest for businesses to leverage. These two forces represent an astronomical increase in the level of risk organizations face with regard to leaked data. This rapidly increasing risk coupled with an organization's need to share critical data with key partners renders the traditional approach of employing moats and walls incompatible.

Positively identifying that a data leak has in fact happened is step one, but what is step two? Businesses need to be able to answer questions surrounding the who, when and how did that information leak.

Beyond Regulatory Compliance

The initial drive and adoption of DLP and other data protection technologies was on the back of U.S. state data breach notification laws in conjunction with industry/government regulations like SOX, HIPAA, PCI and ITAR. Regulatory approaches such as HIPAA HITECH and state privacy acts have been pivotal in ensuring organizations report breaches of personal identifiable data. These have provisions for external whistle blowers and agencies that ensure there is a threat in the case an organization does not properly disclose.

If you look at HIPAA prior to the recent enhancements part of HITECH, you will recall that enforcements were loose, and the impacts of breaches were unclear. When the HITECH act was completed the changes in health care organizations behaviors were significant. Now organizations faced fines when there was a breach and the costs increased if an external whistleblower reported the event. The Massachusetts Privacy Act is a good example of tying monetary costs to breaches.

Data breach information sources such as Verizon's 2011 Data Breach Investigations report <http://newscenter.verizon.com/press-releases/verizon/2011/verizon-2011-data-breach.html> or datalossdb.org<http://datalossdb.org> provide an opportunity to gain insights into the depth of problem (like turning a light on in a dark cave), but the key challenge is to create teeth to change corporate behavior and improve protections. Verizon's report is a good step towards shedding light on the problem, now we need enforcement to cause action.

Today a public company can lose a top-secret recipe, a go-to-market plan or other key piece of sensitive data and they are not required to report it. Some organizations recognize the threat and have taken proactive steps to prevent this from happening however many others don't take steps because there is no forcing function. Wall Street should demand that companies certify that none of their sensitive data was lost when completing financial reports. This would increase the visibility of the issue and get proper executive commitment to solve the challenge.

Corporations today are required to report events that are "material". General agreement exists around the concept that entities have an ongoing obligation to disclose information that would be material to an investor's investment decision. This would appear to be sensible, as the loss of critical sensitive data could result in disastrous market consequences. Consider hypothetical examples such as:

- design documents securely sent to an offshore manufacturing facility, are careless stored by the recipient and stolen off of the unprotected endpoint. If counterfeit goods arrive in market prior to the availability of legitimate product, months, if not years, of corporate product development investment could be nullified;
- upcoming pricing changes for a company's goods and services are prematurely disclosed. This situation often causes forecasted business to "stall" while waiting for lower, more attractive pricing eventually resulting in the quarterly revenue forecast not being met;
- a pharmaceutical company's clinical drug trial information is inappropriately leaked. If interpreted by the market out of context it would cause the firm's share price to plummet;
- marketing launch plans for an upcoming revolutionary mobile product are leaked. If made public, these plans could prematurely inform and influence competitors, and diminish the firm's ability to maximize the effectiveness of the launch.

Clearly the more attractive approach, especially from a financial and reputational perspective, is to prevent such leaks from happening in the first place rather than worry about what and how to disclose. Modern management teams insist on having the most current, up-to-date, and complete data regarding their business. The best decisions are informed ones; risk can only be properly assessed when there is knowledge.

Global Competitiveness and the Threat of Data Loss

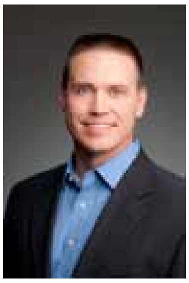
All organizations are increasingly conducting business in a global theatre, resulting in the presence of sensitive data being scattered throughout. Trying to locate information is like trying to drill an oil well without a geological map of what lays below the surface, likely resulting in failure. Traditional DLP asserts that you must have this map prior to drilling, and hence these projects begin with a tough, if not impossible, challenge to overcome. We see the market very differently and believe in enabling education through mapping business processes, and focusing on data protection efforts on demonstrably high-priority areas.

Data protection also acts as a business enabler. When data is properly protected, opportunities become available that would otherwise be XXX. For example, leveraging cloud infrastructures can be done with confidence when your data is protected before it leaves your premises. Doing business in a new, far-flung geography is less risky when you can ensure that your sensitive data remains yours and yours alone.

Today, organizations are looking beyond "check-the-box" compliance, and looking to protect more sensitive data - data like design documents, schematics, product launch plans, pharmaceutical formulas, etc. These types of documents are much more complex than simple Social Security numbers or credit card numbers, and as such, traditional DLP solutions tend to not be as effective in identifying this data.

Data leads an organic and unpredictable life. Imagine how many people an organization shares data with on an upcoming smartphone design. Now consider that each person with access to the data could modify the data creating a new instance of it and even re-share it with someone else, thus making it next to impossible to predict where it ends up. Safeguarding and protecting this type of sensitive data and its use is all about understanding business processes, which is orthogonal to organizations charged with protecting data (InfoSec). McAfee has an approach that bridges this gap by enabling organizations to discover how business processes are actually used in the wild versus how they were designed. This knowledge effectively facilitates the alignment of purpose for these typically orthogonal groups.

