

Vol2 Issue 4 Jan./April 2012

SecurityKaizen

MAGAZINE

CONTROL YOUR VULNERABILITIES

ONE Year of Success



BLUEKAIZEN.ORG

What happened in
Cairo Security
Camp 2011?

Interview with
Dr. Sherif Hashem
vice president of ITIDA

Awareness tips from
Facebook Team



**Data is encrypted
Using AES/TwoFish**

**DON'T MISS OUR
SPECIAL OFFERS**
End of year Discounts

DSphinx

The Ultimate Backup Solution



Get your files securely anytime ... anywhere !

Download your trial version now

<http://www.dsphinx.com>




Cloud Backup Solutions



Cross Platform



+2 0222638292

+2 0222615685


Facebook.com/dsphinx

www.dsphinx.com

www.fixed-solutions.com


Contents

Editor's Note



1 year, 12 months, 365 days and 8760 hours had been passed since the release ...

True Story



Treachery, deceit and pilfering have always been associated with mankind ever since the Neanderthal age. History has been a sore witness

Grey HAT



It all started while being so hungry and trying to figure out what to eat ...

Awareness



Facebook Tips
At Facebook, we work hard to protect the people ...

New & News




For those who are not familiar with CSCAMP, it's an annual conference for information security professionals where we gather all security

Interview

With ... Dr. Sherif Hashem

Senior Advisor to the CIT Minister for CyberSecurity at Ministry of Communications

Best Practice



Constructing mature information security awareness and educational models, Information Security is defined as protecting information and the systems that hold and support them directly from unauthorized use, access, disclosure, disruptions, modification and destruction. Any organization irrespective of their size and number util ...

SK Magazine Team

SecurityKaizen magazine

Chairman & Editor-In-Chief
Moataz Salah

Editors
Hidayath Ullah Khan
Joe Sullivan
Sameh Sabry
Ahmed Nile
Omar Sherin
Vinoth Sivasubramanian
Naveen Sharma

Website Development
Mariam Samy

Translation
Mai Alaa El-Dein
Asmaa Ibrahim

Marketing Coordinator
Mahitab Ahmed

Photographers
Mohamed Mohsen
Mohamed Samy

Designed & Printed By
2DAY Adv.

Security Kaizen is issued Every 3 months
Reproduction in Whole or part without written permission is strictly prohibited
ALL COPYRIGHTS ARE PRESERVED TO WWW.BLUEKAIZEN.ORG



Connecting Minds Improving Lives

For Advertisement In Security Kaizen Magazine and www.bluekaizen.org Website
Mail:info@bluekaizen.org Or Phone: 0100 267 5570

Editor's Note

1 year, 12 months, 365 days and 8760 hours had been passed since the release of our "Security Kaizen Magazine" first issue. Today, we are celebrating with you the first birthday of your Magazine.

Days passed so fast and I believe everyone feels the same, I still remember, as if it was last month, the 25th of January revolution days, Tahrir square, the internet cut off and the waking up at nights protecting our homes, although a whole year has gone now.

During this year, if I have the right to say that, we have been moving from success to another, the feedback we got from our followers whether internationally or locally was beyond my expectations and was something that made me feel so proud, not of myself, but of the great work that my team did and regardless of the hard conditions the country was in, we were able to survive and continuously improve ourselves

2011 ACHIEVEMENTS

After the release of the First issue in English language, we received many requests to release another version in Arabic, so we started, from the second issue, to release 2 versions one in Arabic and another in English and it was really hard to translate some technical expressions and concepts to Arabic especially that our translators are not technical ones but I would like to use this opportunity to thank all the translators who helped us to release the Arabic issues till we reached now a stable state.



We were able to be a media sponsor for nearly most of the famous Information Security Conferences during 2011 Starting by Hacker Halted Cairo in December 2010 passing by HITB in Amsterdam and Malaysia, Takedowncon in Dallas, Hacker Halted in Miami, RSA in London, Abu Dhabi Cyber Defense Summit and Others. We were also a media sponsor for the first Cyberlympics games.

The most astonishing thing to me is that, despite the expensive ticket price of these conferences, average of 2000 \$, our international readers in USA, Amsterdam and London were so keen to attend the above conferences using our discount code, we were able to get one reader in USA to attend Takedowncon in Dallas, 4 readers from Amsterdam to attend HITB, 1 reader to attend RSA in London.



We had a list of interviews with the highest prestigious professionals in the Information Security field such as: Joe Sullivan (the chief security officer of facebook). Also we were able to make a partnership with facebook where they will write an article every issue covering Security tips in Facebook.com. We had an interview with Clement Dupuis (the founder of CCCURE.ORG Portal) and Al Berman (CEO of DRII.ORG) and in this issue Dr sherif Hashem, senior Advisor to the Minister of Communication and Information Technology for Cyber security, and the Executive vice president of ITIDA, Egypt.

During this year, the biggest challenge to us was to transfer the magazine from an electronic version to a printed one, printing a magazine is not that cheap especially that "Security Kaizen Magazine" is a free magazine and the only



source of expenses' coverage is through advertisements and we all know how the business was hard during this year that even caused some companies to close, but we were able to do it and we are continuing to do it.

Due to these financial problems, we were not able to release the fourth issue on time and we had to merge the October and January issue together to release one issue in December to be the yearly issue, but we tried to make it



unique and I hope you will like it. But to be able to survive and continue producing your magazine and keep it for free, we decided to make a sort of fund from all fans of "Bluekaizen" and "Security Kaizen Magazine" who are willing to participate, usually in such cases in western countries a donation button on the website is enough, but in Middle east countries we don't have such culture so we decided to make a section called "Bluekaizen Store," in this section you will be able to buy T-shirts, Mugs and different products with Security Kaizen Logos, our animated character "kaizono" and other designs. We have been thinking about an idea that won't be a direct donation for money and we found that this solution will be the best so if You like our magazine and our activities help us to continue producing it by giving an amount of your liking.

Finally, I am not saying all of this to take pride in what we have done, although we should, but mainly to share that success with all our beloved readers and let them be sure that we wouldn't have gone that far without them and also to thank all my team members who are volunteering with their time and effort because they believe in "Bluekaizen" goals and I want to thank especially Mariam Samy (our website developer), Mai Alaa and her team (our Arabic translator) who really did a great effort during this year to move "Security Kaizen" forward and finally a special thanks to my wife that without her support and the calm atmosphere she provided, I wouldn't have been able to achieve this success.

Moataz Salah
Bluekaizen founder



Together, we can do more

Security Solutions Engineer- Proxy & Cashe (Ref: 526460)

- ❑ Very good understanding of networking (TCP/IP, routing OSPF, switching)
- ❑ Very good understanding of application & network security concepts & technologies
- ❑ In depth experience of Bluecoat proxies and preferably BCCPA & BCCPP certified.
- ❑ Good knowledge of Bluecoat (or else) reporting systems (Reporter), management systems (Director), content delivery network (CDN), data leakage prevention (DLP) and cloud computing.
- ❑ Sound understanding of service design especially validation, testing and release management.
- ❑ Hands- on experience in analyzing architecture and building proposals.
- ❑ Ability to write technical documentation for operations, sales and marketing. working knowledge routing, load balancing and resiliency.

Security Solutions Engineer- Intrusion Detection (Ref: 526461)

- ❑ Very good understanding of networking (TCP/IP, routing OSPF, switching)
- ❑ Very good understanding of application & network security concepts & technologies
- ❑ In depth experience of Juniper IDP sensors and preferably JNCIA -IDP certified.
- ❑ Good Knowledge of security event & incident management systems (Archsight) and working experience in developing signature and tuning sensors as well as investigating security incidents.
- ❑ Sound understanding of service design especially validation, testing and release management.
- ❑ Hands- on experience in analyzing architecture and building proposals.
- ❑ Ability to write technical documentation for operations, sales and marketing.
- ❑ working knowledge routing, load balancing and resiliency.

Mobility Operation Engineer (Ref: 525906)

- ❑ Working experience in routing and VPN configuration.
- ❑ Very good understanding of traffic security technologies and products in particular IPsec using Nortel
- ❑ Contivity & SSL using Juniper SSL-VPN; JNCIA-SSL is a plus.
- ❑ Working experience in authentication systems and in particular in RADIUS, TACACS, AAA & PKIs.
- ❑ Very good understanding of host firewalls Antivirus and HIPS notably from BigFix.
- ❑ Excellent understanding of IT & networking fundamentals.
- ❑ Good understanding of remote access technologies and mobility technologies.
- ❑ Good understanding of Unix/ Linux and certification is a plus.
- ❑ Good understanding of ITIL incident & change management processes.

Internal Security Engineer (Ref: 527064)

- ❑ Very good understanding of information security concepts and mainly access control domain.
- ❑ Very good understanding of networking (TCP/IP, routing OSPF, switching)
- ❑ Working experience in administration and management of firewalls & proxies (as security not acceleration devices) notably Checkpoint FWs & Bluecoat proxies.
- ❑ Knowledge and practice of Windows & Unix systems administration required
- ❑ Knowledge of security technologies such as Authentication, Encryption, PKI, Anti-Virus, Firewalls and Intrusion protection.
- ❑ Practice of network and security support & operations appreciated.
- ❑ Certification in security products is a plus.
- ❑ Very good understanding of ITIL processes and mainly change management process.

Check the jobs in <http://jobs.orange.com>
Or email osama.hijji@orange.com

True **STORY**

Hacking the Banks for **Fun and profit!**

© Cartoonbank.com



"You know, you can do this just as easily online."

Treachery, deceit and pilfering have always been associated with mankind ever since the Neanderthal age. History has been a sore witness to the many acts of treason perpetrated by man to entice, dupe and usurp the innocent. Currently, as the world is shifting to a new paradigm propelled by technological advancement, the temperament of man remains much the same. The medieval swindling tactics have been augmented with sophisticated cons. Today, the highly precarious Internet is relentlessly misused for committing atrocities over the cyber space. Among the numerous cyber-crimes committed, "hacking the banks" provides the best bang for buck for the cyber criminals.