While no single technology, DLP included, provides 100% protection against leaking data, experience tells us that most leaks happen through traditional channels that can be easily controlled. Data Loss Prevention can provide your business with the insight needed to make informed decisions, not just about data protection, but data usage and business process. We expect that DLP features and functionality will continue to permeate the fabric of data protection technology, and provide increasing value to those businesses who adopt it.



JOHN DASHER, SENIOR DIRECTOR, PRODUCT MARKETING

Mr. Dasher brings more than 25 years of technology marketing and development experience to McAfee, where he is responsible for Product Marketing for the Data Protection Business unit. Most recently, he served as PGP Corporation's Director of Product Marketing and Product Management. Prior to PGP, Mr. Dasher was Director of Business Development & New Products for FileMaker, Inc. (a wholly owned subsidiary of Apple Computer), with responsibility for all aspects of FileMaker's applications business, held senior marketing and development management positions at Ventro (the first venture-funded business-to-business e-commerce marketplace) and Xerox's Internet & Software Solutions organization. He co-founded and was Vice President of Engineering for Verano, an enterprise content management and supply chain management software startup. Previously, he spent 12 years at Apple Computer, playing a key role in the development of its standard-setting PowerBook products and making significant contributions to its award-winning imaging products. Mr. Dasher also founded and managed Fifth Wave, a software development company. He holds a patent on multi-platform search (U.S. patent number 6,055,543) and has a B.A. from the University of San Diego.

Virtual Crime in the Real World

We live in an environment that is encapsulated by two worlds; the real world and the cyber world. In the real world dangers lurk around every corner and many people are very aware of the possibilities and the harm that can be caused. The everyday stresses and pressures lead people to seek solace in a place they can manipulate and control. This solace comes in the form of the internet and all the services the digital world can offer.

Is the digital world safe?

However, the digital world isn't as safe as it first seems. The alluring world may provide comfort and flexibility to the user's needs but it is just as dangerous if not more so than the real world today.

The dangers in the real world seem threatening because they can endanger you physically, mentally and in the worst scenario can terminate your life. Although cybercrime does not come in the form of bullets or knives it can be just as deadly when your life is still at risk.

Identity theft is one of the most frequent crimes that occur on the internet, cybercriminals build up a profile of a user's character and habits then use those to transform themselves into the person. Payment details are stolen using man in the middle attacks and accounts such as e-mail and social networking are locked and controlled by the new user. Many people's first response would be not to worry because what happens on the internet cannot be transferred into the real world but those details can be used to obtain bank accounts, personal lending such as credit cards and mortgages, birth certificates and passports. All these details could enable a cybercriminal to transfer your digital fingerprint onto someone else in the real world.

The previously mentioned man in the middle attack is a process whereby if a user inputs information on an unsecure connection the information could be intercepted and stolen without the user's knowledge. Most websites have trusted signs and securely signed logos which identify that the website enters an encrypted channel when handling sensitive information. However there are websites which don't have trusted signs and when entering an unsecure connection there are risks that the information can be stolen.

Cyber criminals are becoming more sophisticated and continue to develop malicious software and devise improved methods for infecting computer and networks. This is not confined to the advances in technology, the criminals are also refining their social engineering techniques to improve infection rates and continually adapt their tactics as new defences are implemented in order to serve the illicit market in compromised private data. The infection of personal computers does not only have the effect of the owner losing their online identity, it can also then be used in conjunction with tens of thousands of other computers to mount an attack on industries or the national infrastructure.Child Sex offenders have also adapted to the growth of computing technology, the internet and other digital mediums i.e. Digital camcorders, and are not only reacting to the youth of today being more easily contacted via site such as FACEBOOK or MYSPACE, and that they are not aware or worried about the risk that could come of using such site, but also becoming active creators and distributors of content over the world wide web.

Crimes and technology

There is a wide range of offences that can be committed through communication technology. Cyber-crimes are commonly considered as falling into one of twocategories:

1. New offences committed using new technologies, such as offencesagainst computer systems and data, dealt with in the Computer Misuse Act 1990. Such as hacking or breaking into computer systems to steal or alter data.
2. Old offences committed using new technology, where networked computersand other devices are used to facilitate the commission of an offence. Crimes such as the transfer of illegal images or fraud.

Even though the offenses break down into two categories the three main cyber-crimes we hear about are; ID theft, pornography (especially child pornography & paedophilia) and fraud. Each cyber-crime has its scales of severity similar to 'traditional crimes'. The punishment for cyber-crimes aren't deemed as strict as the punishment for traditional crimes. There is next to no legislation on cyber-crimes besides the Computer Misuse Act 1990 which means that Judges don't have a guide for their rulings. Any actions should be legal or illegal according to their merits, rather than the medium used so that what is illegal offline should be illegal online.