Take a look at the recent online bank heists that have occurred over the last couple of years:



- In mid-July 2010, computer crooks stole \$447,000 from Ferma Corp. a Santa Maria, California based Demolition Company by initiating a large batch of transfers from Ferma's online bank account.
- Also in July 2010, attackers stole \$415,000 from Bullitt County Bank, Kentucky in US.
- In December 2009, cyber criminals successfully stole 300,000 Euro from a German bank's online accounts.
- And the list goes on.....

The modus operandi adopted by cyber criminals for hacking banks is evolving continuously keeping in pace with today's modern banking technology. The Basic Attack Plan

In order for the attack to work, the attacker has to first remotely take control of an online-bank user's desktop/laptop through which the user will be doing his/

her online banking transactions. There are many ways of taking control of the victim machine remotely, but the easiest approach for the attackers would be to attack the desktop applications like web browser, PDF reader and MS-Office applications etc. which are by default installed on the victim's machine. These desktop applications contain a plethora of vulnerabilities that can be remotely exploited by the attackers to give them unauthorized access to the victim's machine.

Attacking these desktop applications could be done in many different ways. The easiest way would be to send a fraudulent e-mail to the online bank user containing a PDF or MS-office attachment with malicious software embedded inside the attachment. When the user unwittingly opens the attachment, the ma-

licious software will get downloaded on his/her desktop. This malicious software is some type of data-stealing Trojan horse program which seemingly looks very innocuous but its main purpose is to silently connect the victim's machine to a remote command server controlled by the attacker.

Alternatively, instead of sending a direct e-mail, the attacker will try to entice the online bank user to visit some fraudulent websites controlled by the attacker which will contain attack code planted invisibly within the website. Once an unsuspecting user visits such websites, his/her web browser will be automatically attacked by the attacker's attack code forcing the user's machine to download some malicious Trojan software unbeknownst to him/her.

Malicious Banking Trojans

Cyber criminals use specialized banking trojans like "Zeus", "LuckySploit", "MPack", "Clampi", "URLZone" etc. for this purpose. Some of these trojans are commercially available for as little as \$500 with options for software updates, remote support, annual maintenance etc.

These trojans are tailor-made for hacking online bank accounts and come with all the bells and whistles required for making online bank hacking a relatively easy chore for the attackers. Following are some of the features found in banking trojans like URLZone or Zeus:

- Ability to log credentials and activities of bank accounts
- Can take screenshots of web pages served by the websites
- Can steal money from the compromised accounts
- Ability to hide its fraudulent transaction(s) in the report screen of the compromised account
- The Command control server can send instructions remotely to the banking trojans about the amount to be stolen and where the stolen money should be

deposited

- Logs and reports on other web accounts (e.g.: Facebook, PayPal, Gmail) and banks from other countries

Current versions of Zeus sell for up to \$10,000 and are used by elite cyber gangs to wire funds from the online banking accounts of small-sized and medium-sized businesses.

A relatively new type of financial malware with the ability to hijack customers' online banking sessions in real time using their session ID tokens called "OddJob" has been released. This new banking Trojan, keeps sessions open after customers think they have "logged off", enabling criminals to extract money and commit fraud unnoticed. This is a completely new piece of malware that pushes the hacking envelope through the evolution of existing attack methodologies. It shows how attacker ingenuity can side-step many commercial IT security applications traditionally used to defend users' digital – assets and online monetary – assets.

At the time of this writing, a far nastier banking Trojan by the name "tatanga" has been just released. Tatanga hooks into explorer.exe and can inject HTML in Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Minefield (Firefox dev builds), Maxthon, Netscape, Safari and Konqueror, basically every popular browser.

How Do These Banking Trojans Work?

- Banking Trojan sits inside a user's browser and waits for the user to log into a bank. During login, the banking Trojan copies the user's ID, password and OTP (One Time Password), sends them to the attacker and stops the browser from sending the login request to the bank's website, telling the user that the service is "temporarily unavailable." The fraudster immediately uses the user ID, password and OTP to log in and drain the user's accounts.

- Some banking Trojans overwrites transactions sent by a user to the online banking website with the criminal's own transactions. This overwrite happens behind the scenes so that the user does not see the revised transaction values. Similarly, many online banks will then communicate back to the user's browser the transaction details that need to be confirmed by the user with an OTP entry, but the malware will change the values seen by the user back to what the user originally entered. This way, neither the user nor the bank realizes that the data sent to the bank has been altered.

- Authentication that depends on out-of-band authentication using voice telephony is circumvented by a simple technique whereby the fraudster asks the phone carrier to forward the legitimate user's phone calls to the fraudster's phone. The fraudster simply tells the carrier the original phone number is having difficulty and needs the calls forwarded, and the carrier does not sufficiently verify the requestor's identity before executing the fraudster's request.

Command & Control Server

After having infected the victim's machine, the banking Trojan then connects to the Command & Control Servers to receive instructions. The Command & Control Servers for these trojans are usually hosted in Russia and other far eastern European countries. The Command & Control Server will then issue instructions which will include the amount to be stolen from the bank account, the money mule's account details to transfer the money, instructions to capture the screenshot of the online banking interface, etc.

Money Mules

Money mules are "willing or unsuspecting" individuals typically hired via Internet job search Web sites to act as "local agents" or "financial agents" responsible for moving money on behalf of a generic-sounding international corporation, le-

gal experts say. Once a "mule" is hired by the cyber-gang, the stolen money is transferred to the "mule's" bank account. Later on, the "mule" is asked to transfer the stolen amount – after deduction of his or her commission – to a bank account provided by the cyber gang via Western Union or Moneygram typically in far Eastern Europe countries.

Evading Anti-fraud systems

To avoid warning signs by anti-fraud systems at the bank, the money mule accounts are only used for a limited number of times within a certain timeframe. Since banks monitor large bank transfers, the amount of money deposited in a money mule account is predefined in order to stay under the radar.

To minimize detection by anti-fraud systems, the cyber criminals use various parameters to define the amount of money they will steal on each transaction. Criteria used by the criminals include: making sure that the victim's balance is positive, ensuring that the amount to be stolen is not too high, setting a random amount on each transaction, making sure that the remaining balance remains positive. The aim is to minimize detection by the anti-fraud systems.

Avoiding Detection by the Victim

In order to continue with their nefarious business activities in a clandestine way, the cyber criminals also need to hide the illegal money transfer transaction from the victim, otherwise the game will be over for them if the victim were to detect the unauthorized transfer and complain about it to his/her bank. To minimize the chances of their detection, the Trojan creates a forged bank report page that will be presented to the victim, effectively hiding the fraudulent transaction. The Trojan hides the transaction it conducted from the victim's machine by forging a bank report screen on the infected computer.



In the case of German Bank as discovered by M86 security group, the transferred amount below is shown as Euro 53.94, instead of the real amount of Euro 8,576.31. The Trojan generated a forged screen showing the transferred amount as Euro 53.94, and sent it back to its Command & Control server as an image. If the victim would log into his/her online banking account from a different, uninfected computer the real transaction will show up.

Conclusion

Cyber attacks and attackers are getting increasingly sophisticated and there is an urgent need to protect our resources from these threats.

Online bank users should be alert and keep abreast of the various tricks used by the cyber criminals while surfing the web. Users should also ensure adequate security of their systems by installing personal firewalls and other security tools that will alert on any suspicious activity.

Banks and financial institutions should employ unified web security solutions like web application firewalls with real-time content inspection, multi-factor authentication etc. Banks should consider deploying the following measures:

- Server-based fraud detection to monitor transactions for suspicious behavior.
- Out-of-band transaction verification to verify user transaction requests, and execute only the specific transaction verified or signed by the requesting user.
- Out-of-band communication protocols that can prevent calls from being forwarded to numbers that are not registered to a specific user account.

Hidayath Ullah Khan

I am the CEO of Sentelist MiddleEast – an IT consultancy firm specializing in Application Security, Penetration Testing and Forensics

Security Kaizen Labs 2012

Registration Opening Soon



It's time
To learn how hackers do it
<http://www.bluekaizen.org/sklabs.html>

Crack into a Wireless Network or Make a Sandwich?

GREY HAT

That's right

It all started while being so hungry and trying to figure out what to eat, during the last visit to my family and found out that my brother has changed the wireless connection password.

The moment I started thinking of what to do, few application names popped out of my head such as aircrack-ng, weplab, WEPCrack, or airtsnort. As my eyes gaze around the room, checking what else could have possibly changed, I found this mini-live-cd based on Tiny Core Linux called "Beini" a Chinese GNU/Linux distribution, created and maintained by ZhaoChunsheng from Tianjin, China lying around on my desk.

The distribution is not commonly known and/or used however, it is very light and if you need an easy and simple way to crack into a wireless network, Beini is the best open source tool for it.

It took me less than a minute to boot from the CD, and another couple of minutes to get the key for the house wireless network.