The internet and crime

Cyber criminals can operate from anywhere in the world, targeting largenumbers of people or businesses across international boundaries, and there arechallenges posed by the scale and volume of the crimes, the technical complexityof identifying the perpetrators as well as the need to work internationally to bringthem to justice. The internet opens up new opportunities to cyber criminals andenables aspiring criminals to enter the environment; based on a belief that lawenforcement struggles to operate in the online world.

From a child protection perspective a key issue facing law enforcement is not simplythe volume of child sexual abuse material that is being circulated, but the ease bywhich this medium offers child sexual predators the opportunity to network witheach other to create and distribute content.

While the offence committed may be recognisable, cyber-crime poses a number of significant difficulties for traditional policing across all types of crime committed on the internet.

Not only are criminals making or developing their own tools, but they also uselegitimate or publicly available software, such as peer to peer network toshare files and illegal images.The nature of the internet not only allows criminals to be located in a differentcountry to the victim, but they can target many thousands of victims at once. Aphishing e-mail can be sent easily to hundreds of thousands of people from onecomputer, and a single person can infect many computers with malicious software.

A major concern with regard to cyber-crime is the lack ofaccurate information relating to the scale and scope of crimes committed throughthe medium, which makes it difficult to identify what action should be taken in response.

Can the internet be policed?

Policing the internet isn't as easy as policing the streets. If there has been a crime on the streets you can secure the area and make sure that no one enters or leaves the crime scene and causes something to be changed but on the internet it isn't that easy. There aren't many ways in which the 'area' the crime occurred in can be controlled. The internet spreads like wildfire; thousands of new websites are being created and deleted everyday overwriting old data and old files relating to the websites.

Policing and controlling cyber-crimes are causing great concern and if boundaries are not put in place soon then the internet could change the way the virtual world operates. Will anyone ever feel safe if they don't know what they can or cannot trust?

There are several websites, restrictions and operations in place to keep everyone safe online and to keep everyone's private information such as payment and banking information but the main message is to remember that not everything is as it first appears.

One of the most recent cyber attacks took place at the start of May with the Sony Playstation network being taken down following an external intrusion. The system remained down for 5 days and over 77 million user's accounts had their details removed despite Sony stating they are kept encrypted.

This theft of the data included names, addresses, date of births, email addresses and login details along with the credit card details stored. Sony assured its user's that the credit card payment details were not accessed and that their payment details were still safe.

This cybercrime spread across the media like wildfire and Sony's reputation has been damaged due to their inability to keep their system secure.

It has been claimed that the attack was made from a rented server from Amazon's EC2 service cloud; the cyber criminals launched the attack from the cloud and penetrated the popular network. False information was supplied to Amazon in an attempt to create an account when using the rental server. Neither Sony nor Amazon has commented on these claims.

If these claims are true it wouldn't be the first time that the cloud has been used to perform an attack. Thomas Roth (a German security officer) earlier in 2011 showed how tapping the EC2 service allowed him to crack Wi-Fi passwords in the fraction of a time and a fraction of a cost using his own computing equipment. The attack cost him $1.68 he used 'Cluster GPU instances' of the Amazon cloud to carry out brute-force cracks that allowed him to access a WPA-PSK protected network in 20minutes.

Although Cloud Computing is a development that is allowing people to harness computing power for research and to emphasise projects it also has a malicious side whereby the power can be harnessed and used in an inappropriate matter.

New developments will be created every few days or weeks with the internet developing so strongly but how many of them will be used maliciously? If there is a way in which it can be done, someone will figure it out and test it to see how much the boundaries can handle.

Many users are worried about their details and how they have now been compromised because of the Sony attack. Sony has offered customers a free year of identity theft protection to try and limit the damage this could cause but unfortunately the effects of cybercrime last much more than a year and whether their information will continue to be monitored after a year is unknown.

Why only an estimated cost of cyber-crime?

In the UK the Government has estimated that Cyber Crime costs the economy £27 billion per year. However this figure seems fairly small and it is presumed that this is based on the cases that have been reported as many companies won't report cyber crimes because they fear about how their reputations will be affected.

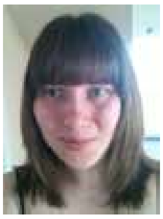
The report from the Office of Cyber Security and Information Assurance (OCSIA) and security consultancy Detica said businesses were losing £21 billion a year mainly through IP theft and industrial espionage in the form of cyber crime.

Unfortunately accurate figures cannot be created if companies and people who have been affected by cyber crime do not step forward and get their cases recorded. It can be done online, by telephone and by visiting an authority member. Whatever method the user finds most comfortable is available.

As previously stated companies feel reluctant to report cybercrimes that have occurred within their businesses as they feel this could ultimately damage their reputations and reveal their vulnerabilities. Hopefully this issue is about the change due to a group of lawyers including Jay Rockefeller (a powerful chairman on the Senate Commerce Committee) has put forward a letter to the SEC who will compel companies to raise all cyber-crime issues no matter how big or small. The SEC committee (Securities and Exchange Commission) are a U.S. department. This does mean that unfortunately at the moment there is no UK legislation going under way but hopefully this matter will be changed shortly as we hopefully follow in U.S. footsteps towards protecting people and companies against cyber-crimes.