As I am about to show you step by step how-to crack into a wireless network, first let me show you how would I think and what are the techniques that could be used on the figure below (Figure 1):

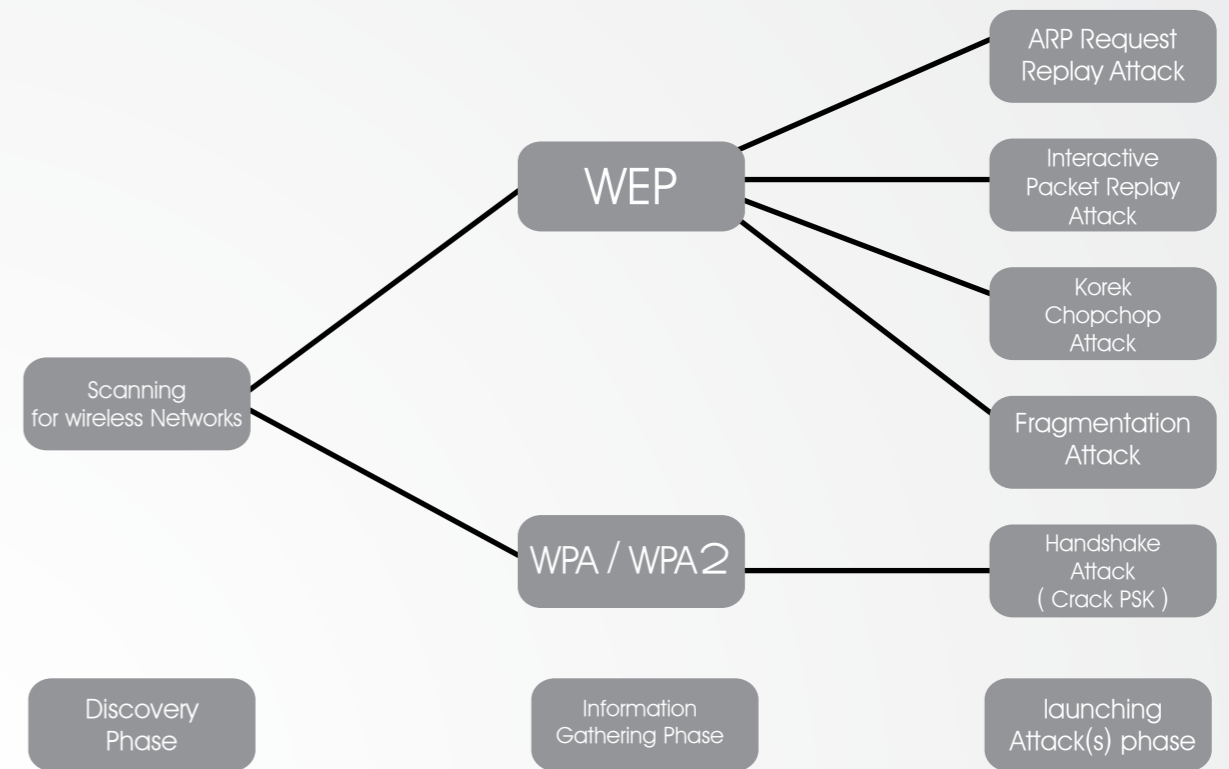


Figure 1. Wireless/Security Cracking Techniques

Wired Equivalent Privacy (WEP)

I would probably use the following cracking techniques:

1. ARP Request Replay Attack

This is a very effective way to create new initialization vectors (IVs), the program listens for an Address Resolution Protocol (ARP) packet then retransmits it back to the access point. The access point keeps responding with ARPs (new IVs) and this way we'll be able to determine the WEP key

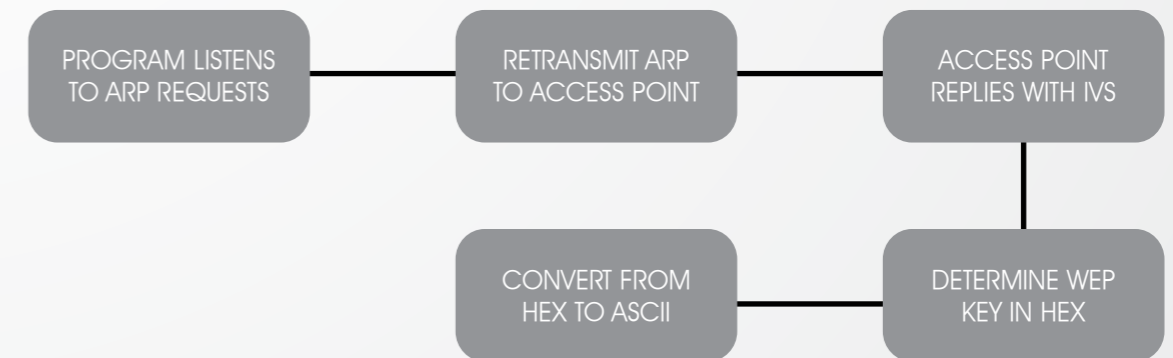


Figure 2. ARP Request Replay Attack Process Flow

2. Interactive Packet Replay Attack

This attack allows you to inject and obtain packets to replay from your own wireless card and a pcap file (heard of something called "libpcap" before? Maybe?). Certain packets would only work (to be accepted by the access point) which will in return cause new IVs, and that's the goal of this whole process, new IVs to find the WEP Key.

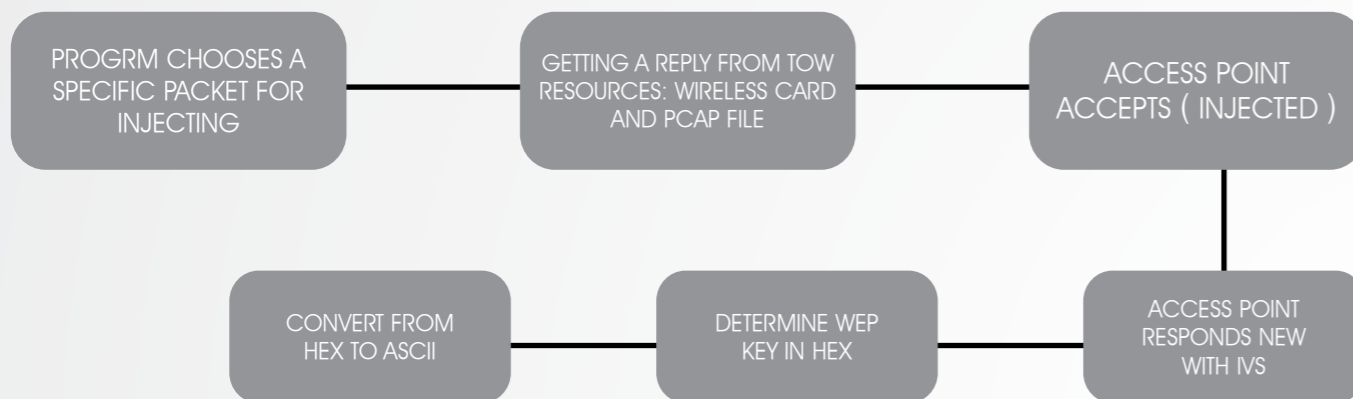


Figure 2. ARP Request Replay Attack Process Flow

3. KoreK ChopChop Attack

Decode one packet! Disclose the plain text. Successful attacks can decrypt a WEP data packet without knowing the key. It is also worth mentioning that it can even work against dynamic WEP which is a combination of 802.1x technology and the Extensible Authentication Protocol (EAP) -- Dynamic WEP changes WEP keys dynamically.

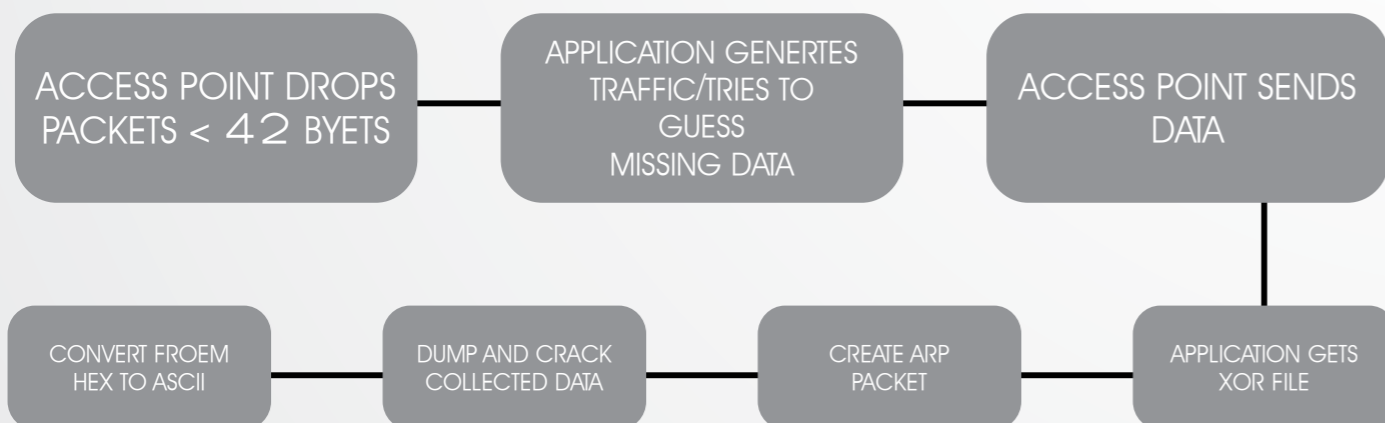


Figure 4. KoreK ChopChop Attack Process Flow

4. Fragmentation Attack

Again, fragmentation attack does not recover the WEP key itself, but only obtains the PRGA (Pseudo Random Generation Algorithm). PRGA can be utilized later on to generate packets which is also in return help in the injection attacks. The attack obtains the full packet length of 1500 bytes xor, so any size of packet could be generated, and is sufficient to create ARP request.

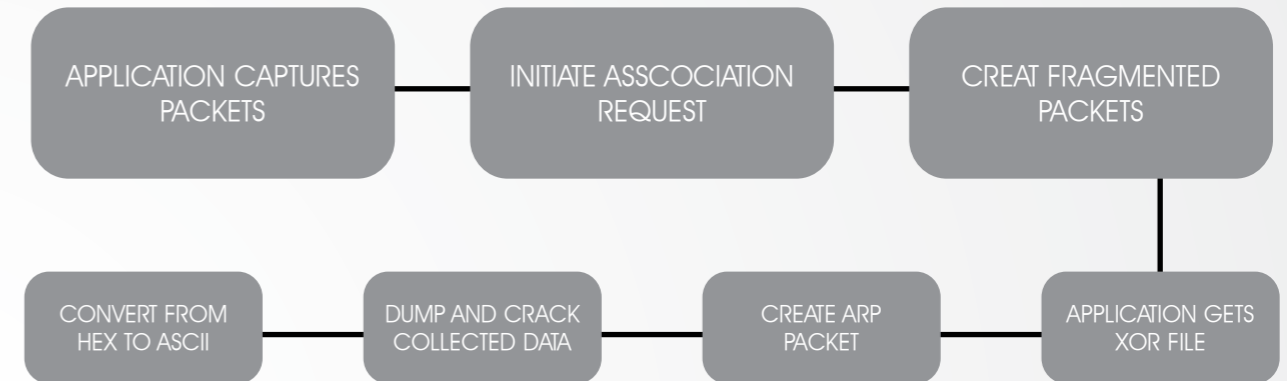


Figure 5. Fragmentation Attack Process Flow

Wi-Fi Protected Access (WPA/WPA2)

The authentication methodology is the same on both, a dictionary attack must be deployed otherwise forget about it (in case of brute-force/dictionary attack failure)

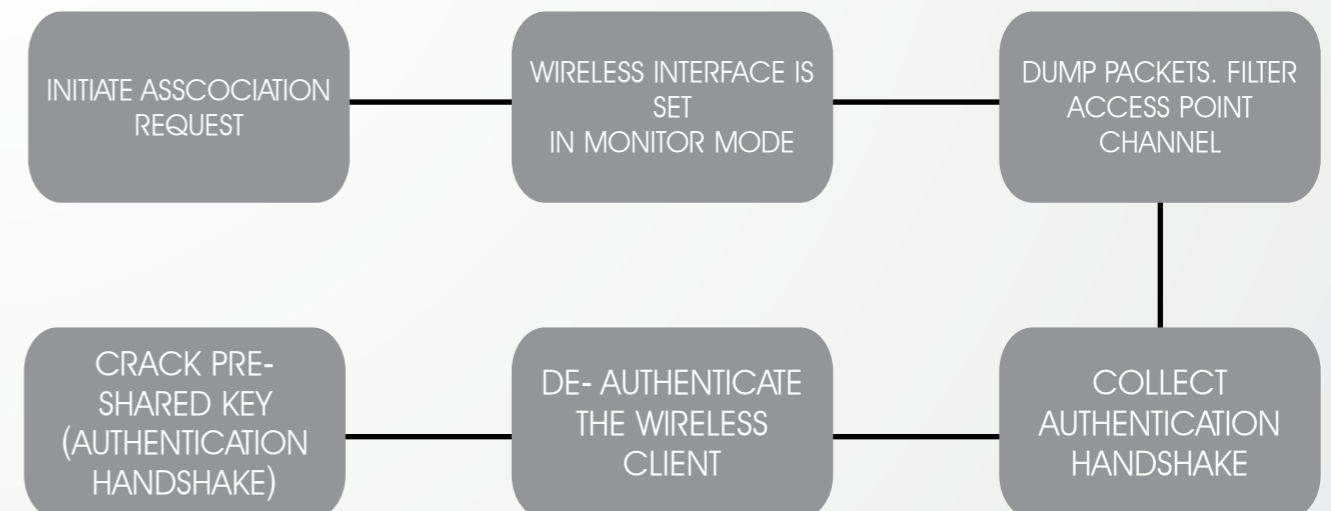


Figure 6. WPA/WPA2 Attack(s) Process Flow

Alright alright, enough talking, let's start cracking.

First, I will boot up my device using the Beini Live CD (from a USB stick or a regular CD)



Figure 7.

First Screen After Booting Beini Live-CD

Choose the "FeedingBottle" icon from the task bar.

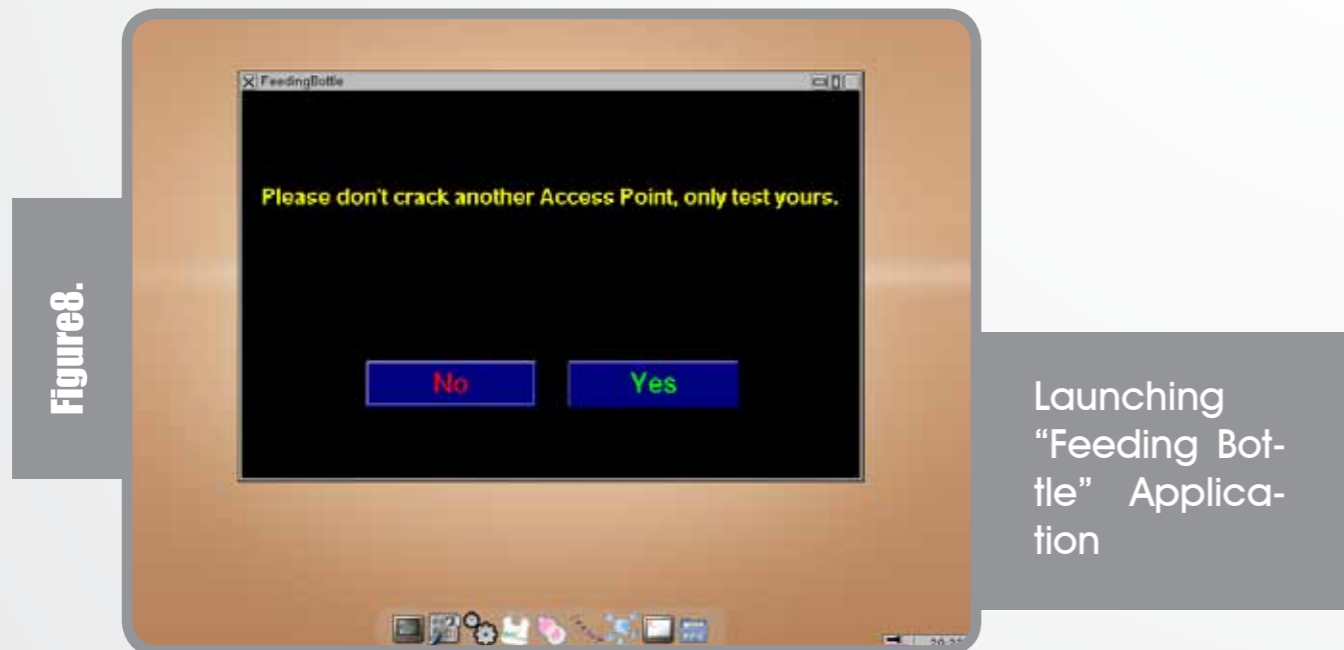


Figure 8.

Launching "Feeding Bottle" Application

Please remember, this is only a proof of concept and you may test it on your access point only. After clicking "Yes" you will get the following screen to choose your wireless card and setting it into "Monitor" Mode.

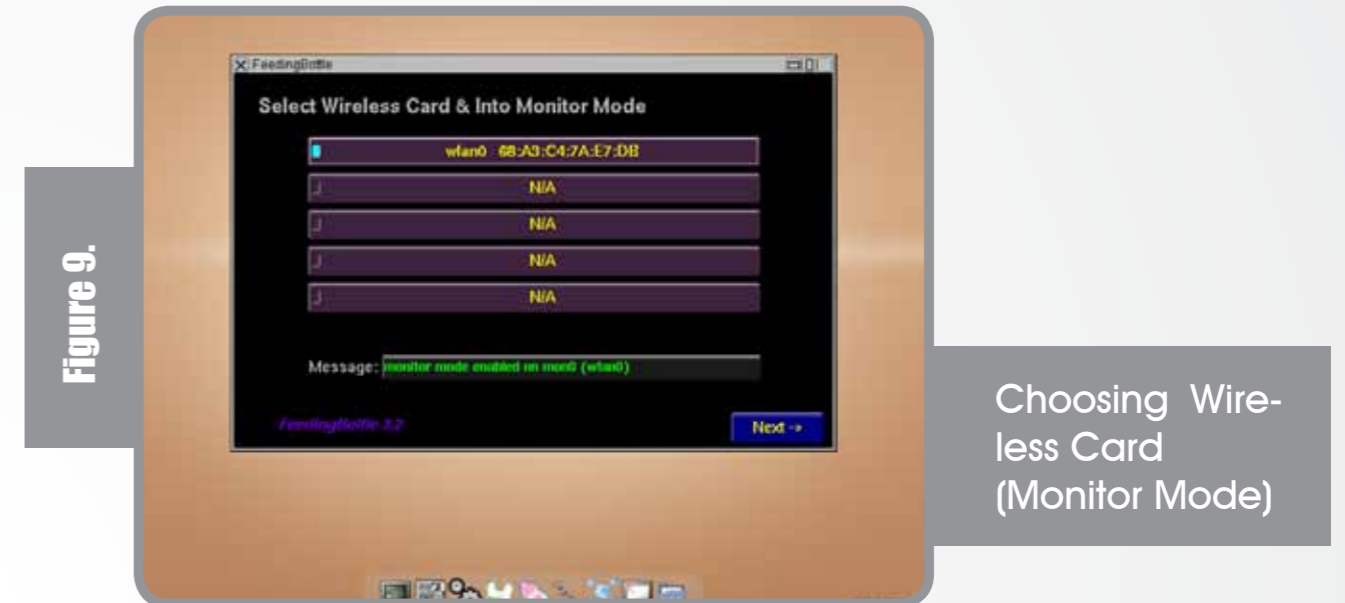


Figure 9.

Choosing Wireless Card (Monitor Mode)

Once you hit "Next ->" and "Scan" airdump-ng starts to capture raw 802.11 frames to start collecting IVs.