Everyone is focused on the big scale cyber-crimes, all the dangers that everyone reads about frequently and hears about. However is any one actually prepared for the smaller problems? We are all worried about identity theft and protecting our identity which is very important but what about protecting others identity and the confidential data they store? Virus' aren't deemed that serious nowadays because they are seen as more of a nuisance than malicious but virus' come in many forms and can have an underlying threat which whilst your disabling the virus will be causing harm or collecting information regarding your profile or bank details.

When it comes to cybercrime, we are caught between a rock and a hard place. Making our systems tough enough to thwart the criminals would not just be vastly expensive, but could render many daily actions and transactions exasperatingly difficult and time-consuming. Yet the situation is rapidly getting out of hand and the need to secure systems is of upmost importance.



SIÂN LOUISE HAYNES

Siân Haynes is currently a final year student at University of Wales, Newport studying BSc (Hons) Forensic Computing due to complete her studies in June 2011. She is aspiring towards getting a job as a digital evidence technician or a role within the forensic evidence technician field. She is an active member of the British Computing Society and is hoping to develop her education further in the future.

PETER BURDEN

Peter Burden is currently a final year student at University of Wales, Newport studying BSc (Hons) Forensic Computing due to complete his studies in June 2011. He is 32 and is a member of the British Computing Society. Before starting his studies he worked as a manager for a Ladbrokes Ltd and Currys Plc and spent the last 7 years in London working as an administrator before moving back to Wales to study his current course. He chose this course because he had a profound interest in the way computers operate and the mystery of how to discover the digital footprints left behind. He also strives to improve his knowledge in the field of computing and is undertaking this degree to better understand the workings of computer misuse and the laws surrounding them.

Examining aspects of Cloud Security and Risk

These days when we hear the term "Cloud Computing" there is an understanding that we are speaking about a flexible, cost-effective, and proven delivery platform that is being utilized or will be utilized to provide IT services over the Internet. As end users or researchers of all things "Cloud" we expect to hear about how quickly processes, applications, and services can be provisioned, deployed and scaled, as needed, regardless of users' physical locations.

When we think of the typical traditional IT security environment, we have to be cognizant of the potential for an onslaught of attacks be they zero day, the ever evolving malware engines and the increase in attacks via social engineering The challenge for any security professional is to develop and ensuring as secure an IT system as possible.

Thoughts on traditional Security and Risk

Common discussions within the spectrum of IT Security are Risks, Threats and Vulnerability. One can then ask; what then of the Cloud and Cloud Security and related risk derived from selected services being outsourced to a third party provider?

ISO 27005 defines risk as "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization."

In terms of an organization, Risk can be mitigated, transferred or accepted. Calculating Risk usually involves:

- calculating the value of an asset
- giving it a weight of importance in order to prioritize its ranking for analysis
- conducting a vulnerability analysis
- conducting an impact analysis
- and then determining its associated risk.

As a security consultant, I also like the Balanced Scorecard as proposed by Robert Kaplan and David Norton, especially when aiming at demonstrating compliance with Policies that will protect my organization from loss.

Cloud Security and Risk

In terms of Cloud Security, one key point to remember is that there is an infrastructure somewhere that supports and provides Cloud Computing services. In other words the same mitigating factors which apply to ensure security within a traditional IT infrastructure, will apply to a Cloud providers infrastructure.

All this is well and good within the traditional IT environment, but how then can we assess, or even forecast for and/or mitigate Risk when we are working with a Cloud Computing System? Some argue that "cloud authorization systems are not robust enough with as little as a password and username to gain access to the system, in many private clouds; usernames can be very similar, degrading the authorization measures" (Curran,Carlin 2011)

We have had the arguments that the concentrated IT Security capabilities at a Cloud Service Provider (CSP), can be beneficial to a Cloud Service Customer (CSC); however business are in the realm of business to ensure a profit from their engagements. One study by P. McFedries (2008) found that "disciplined companies achieved on average an 18% reduction in their IT budget from cloud computing and a 16% reduction in data center power costs."

To mitigate this concern, a CSC will need to ensure that their CSP defines the cloud environment as the customer moves beyond their "protected" traditional perimeter. Both organizations need to ensure that all high risk security impact to the customer organization mirrors meets or exceeds the customer organization's Security Policy and requirements and their proposed mitigation measures. As part of a "Cloud Policy" a CSC security team should identify and understand any cloud-specific security risks and their potential impact to the organization.

Additionally a CSP should leverage their economies of scale when it comes to Cloud Security (assets, personnel, experience) to offer a CSC an amalgamation of security segments and security subsystem boundaries. Any proficient IT Security practitioner then can benefit from the advantage of leveraging a cloud provider's security model. However when it applies to business need the 'one size fits all' cloud security strategy will not work.