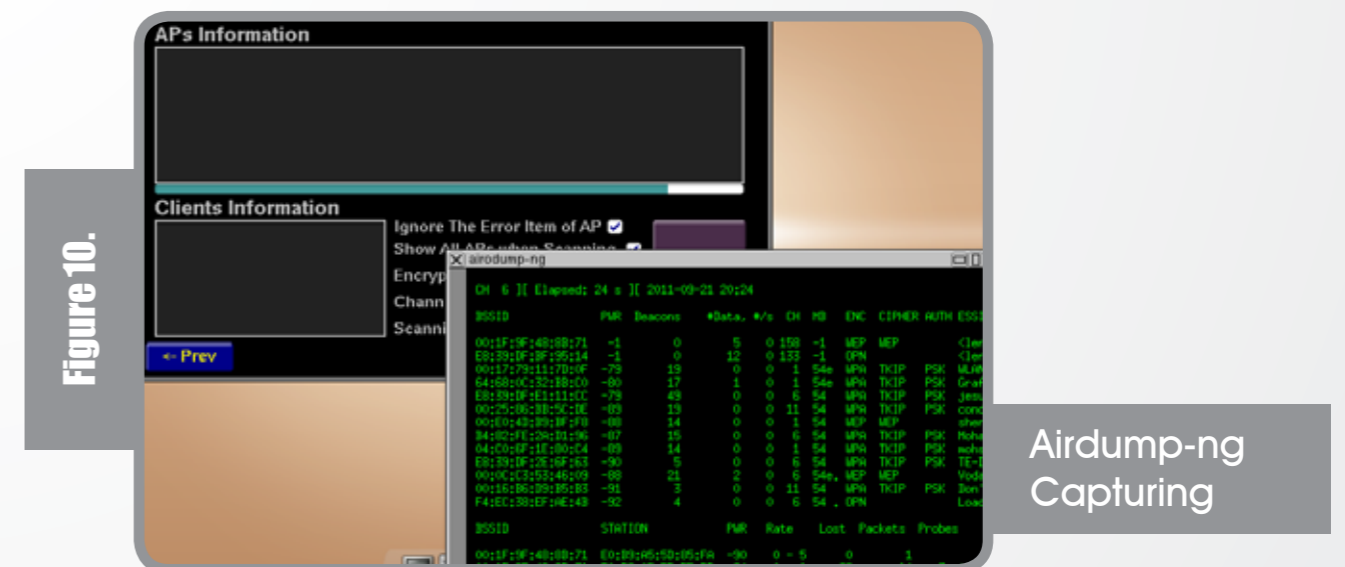


Figure 10.

Airdump-ng Capturing

After scanning the large network (so many birds to hunt) I choose my house access point, I am a good guy.

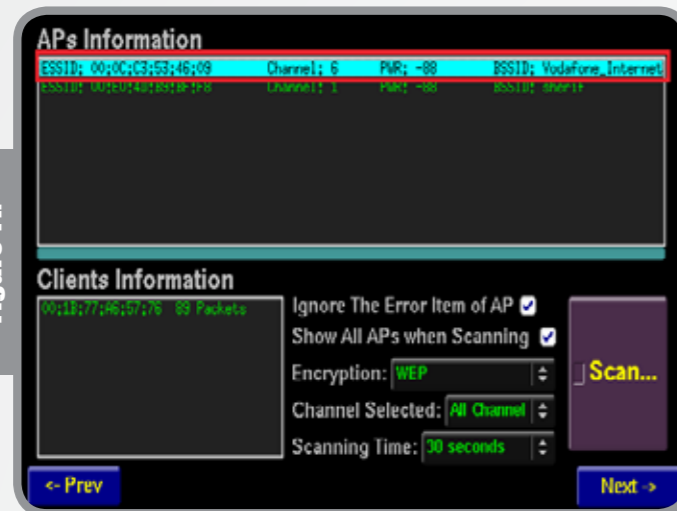


Figure 11.

WEP Wireless
Access Point
Found

As previously mentioned, I would think of 4 attacks to launch against WEP of which “ARP Request Replay Attack” is considered to be the quickest and “Fragmentation Attack” is considered to be the longest, at least in my very own opinion and more reliable since ChopChop attack doesn’t work with all access points. On this proof-of-concept I will be showing you the longest way “Fragmentation Attack”.

Once the attack is launched, airdump-ng starts to capture, IVs are the keys of our success, we try to initiate association request for fake authentication.

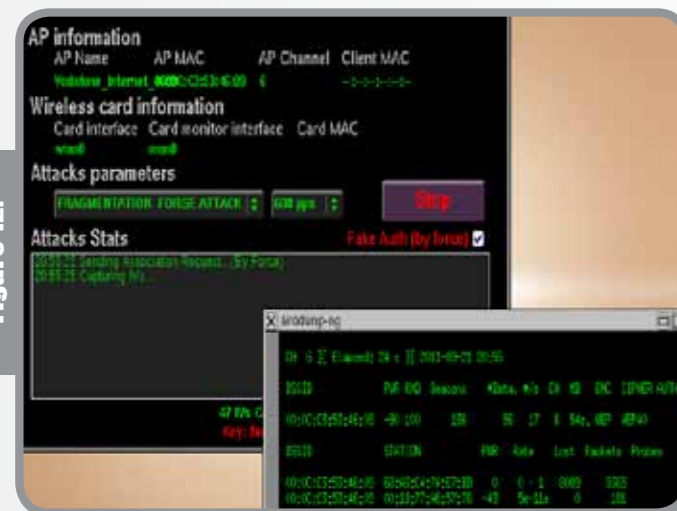


Figure 12.

Launching
Fragmenta-
tion Attack

Now association is happening, fragmented packets will be sent and generating a key stream file (xor file that will help in creating packets without knowing the key).

After the injection, IVs are being captured and collected to start cracking. IVs collecting/capturing is what counts and not the packets because it doesn’t help us with WEP cracking and many of the packets will be beacons (transmitted by access points to show their existence – hey I am here!).

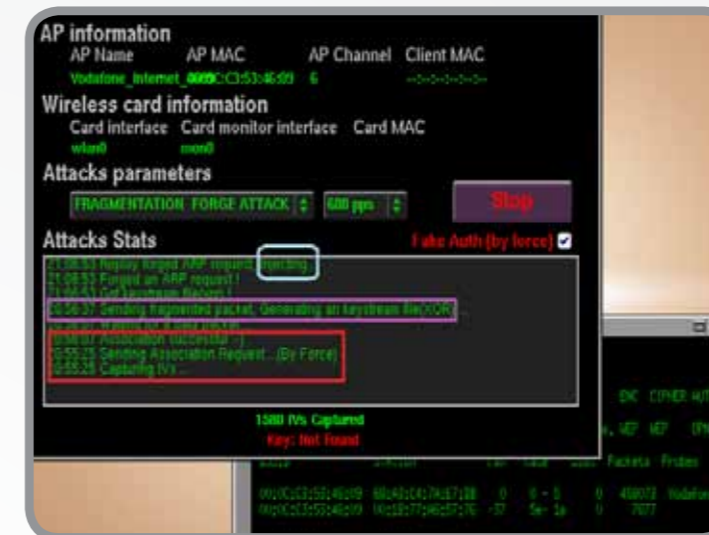


Figure 13.

Generat-
ing XOR File,
Forged ARP
Request and
Injecting

When enough IVs are captured (depending on the WEP Key size) you shall find the cracker working smoothly and in a few minutes the message “Key Found” will light up your eyes. Below you will see that the key was found and even converted to ASCII (from HEX).



Figure 14.

Cracking IVs,
Key Found

Finally, cracking into wireless networks could be easy, and it could take a few minutes, especially in the case of Wired Equivalent Privacy (WEP) Security. In that case, it is highly recommended to switch to the newer security, WPA2 which is using Advanced Encryption Stand-

ard (AES), and use higher security techniques in order to protect your wireless network. Also, it is worth mentioning that the strength of your password plays a main role, so please consider using a strong password including uppercase/lowercase characters, numbers, and symbols. Last but not least, please use the above mentioned information wisely and remember: “With Great Power, Comes Great Responsibility” – Spider Man.



Sameh Sabry

I am Security Consultant, OSCP, LPT, CHFI, C|EH, SANS PCI/DSS, Security+, Linux+, RHCE, LPI, CCNA

CSRF Attack

What is CSRF?

CSRF (Cross-Site Request Forgery) is web application vulnerability. It enables the attacker to obtain any kind of information through creating a website or email after the authenticated user/viewer access this website or e-mail remotely. The purpose of this malicious code is to redirect the user's request to a specific task URL. Actually this kind of attacks is severe and difficult to detect, because all the process is done without user's knowledge.

Example

Imagine that a user want to chat with his friends through his favorite social networking site (for instance www.socialnet.net). Unfortunately this website allows its users to insert their images into the website such as the avatars for forums or social networks as in face book.

The normal action taken in this case is like this: (the user's method)

```
< img src=http://socialnetworking/image.jpg>
```

The attacker's method:

```
< img src=http://socialnetworking/changepassword?newpassword=password12345">
```

Illustration

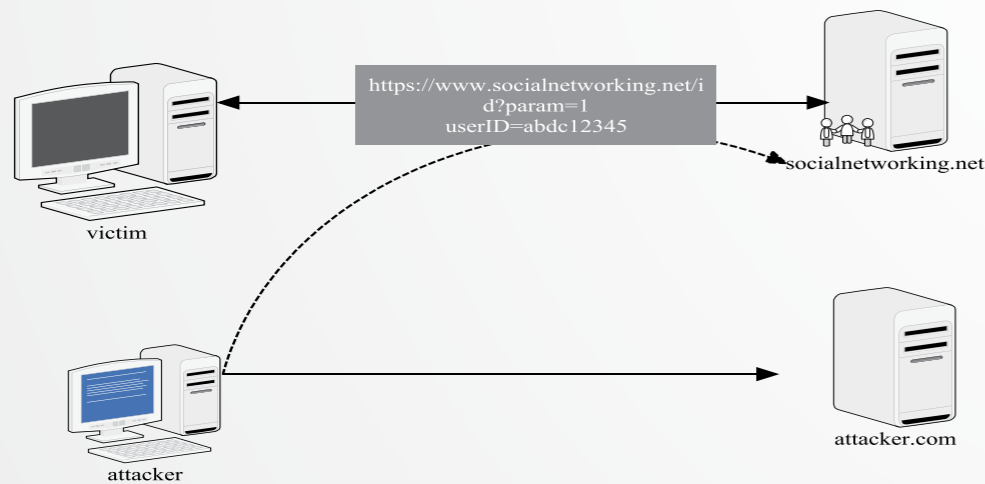


Figure 1: example on how the CERF attack would happen.

There are many ways used by the attackers to execute the CSRF attack. The most popular way is to use an HTML image tag, or JavaScript image object. As I stated previously; the attacker will embed these tags into an email or website. Without the user's knowledge, he loads the page or email, by which a request to any URL that the attacker has the link. Below is a list of the common ways that an attacker may use to try sending a request.