Of utmost importance when looking to engage the services of a Cloud provider is gaining a clear picture of how the provider will ensure the integrity of data to be held within their cloud service/s. That said all the security in the world would not prevent the seizure of equipment from government agencies investigating a crime. Such a seizure can interrupt business operations or even totally halt business for an innocent CSC sharing a server that hosts the VM of an entity under investigation. One way to manage the impact on a CSC function within the cloud as suggested by Chen, Paxon and Katz (2010) is the concept of "mutual auditability."

The researchers further went on to state that CSPs and CSCs will need to develop a mutual trust model, "in a bilateral or multilateral fashion". The outcome of such a model will allow a CSP "in search and seizure incidents to demonstrate to law enforcement that they have turned over all relevant evidence, and prove to users that they turned over only the necessary evidence and nothing more."

Is it then feasible for a CSC to calculate Risk associated with such an event and ensure that there is a continuity plan in place to mitigate such an incident ? That will depend on the business impacted.

Another cause for concern from cloud computing introduces a shared resource environment from which an attacker can exploit covert and side channels.

Risks such as this need to be acknowledged and addressed when documenting the CSP-CSC Service Level Agreement (SLA). This of course may be in addition to demands with respect to concerns for Availability, Integrity, Security, Privacy and Reliability? Would a CSC feel assured that their data is safe when a CSP provides assurance that they follow the traditional static based risk assessment models?

I argue not, since we are working within a dynamic environment. According to Kaliski, Ristenpart, Tromer, Shacham, and Savage (2009) "neighbouring content is more at risk of contamination, or at least compromise, from the content in nearby containers."

So how then should we calculate risk within the Cloud? According to Kaliski and Pauley of the EMC Corporation, "just as the cloud is "on-demand," increasingly, risk assessments applied to the cloud will need to be "on-demand" as well."

The suggestion by Kaliski and Pauley was to implement a risk as a service model which integrates an autonomic system, which must be able to effectively measure its environment as well as "adjust its behaviour based on goals and the current context".

Of course this is a theoretical model and further research will have to be conducted to gather data points and "an autonomic manager that analyses risks and implements changes".

In terms of now, I believe that if we can utilize a portion of a static risk assessment, define specific controls and control objectives as well as map such to that within a CSP or, define it during the SLA process; a CSC can then observe control activities which manage and/or mitigate Risk to their data housed at the CSP.

Traditionally governance and compliance requirements should also still apply to the CSP e.g. there must be a third party auditor for the CSP cloud services and these services should have industry recognized security certificates where applicable.

Conclusion

In conclusion some things that a CSC needs to be cognizant with regard to Cloud Security in addition to tradition IT security measures with a CSP are:

1) The ability of the CSP to support dynamic data operation for cloud data storage applications while ensuring the security and integrity of data at rest
2) Have a process in place to challenge the cloud storage servers to ensure the correctness of the cloud data with the ability of original files being able to be recovered by interacting with the server (Wang 2011)
3) Encryption-on-demand ability or other encryption metrics that meets an industry standard e.g. NIST
4) A privacy-preserving public auditing system for data storage security in Cloud Computing (W. L. Wang 2010)
5) Cloud application security policies automation
6) Cloud model-driven security process, broken down in the following steps: policy modelling, automatic policy generation, policy enforcement, policy auditing, and automatic update (Lang 2011)

JON RAV GAGAN SHENDE

is a business executive who started out in the medical arena, then moved into the Oil and Gas environment where he was introduced to SCADA and network technologies. Here he also became certified in Industrial Pump and Valve repairs.

He gained global experience working within several verticals to include marketing, sales and technical services eventually becoming the youngest VP of an international enterprise.

Academically he is a graduate of the University of Oxford, holds a masters certificate in Business Administration, as well as an MSc in IT Security from Royal Holloway –The University of London's Information Security Group.

Jon has managed divisions within with the technology startup and midsized venture ecosystems and has experience with Virtualization technologies, Governance, Risk Management and Compliance as well as IT Security. He was an early adopter of web-services, web-based tools and successfully beta tested a remote assistance and support software for a major telecom.

Currently he serves as a Director – Advisory Board for a boutique consulting firm headquartered in South Florida as well as a Management Consultant – IT Strategy, Security and Risk Management for a Global Big Four firm.

Works Cited

- Curran, Sean Carlin and Kevin. "Cloud Computing Security. ." *International Journal of Ambient Computing and Intelligence*, 2011: 38-46.
- Lang, Ulrich. Model-driven cloud security. IBM, 2011.
- Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. *Hey, You, Get Off of My Cloud!Exploring Information Leakage in Third-Party Compute Clouds*. CCS 2009, ACM Press, 2009.
- Wang, Wang, Li, Ren. *Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing.* IEEE INFOCOM, 2010.
- Wang, Wang,Li Ren. Lou. "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing." Chicago, 2011.
- Yanpei Chen, Vern Paxson,Randy H. Katz. *What's New About Cloud Computing Security?* Berkeley: University of California at Berkeley, 2010.