HTML Methods

IMG SRC

```

```

SCRIPT SRC

```
<scriptsrc="http://ost/?command">
```

IFRAME SRC

```
<iframe src="http://host/?command">
```

JavaScript Methods

'Image' Object

```
<script>
var foo = new Image();
foo.src = "http://host/?command";
</script>
```

'XMLHTTP' Object (See "Can applications using only POST be vulnerable?" for when this can be used)

IE

```
<script>
var post_data = 'name=value';
var xmlhttp=new XMLHttpRequest();
xmlhttp.open("POST", 'http://url/path/file.ext', true);
xmlhttp.onreadystatechange = function ()
{
if (xmlhttp.readyState == 4)
{
alert(xmlhttp.responseText);
}
};
xmlhttp.send(post_data);
</script>
```

How to Avoid Such Attacks?

After we illustrated an overview on CSRF attack and how attackers think about it. Now you have to know to keep yourself safe.

I personally recommend reviewing the OWASP CSRF attack prevention cheat sheet which can be found in [https://www.owasp.org/index.php/Cross_Site_Request_Forgery_%28CSRF%29_Prevention_Cheat_Sheet]

In the OWASP web site you can find also, tools that help you to test your code, and more about other related attacks in details.

Actually, if you look online for how to prevent yourself from CSRF attack dozens but millions of articles and resources online will give you suggestions about that. But if you have a deeper look at most of these best practices as they claim you will find there is a huge misconceptions which discussed by Eric Sheridan (who was one of the team who reviewed this update of the Top 10 web application vulnerabilities by OWASP you can find more about on [https://www.owasp.org/index.php/Top_10_2010]), to be as follows:

1. Only accept POST

- Stops simple link-based attacks (IMG, frames, etc.)
- But hidden POST requests can be created with frames, scripts, etc...

2. Referrer checking

- Some users prohibit referrers, so you can't just require referrer headers
- Techniques to selectively create HTTP request without referrers exist



Figure 2: example on HTTP Referrer [4]

3. Requiring multi-step transactions

- CSRF attack can perform each step in order

Conclusion

Due to the severity of CSRF attack targeting our financial, health care, and computer infrastructure which enables the attacker to take advantage of any authenticated transaction the user can do.

As I stated before you can find your bank account is transferred to another account with your knowledge or more than that, your password on any web application is modified, on that you can measure. The severity of this attack is based on all the transactions done by the attacker sound authenticated.

Acknowledge

I hereby certify that most of this article has a reference of other authors, in addition to that some of the code above has been taken from another web sites which is referenced in the reference section. Besides I would like to thank the editorial team for making this work come to the light. If you have any suggestions, comments, or questions. Please contact me @ Ahmed.neil@owasp.org

Reference and Further Reading

1. OWASP [https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29]
2. Robert Auger @ [<http://www.cgisecurity.com/csrf-faq.html>]
3. [<http://haacked.com/archive/2009/04/02/anatomy-of-csrf-attack.aspx>]
4. [<http://knol.google.com/k/preventing-cross-site-request-forgeries-csrf-using-modsecurity#>]
5. [<http://evilzone.org/tutorials/csrf-tutorial-by-connection/>]
6. [<http://www.gnucitizen.org/blog/csrf-demystified/>]
7. Eric Sheridan, Cross-Site Request Forgery: Danger, Detection, and Defenses, can be found on OWASP
8. [<http://www.techrepublic.com/blog/networking/csrf-attacks-home-dsl-routers-are-vulnerable/756/>]
9. Jesse Burns, Cross Site Request Forgery , An introduction to a common web application weakness, can be found in <https://www.isecpartners.com>
10. Kurt Seifried, Attack of the CSRF, 2008



Ahmed Nile

I am the OWASP Mansoura- Egypt chapter leader. Neil is an Information Security researcher in the Faculty of Computer and Information Sciences at Mansoura University-Egypt.



If You like our magazine and our activities help us to continue producing it by giving an amount of your liking.



Opening Soon

Securitykaizen
magazine

Vulnerabilities Opportunities

Vulnerabilities are indeed opportunities for information security professional regardless whether you are a good or a bad guy.

If you are a hacker then this is your golden ticket to fulfill your dreams of hacking glory, and if you are a system or network admin then these are the holes that you need to cover.

For SysAdmins (at least the good ones), vulnerabilities means... "finally some serious work"...at least better than resetting passwords for idiotic users "also known as top management" who keep forgetting the CAPS Lock on after 6 attempts.

The question is.....how to find vulnerabilities?

Professional hackers follow a process (called Triage) to collect information about their target. The information will help them identify and answer questions like:

- What Operating systems are they using?
- What is the target patch level?
- What vendors are they using (Cisco, Linksys, Microsoft...etc.)?
- Do they have a surveillance camera online that can give me a peek inside the company?
- Do they have any printers accessible from the Internet?

And ultimately and after long days of search they will know the exact vulnerability they should be targeting.

Having said that, I never thought that a day would come where a hacker or just a curious professional can have an entire search engine doing this for him.

Then about 2 years ago I meet Shodan: www.shodanhq.com

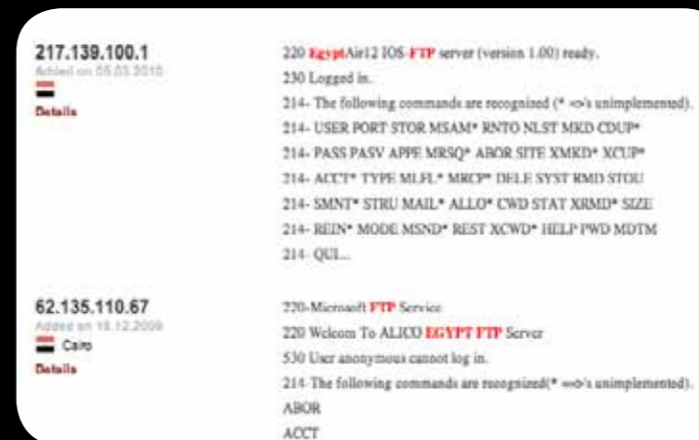
Shodan is an online computer search engine that lets you find servers/ routers/ printers/ surveillance cameras...etc. by using simple search keywords like (Ports, Services, vendors, country names...etc.).

Typing the search keywords: cisco country: eg returned for me 1409 IPs for Cisco devices accessible from the internet in Egypt. Why not spend some time trying the default user names and passwords and see what you can get. You will be surprised.

Typing FTP country: eg returned 9373 FTP servers in Egypt, I managed to access some of them just by trying the guest credentials. That left me depressed for days.

In those 9373 FTP servers, some of those companies even provide the exact version of the FTP server they are using which only makes it easier for the bad guy to look for the vulnerabilities available in this particular version. It's really that easy.

In the above example, "Egypt Air" our national carrier disclosed that they have a CISCO device (IP: 217.139.100.1), with the FTP server enabled and publicly published online and its version (1.00), and this obsolete version has known vulnerabilities. This FTP server can be either insignificant or of great value.



"Alico Egypt", the insurance company apparently has a Microsoft FTP server accessible online that doesn't accept anonymous accounts, which is a good security practice.

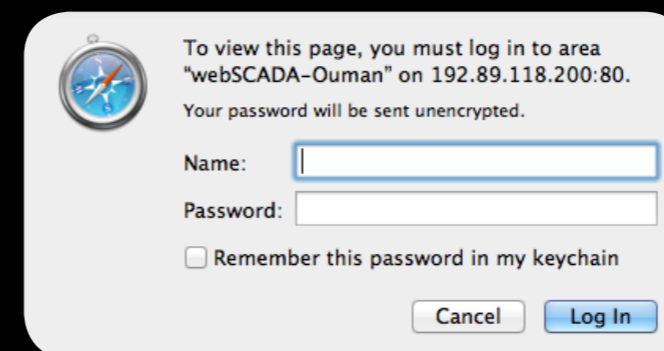
To take it up a notch, how about a query that can get you all the IIS servers (Web servers) in Egypt that are still using IIS 6.0 for example: Typing: IIS 6.0 -404 -403 -302 country: eg returned 2443 web servers in Egypt still using Microsoft IIS 6.0 with its known vulnerabilities, at least 8 ministerial/government websites are on the list.

Ever wondered who in Egypt is still using IIS 5.0 just ask Shodan.

Typing IIS 5.0 -404 -403 -302 country: eg returned 526 web servers including the website of the American University in Egypt, so the AUC is still using IIS 5.0 that originally was released with Windows 2000 (around 12 years ago). They can definitely do better than that.

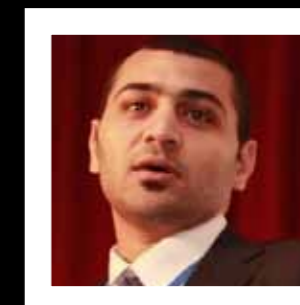
Another IIS 5.0 worthy note was an exchange securities trading company called Optima (<http://41.205.125.68/>), the vulnerable website host important clients information. Who is monitoring the private information protection in Egypt?

But to be fair this is a global problem, even looking for SCADA keywords returned more than 59 SCADA services available online...for example this particular webSCADA in Finland owned by a tractor manufacturing company just asks you about your (username/password) and you are in, how immune is this against brute force attacks...only the experiment can tell.



Looking to cause an empty tray of papers somewhere, how about looking for HP print servers with anonymous FTP access: searching for 230-Hewlett-Packard retrieved more than 350 print servers available online that you can try and access.

If you are just looking for fun, try searching for PelcoNet-Web server, which is the default streaming server for Pelco surveillance cameras, the world's best CCTV cameras. And you can see what your target company security officer is watching live. I believe this can be useful if you are planning on robbing a bank.....you didn't hear that from us.



Omar Sherin

I am a certified CBCP, CRISC And ISO27001 LA and in my spare time an active blogger in CILP. Wordpress.com

AWARENESS

facebook® Tips

At Facebook, we work hard to protect the people who use our site. From our User Operations team, who work to re-secure compromised accounts, to the Engineering team, that designs and implements new security features like login notifications. Everyone is working to ensure users have a safe, enjoyable experience. Our personnel, investment in equipment, development of proprietary tools and optional security features help us keep you safe. But we know this task is never completed, and so we continue to innovate.

Facebook Security Tips

Use our Security Tools - Review your security settings and consider enabling login notifications and login approvals. They're in the drop-down box under "Account Settings" on the upper right hand corner of your Facebook home page.

Dont Click on Strange Links: even if they're from friends, and notify the person if you see something suspicious.

Dont Click on Friend Requests from Unknown Users

Use the Report Links on the Site: if you come across scam or spam click on the report links so that Facebook can take it down.

Dont download any applications that you don't trust.

Visit Facebooks Security Page: <http://www.facebook.com/security>, read the items "Take Action" and "Threats."

Facebook has always been committed to protecting the account and information of people who use our site. Our 300-member Security Team works around the clock to thwart spammers and keep Facebook safe. We process a huge amount of content everyday to protect the people on Facebook - we vet over 26 billion pieces of content and 2 trillion link that clicks daily.

By utilizing advanced technology, our engineers work to ensure that using Facebook is a safe experience. We have several systems that run behind the scenes to discover, disarm, and disable threats. We have added tools to prevent various forms of spam and have implemented anti-scraping protection to ensure that your data stays safe. We also work with law enforcement and check the 300 million photos that are uploaded daily against a blacklist database from international, federal, state and local law enforcement agencies.

But, not all the security mechanisms operate in the background and we want to give everyone more control over their Facebook experience. We have several user controls that utilize the power of social connections to keep everyone safe on the site. Some of these are automatic parts of your account, while others allow you to choose what level of security best fits your lifestyle. We encourage people to visit the Facebook Security Page or our Help Center to learn about these tools.

We arm the people who use our site with the power to protect themselves. You can easily enable controls that will keep you updated and secure. Over the last year we have launched tools such as login approvals, login notifications, one-time passwords and HTTPS browsing and we are constantly looking for ways to educate users and encourage them to use these tools.

So far we've been pleased with our results to keep Facebook safe and are working hard each day to improve our systems and tools. Less than 0.5% of users experience spam on any given day, and less than 0.1% of logins are classified as suspicious. However, we are never fully satisfied, and strive to build innovative tools and systems to adapt and respond to new threats. We take the safety of our users and the security of their data seriously and strive to ensure a safe and secure experience when you use Facebook.



Joe Sullivan

I am the chief security officer of facebook.com, i manage a few of the teams at facebook focused on making sure that people who use facebook have a safe and positive experience

What happened In Cairo Security Camp 2011

New & News 2011

For those who are not familiar with CSCAMP, it's an annual conference for information security professionals where we gather all security related experts and non experts in one place for 2 days to discuss and share security knowledge and technologies. Cairo Security Camp was launched in 2010 with a small gathering (80 persons) in Nile University in smart village. In 2011, the event was held in the American University in Cairo and the attendees reached more than 300 persons from the security professionals in Egypt and Middle East, for more info about CSCAMP archive kindly visit www.bluekaizen.org

This year's event was a very new and unique experience for everyone who is interested in information security in Egypt and Middle East. Everyone was able to mingle freely in this "geeky" community, meeting up with new people, learning new stuff and having fun at the same time. Not to mention of course being able to witness for the first time Capture the Flag Competition in Egypt sponsored by synapsLabs.

The first day started with CTF competitors' registration and teams' formation, accompanied by the registration of the Conference and the distribution of the latest issue of Security Kaizen Magazine. Attending the CTF, that was fully developed by synapse-labs.com, required to pass 2 levels of JavaScript reversing a couple of weeks before the competition days, where you had to extract the key by reversing the encryption functions that was a bit of programming and cryptanalysis. In CSCAMP, the competitor received 6 problems, two of which were based on reverse engineering executable programs, the other two of challenges were writing exploits to attack the vulnerabilities in the programs, and the other two were related to web application exploitation where you needed to gain access over a web server from an exploit in session values to abuse RFI (Remote file inclusion) to view the SAM and System contents to crack the hash. The remaining one was a

brutal challenge which, till now, no one solved this exploit which was based on gaining access through passing parameters to the system dir command called in a PHP script. We hope that the dir challenge can be added to next years CTF. as it gave nightmares to the CTF competitors.

After the Gomaa prayer, Moataz Salah, CSCAMP Founder, gave an introductory session about Cairo Security Camp and expressed his feeling towards CSCAMP as it is his second kid and that we all should contribute with care and support and excuse its lapses as your little kid till it finally stands on its feet and start running as an athletic.

After that, first day's Keynote by Mr. Chris Brown, Director EMEA Operations NetWitness at RSA, was on the stage and his session was about why the golden solutions of Ant viruses are over. After that, Mr. Samer Omer, Middle East Managing Director at Qualys was on stage to talk about securing the cloud, and then the Rest of Speakers.

The Second day started with the 2nd day's keynote by Dr. Sherif Hashem, Senior Advisor to the Minister of Communications and Information Technology for Cyber Security, and the Executive Vice President of ITIDA and then the rest of sessions were followed

One of the most sessions that attracted the attentions of users was Omar Sherin's Session. Omar is a Critical Infrastructure Information Protection Manager in QCert his session name was SCADA Security the emerging Threat. The session was number one in the evaluation of the conference and gained the top score in everything including the profile of the speaker, presentation skills, topic and the slide show. He mentioned major threats in Egypt's SCADA systems, the video is highly recommended to be watched on www.bluekaizen.org. Also the Closing note by Osama Hiji and Ahmed Elezabi was a unique one; the session name was "Information Security and Egypt Future". They talked about the future of information security in Egypt after the 25th of January and how we should take quick actions in the progress of fixing our Information Security issues. Osama and Ahmed focused on the free of communication Law and the rights to make the communication medium allowable to everyone and avoid what happened during the revolution of cutting the internet and the mobile communications. The choice of the talk and the discussion was opened during and after the session was a good choice to close CSCAMP2011.



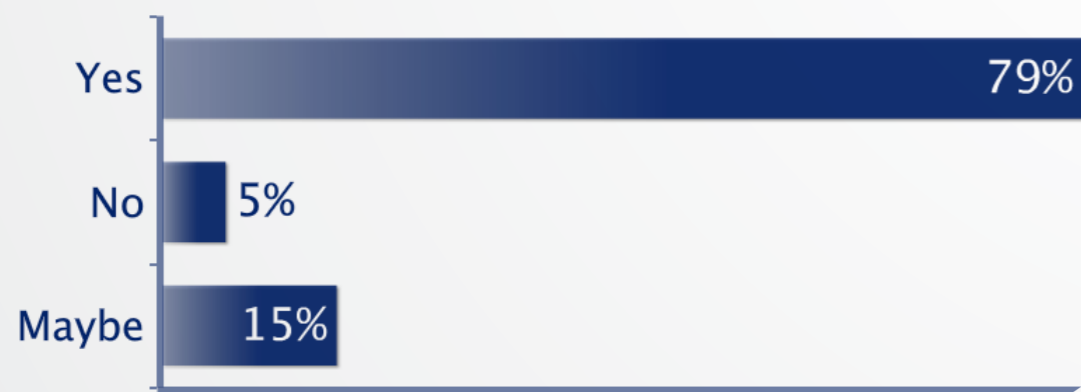
At the end of the Conference, free prizes were distributed randomly on all attendees including 5 free subscriptions to the famous hakin9 magazine, 3 courseware for CEH v7 from EC Council and others. Also valuable prizes were distributed to the winners of the CTF competitions including free courses and Free Exam Vouchers from Raya Academy for the winning teams and more.

Before leaving, Moataz Salah was so keen to take a live feedback from the attendees about CSCAMP 2011. So, a live survey was made to users if they would like to attend CSCAMP 2012 or not? Check fig.1 for results.

From Nearly 80 users submitted the live survey, 79 % from the users are interested to attend CSCAMP 2012, 5 % said No, and 15% said May be

Will you attend CSCAMP2012 ?

 This poll has received the maximum number of votes



Finally, Although CSCAMP 2011 is just a small baby trying to stand up and move, we received a lot of positive feedbacks and supporting comments on the event's hash tag #CSCAMP2011 and facebook page that made us sure that CSCAMP conference was born to live and to be one of the main conferences for Information Security in Middle East that you shouldn't miss.

CALL FOR SPEAKERS

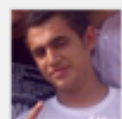
CSCAMP
2012
WWW.BLUEKAIZEN.ORG

SecurityKaizen

Comments

ADHAM (one of CTF winners) said:

"It has been long time searching for a challenge or a security competition to evaluate my experience and meet real security geeks. That search ended when I knew about CSCAMP. One of the major things that let me joined is that it had a CTF challenge of multi levels; the perquisite phase was 2 levels of JavaScript that measures your way of thinking and ability to circumvent the situation. It was loads of fun, I was a bit worried in the beginning because it was my first time to join a real CTF, But the CTF organizers were available for chat and Qs at the IRC channel all the time and were very friendly. The joy and fun during the two days cannot be described in words. The winner teams got prizes that ranged from huge discounts on security courses to totally free courses and a chance to travel to the next CTF phase in Dubai. No one got out of that a loser, knowing great fellows in the field and meeting new amazing people was the real gift."



Inxg33k Ahmed Shawky

I'll never forget #CSCAMP2011 thanks @Bluekaizen

5 Oct ☆ Favorite ↻ Undo Retweet ↩ Reply



Sa3dTalaat Saad Talaat

I think the #CSCAMP2011 have given me all what I need..And I'm happy as never nowdays..everything else I consider luxury.. thnx @Bluekaizen

4 Oct



0xAli Mohab Ali

"@__Obzy__: @Bluekaizen ! IT WAS AWESOME !" <= no, it was more than awesome!

2 Oct ☆ Favorite ↻ Retweet ↩ Reply



__Obzy__ obzy

@Bluekaizen ! IT WAS AWESOME !