Cloud Computing Offers Hope For All

Cloud computing is being touted worldwide for a number of purported benefits. These benefits include elasticity and flexibility, the potential for server consolidation, cost reduction, and a revolutionary new ability to view IT solely as a reasonable, monthly operating expense rather than an enormous capital expense.

The term springs up from the traditional view of the Internet as a cloud in representations of IT architectures and infrastructures. With cloud computing, applications and processing power seemingly fall from the heavens (ie, the cloud), and data is stored there as well.

This point of view makes people nervous, from IT management to the C-Suite. How secure is this information? What guarantee do I have that my data is not being shared with others? How can I enforce a real-time service-level agreement (SLA) when all of my resources are being managed by a third party? How can I even be sure that my data is being stored in my own country?

Human Error Strikes Again

The recent service outage to certain Amazon cloud computing customers and the disastrous theft of private information from Sony's cloud-based online gaming world does nothing to bolster anyone's confidence in cloud computing. So why would one continue to advocate for it? My view is that any problems reported to be the fault of cloud computing are actually, as usual, the fault of human beings. Societies determine acceptable risks for all technologies, whether transportation (plane, train, and automobile accidents), energy (oil spills and nuclear accidents), or housing (hurricanes, floods, and earthquakes). We even take calculated risks with our food supplies. Whether it's good government or corporate policy to say it, we take the same calculated risks with our IT.

The Amazon blackout was attributable to customers who decided not to pay for automatic failover services, but rolled the dice that nothing serious would occur within their localized zones. Sony taunted hackers to break into their systems, showing a hubris that was unintelligent and had no possible upside.

Stick to the Basics

So, as with all IT over the past several decades, there are basic principles and rules that apply to cloud computing:

- A focus on RAS – reliability, availability, and scalability
- Redundancy – be sure you are engaging at least Tier 2 datacenter standards, and don't skimp on failover capacity.
- Security – the same disciplines for privilege, authentication, encryption, and all the rest that you've incorporated for traditional IT apply to cloud computing.
- SLAs – take whatever amount of time it takes to nail down what security details are in place, how much capacity you need (and when), and what measures will be taken should the contract be breached.

Public or Private?

There is also considerable confusion on some of cloud computing's basic terminology, specifically how to define public cloud and private cloud. Most people understand public cloud to mean outsourced cloud, and private cloud to mean on-site cloud. There's also the terms hybrid cloud, which implies anything that's not strictly public or private; and community cloud, something that government agencies and non-profit entities might embrace in an effort to share resources and information.

Yet cloud computing is also being touted for its ability to be viewed as a utility, like electricity or water. Simply flip the switch or turn on the tap and the computing power comes flowing in. Clearly, an on-site datacenter can't provide even the illusion of this unlimited capacity.

The reality is that third parties can't either, really. Cloud computing can be viewed, very prosaically, as simply a bunch of servers sitting around. Whether they are sitting around in your building or a third party's campus doesn't change that fundamental fact.

Virtualize First

But that viewpoint not only takes the romance out of cloud computing, it obscures two other key facts:

- cloud servers have been virtualized
- nobody needs, or can afford, unlimited capacity

The first point involves virtualization software, which has been around for several years. Through its use, data can be liberated from applications in the form of services, and those services can be spread among hardware resources. This approach has shown to increase the utilization of processing power and storage capacity from about 15% to 80% and higher. It's much more efficient, and allows third parties to offer their services at attractive prices.

The second point can be viewed in the context of electricity. When you flip that switch, you expect the lights to go on. But you probably haven't installed an aluminum smelter overnight. In other words, the utility is providing what you need, and what you need is not unlimited, whether you have all the lights on and the air-conditioning running or not.

Efficiency Wins the Day

The efficiencies related to virtualization—moving the needle from 15% to 80%--means that on-site datacenters can either do some serious server consolidation, or scale up significantly without investing in new hardware. If your IT managers start to meter the processing power delivered and the storage capacity utilized by each individual in the company, they have in effect created a private cloud computing architecture.

For companies who are buying cloud services from third parties – whether a simple test project or with an "all in" approach – these efficiencies mean they can get what they need without a big, upfront commitment. Capital expenditure is turned into operating expenditure. Capex becomes Opex. Perhaps the most significant aspect of cloud computing is its potential for developing nations and for small- to medium-sized businesses (SMBs) everywhere. No longer does a small company, with limited resources to cash and credit, have to do without the IT it really needs to make its dreams come real. This holds equally true for developing nations that have the brains and vision to achieve their economic dreams, but until now, have lacked the funds.

ROGER STRUKHOFF

is Executive Editor of Cloud Computing Journal and founder of Samar Pacific Inc., a research firm with offices in Silicon Valley and Manila, Philippines. He's a frequent speaker at Cloud Computing conferences in the US and Asia. He has also served as an executive at the International Data Group and TIBCO Software.

For more information, visit www.samarpacific.com, contact him via Twitter @strukhoff or mailto: rstrukhoff@samarpacific.com

hexagrid

Presents

VX DATACENTER

IaaS Platform for Real-World IT Delivery: It's Your Cloud, Own It!

- Comprehensive Platform: Public/private cloud. No add-ons. 24x7 Support.
- Consolidated Virtual IT Resources: Increased efficiencies. Reduced costs.
- IT Delivery Capabilities: IaaS, PaaS & SaaS. Self-provisioning. Co-branding.
- Controlled Infrastructure: Cohesive compute, network & storage management.
- Simplified IT Administration: Intuitive, unified portal. Anytime, anywhere access.
- Integrated Functionality: Auditing. Monitoring. Scheduling. Accounting. Billing.
- Easy Scalability: Start small, grow unrestricted. Upgrade/expand seamlessly.
- Secure Multi-Tenancy: Segregated access. Policy-based user management.

See How it Works
www.hexagrid.com

hexagrid
Empowering Enterprise Cloud Computing

Mobile Phone Operating System Forensics

Mobile phones are a luxury that most people see as a necessity in the modern day world and security is an issue that is always in the back of most people's minds, but how secure is your mobile phone?

We are now in the era where almost everything that a computer can do, can be done on a mobile phone. This has created an opening for the criminally minded to commit traditional and cyber-crime from anywhere on the planet and any individual or group of people who own a mobile phone could be a target.

Using forensic imaging software such as Encase v6.0 and FTK (Forensic Tool Kit), several mobile phone operating systems are going under the microscope to compare features such as; how easy it is to forensically examine the operating systems that have been selected, enquiring on their data storage locations, challenging and discovering any security risks and finding any third party applications. There is constant competition in the mobile phone industry but which mobile phone is the most secure? (I recommend not trying this unless you are confident with the software, I cannot be held liable for any damages or negative consequences to any digital evidence or items.)

What am I doing?

According to several technical reviews the top 5 operating systems on the market at the moment (ranging from 1 – 5) are: Linux & Windows, RIM, Apple, Android, and Symbian. Now I know what the latest technical reviews say, I can now examine the mobile phones myself and generate my own review. The mobile phone operating systems that I have selected to be examined include; RIM, Apple iOS and Android, this will allow me to perform a case study on which one is the most secure dependant on how easy it was to access the information and how the operating system is set out.

Are all mobile phone operating systems similar?

No, contrary to belief mobile phone operating systems have vast differences; each one has different features and security processes. Mobile phone operating systems have different features and specifications similar to computer operating systems. The major differences with buying a computer operating system and a mobile phone are that most people don't consider what operating system they would like their phone to use; they just prefer the connectivity and application options.

During my study the top 2 operating systems were Android 2.2and Apple iOS 4.

These two operating systems are the backbone for the iPhone 4 and HTC Desire, two of the most popular phones available on the market.

Applications are the key to these operating systems. The development of applications from third parties is strictly overviewed by both Android and Apple and a percentage of the cost of the application goes directly to them to continue to keep the application stores free of viruses or any harmful programmes that could damage or unsecure the device.

The largest security issue found with the HTC Desire was the unlock pattern on the touch screen. This was of great help when needing to unlock the device for acquisition. Unless the screen is cleaned after each use, anyone can follow the fingerprint line that is created when unlocking the device. Following this trail to unlock the phone was easy and therefore a pointless security feature.

Both systems are not without their faults; however the size of the development communities currently working towards securing these systems will continue to close the holes that are exploited.

How secure are mobile phones?

Even though I have been able to image and examine several different mobile phone operating systems they secure, most phones have features such as firewalls (a piece of software that limits unauthorised access to the phone while allowing authorised communications) and encryption algorithms (that transform the message to make it unreadable by others unless they possess the key) this means that the day to day use of a mobile phone is somewhat secure.

The most secure operating system I discovered was the Blackberry RIM. During the examination, this operating system was the hardest to acquire using forensic software. This however was not the case when it came to using the more basic applications such as:

- Blackberry desktop Manager
  Designed to backup blackberry, manage all data from contacts to applications installed.

- ABC Amber Blackberry Converter
  This converts e-mails, contacts, SMS, PIN messages and calendar events to PDF format.
- XVI32
  This is a HEX Editor.
- Opensync
  Used to sync phone to desktop
- Emulation Software
  Used to show the operating system without the uses of a physical device

Using these applications most of the data stored on the device was relatively easily removed and viewed.

The easiest phone operating system to image and examine was the iPhone Mac iOS4. There are many different forensic tools currently available specifically for analysing and imaging the iPhone. The tool used was Oxygen Forensic Suite 2011. This application has the ability to not just gather the basic information that many others can but also gathers the GPRS, EDGE, CSD, HSCSD and Wi-Fi traffic and session logs that make this software ideal if the phone is being investigated is stated to be in a different place to the incident. The other advantage in using this forensic application is that it has Data Integrity protection with MD5, SHA-1, SHA-2, CRC, HAVAL, GOST Ð34.11-94 all being available for use.

Being able to access the data when you have the physical device is as I said previously easy enough. The larger task is to be able to remove the data from the device without the knowledge of the owner. Using the phones built-in Wi-Fi or Bluetooth capabilities against itself, it should be possible to gain access to the operating system and then covertly remove the data.

The Blackberry RIM is believed to have a more ‘sophisticated’ operating system because the phone is dedicated more towards a business lifestyle but in comparison the iPhone is just as complex. The iPhone may have been easy to examine but this was because a range of tools are made available to access the operating system. The Blackberry RIM was difficult to access but this was mainly because of the software I was trying to acquire it with, when I used the specified tools above I was able to examine the operating system.

Both phone’s operating systems are very unique and this is displayed in the way they are set out but the phones are currently at either end of the scale of the market when it comes to the user’s lifestyle.

My personal favourite operating system is the Mac which is the iOS4 operating system. The main two phones used for my examination were the iPhone 3GS and the Blackberry Curve 8250. The main differences between these two phones are basically the lifestyle: the iPhone promotes fun, freedom and flexibility; you can use the applications to create a style to suit you. Whereas the Blackberry is more rigid and focused towards a business lifestyle; the applications aren’t as widely available as the iPhone and are more expensive.

The main reason that there are several brands and designs of phones are because everyone wants a phone that suits themselves and their lifestyle. The iPhone does just that, it allows you to create whatever kind of environment you are happy with and will allow you to organise it in any way that you are comfortable with; you can put applications in designed folders whereas on other phones the folders are standard and the items are placed into a folder created automatically.

The interface comparison isn’t a fair test between these two phones because the Blackberry Curve 8250 is a keyboard interface whereas the iPhone 3GS has a touch screen interface. Again I prefer a touch screen interface because I feel it gives the user more control and is more user friendly than a keyboard that seems more rigid.

Even though the iPhone is a phone that is more flexible towards the lifestyle that you choose, it doesn’t necessarily provide the most security for the user. The iPhone 3GS has a built in firewall that stops harmful viruses or malware being downloaded on to the phone through applications and the internet when browsing but that is as far as the online security goes. It does have user security such as a key word or key code lock, enabling restrictions on the phone such as alterations to locations, accounts and applications. There is an auto-lock which automatically locks the phone after a set period of time and after several incorrect attempts there is a function which will automatically wipe the information, accounts, contacts and all other personal information relating to the owner of the phone.

The Blackberry Curve 8250 however is much more secure in the fact that it gives the user the choice of encryption, firewalls, certificates, tokens and advanced security such as blocking incoming information including text messages, phone calls, e-mails and from accessing certain servers.

How does this review compare to other reviews?

This review is similar to most reviews in the fact that most of the information is based on personal experiences and reviews. Comparing this review to the top five operating systems on the market, I believe they are wrong – the two according to them are Windows & Linux and RIM whereas I believe they are Mac (iOS) and RIM. Despite the security flaws of the iPhone I still believe that overall it is a much better phone and is more flexible and designed for the user. Security and protection of information is important but security is also based on how smart each user is with their phone and the information stored on it.

STILIANOS VIDALIS

Dr. Stilianos Vidalis was born in Athens, Greece, and was raised on an island in the Aegean Sea. He moved to Wales in 1995 where he did his undergraduate and postgraduate studies. He received his PhD in Threat Assessment in July 2004 from the University of Glamorgan. He joined the Department of Computing of the University of Wales, Newport in 2006 where he is currently the Head of the Centre for Information Operations. He is the program leader for the BSc Computer Forensics, and BSc Information Security. Dr. Vidalis is a member of the BCS South Wales Committee, a member of the E-Crime Wales Steering Group, and a member of the Military Educational Committee of the Welsh OTC. His research interests are in the areas of information operations, digital forensics, threat assessment, and effective computer defence mechanisms. Dr Vidalis is involved in a number of R&D projects with the Welsh Assembly Government, Law Enforcement Agencies, and private companies.

PETER BURDEN

Peter Burden is currently a final year student at University of Wales, Newport studying BSc (Hons) Forensic Computing due to complete his studies in June 2011. He is 32 and is a member of the British Computing Society. Before starting his studies he worked as a manager for a Ladbrokes Ltd and Currys plc and spent the last 7 years in London working as an administrator before moving back to wales to study his current course. He chose this course because he had a profound interest in the way computers operate and the mystery of how to discover the digital footprints left behind. He also strives to improve his knowledge in the field of computing and is undertaking this degree to better understand the workings of computer misuse and the laws surrounding them.

In the next issue of Hakin9 magazine:

WEB APP SECURITY

Available to download on June 30th

Soon in Hakin9!

RFID, SQL Injection, Stuxnet, Hacking Facebook, Port scanner, IP scanners, ISMS, Security Policy, Data Recovery, Data Protection Act, Single Sign On, Standards and Certificates, Biometrics, E-discovery, Identity Management, SSL Certificate, Data Loss Prevention, Sharepoint Security, Wordpress Security

If you would like to contact Hakin9 team, just send an email to en@hakin9.org. We will reply a.s.a.p.