2 Oct



An up to date link with the security community bk news is your way
www.bluekaizen.org/bknews.php



> Abu Dhabi

CYBER DEFENCE SUMMIT مؤتمر الأمن السيبراني

This year Cyber Defense Summit hosted in Abu Dhabi, the Capital city of UAE at Radisson Blu Hotel in YAS Island, revolved around the central theme 'Protecting critical assets against cyber threats'. The summit featured high profile Keynotes, Panel Discussions, Round Table Discussions and one to one business meetings. The meeting was well received by all the executives in UAE and the Middle East. Majority of the attendees were government attendees and this shows the commitment of the country's leadership towards cyber security and protecting critical national assets.

Day one included: Highlights

Opening speech by Philip Victor, Director of Policy and International Co-operation at International Multilateral Partnership against Cyber Threats (IMPACT).

Panel discussion on the role and importance of the CERTs participated by (AE Cert and Oman Cert)

Keynote on the integrated cyber shield by Marco Donfrancesco, Head of Special Product Strategy and Selex Sistemi Integrati

This event was attended by various delegates comprising of armed forces, government decision makers, front liners and executives from various organizations.

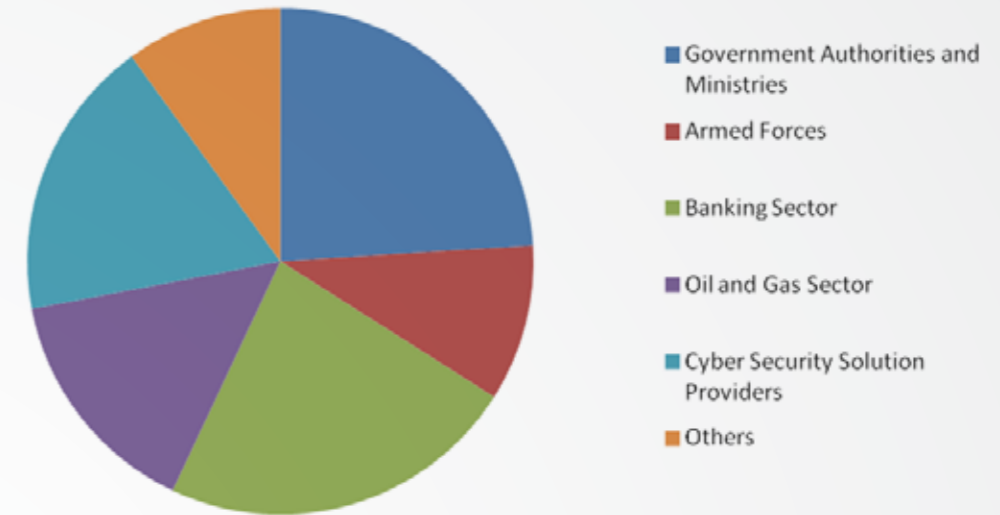
Day two featured: Presentations

A keynote on forward planning to ensure a cyber-protected organization by Carl Williamson, Executive Director of Cyber Strategy Defense Enterprise Solutions, Northrop Grumman Corporation

Panel discussion about the threats and challenges of cloud computing integration for the public sector

Roundtables debating the future of cyber security in GCC, and the feasibility of national and international information sharing and collaboration.

Sector Wise Audience Split Up



A cross section of the audience is represented below.

Executive Result Summary:

The results of the event were very clear and can be summarized below.

1. Greater Intelligence sharing mechanism at the national and international levels.
2. The need for a central forum to look into the cyber security threats.
3. People, the weakest link in the security chain needs to be strengthened through regular training and awareness programs.
4. The need for a national cyber security awareness programs, through focus groups.
5. The need to create central points of contact at enterprise levels to share and mitigate cyber security risks.
6. The need to build in intelligence into traffic coming and going into the networks.
7. The need for a proactive offensive approach rather than a reactive defensive approach.
8. The greater need to build more security into supply chains.

Conclusion

Last but not the least, cyber security risks as growing at an alarming rate and the losses incurred in the Middle East alone is around an estimated 1.44 Billion Dirhams in dealing with cyber security incidents. Countering cyber security threats needs an integrated approach comprising of people, process, technology and international co-operation. This was endorsed by one and all who had attended the event.

About the Author: The author is working as an Infosec professional in UAE. He has deep passion towards information security and leadership. He's continually striving to reach the pinnacle in both areas.



Hacking incidents in Egypt And Middle East

Israeli Prime Minister Netanyahu's Website Defaced by Egyptian Hacker



On the 20th of August 2011, An Egyptian hacker managed on Sunday to hack into the website of Israeli Prime Minister, Benjamin Netanyahu, and placed a picture of Egyptian soldiers raising the Egyptian flag in Sinai during the October, 6, 1973, on the sites' homepage. The hacker who managed to penetrate the webpage of Netanyahu wrote "Anti Zionism"; the site was then gradually taken offline.

Israel Radio is hacked by Egyptian hacker

www.radiolink.co.il

-: Message By Egytian H4x0rZ :-



Hi to greatest son of the bitches of the world ...
This Msg From Egypt " Mother Of The World "We Never Forgot And Never Forgive Any Isrealian Bitch3Z you Started The War Attack Us On The borders of Egypt For Nothing Reason .. So You Have Bear Our Attacks Fuck To All Isreal ./3x!t

Mego : EGS@hotmail.com

Soly : i-7@hotmail.fr

ElgaTed : F7Y@live.com

Egyptian hacker defaced the website of Israel Radio , and Write a message on homepage as shown:

Hi to greatest son of the bitches of the world ...
This Msg From Egypt " Mother Of The World "We Never Forgot And Never Forgive Any Isrealian Bitch3Z
you Started
The War Attack Us On The borders of Egypt For Nothing Reason .. So You Have Bear Our At-
tacks Fuck To All Isreal.

Vodafone Egypt's Facebook page hacked, then disappears

Group of hackers called "Destructive Tornado" hacked Vodafone Egypt Facebook fan page, changed the display picture & posts comments declaring control of the admin panel. Action came expressing Egyptian anger for communication shutdown toke place Jan25. Quickly the fan page gained more popularity with thousands of comments in favour of the hacker "Thanking him" mocking Vodafone Egypt lame "Vodafone Shokran" campaign. However for some reason the hacker decided to delete the fan page which had 800,000 followers. Ewww!! It wasnt before too long when Vodafone Social Team came up with a statement & re-creating their facebook fan page again to gain 1,155 followers.

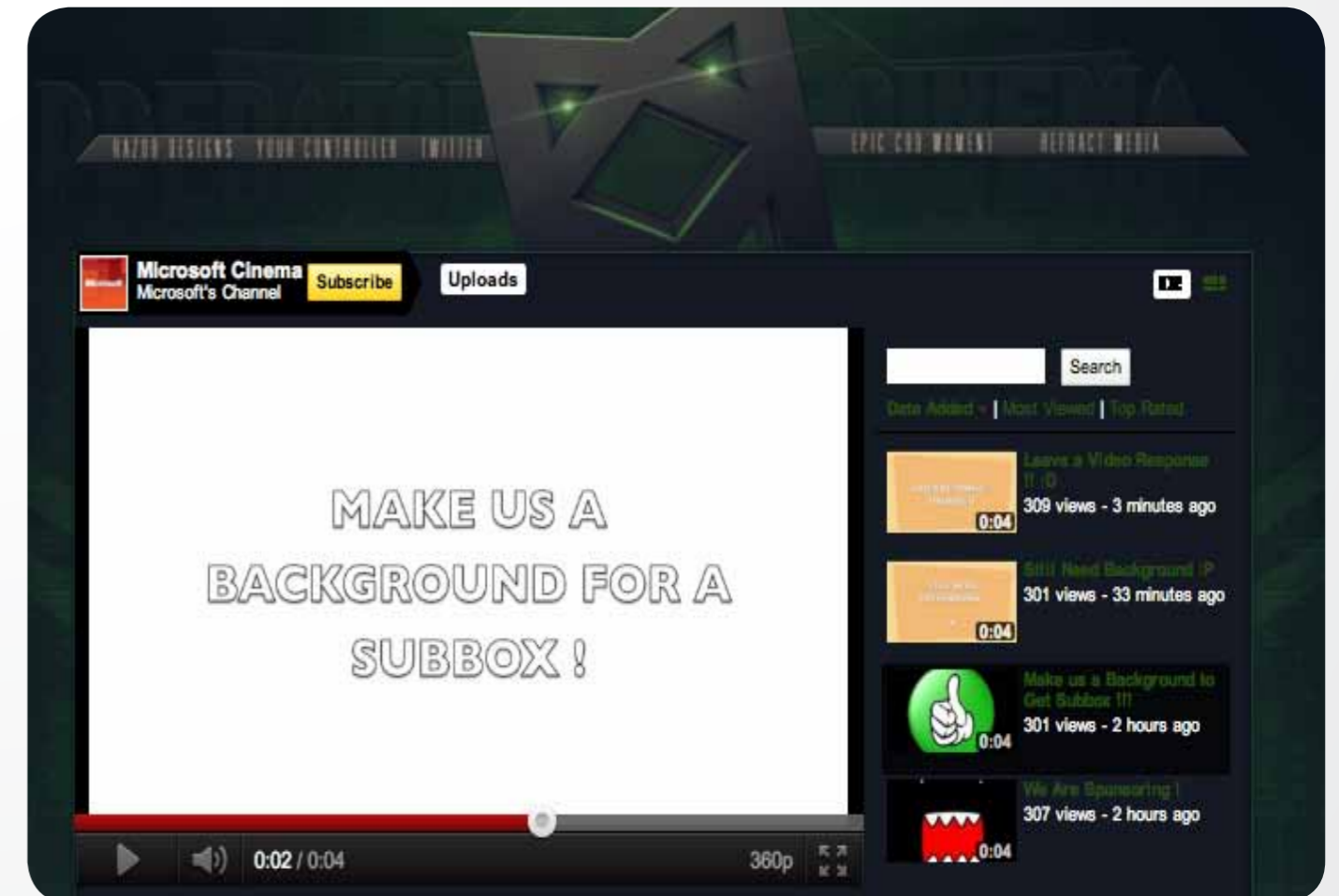
According to Vodafone Egypt the hacker had 45mins window in control of Vodafone's Facebook page which he was in fully control of accessing "Messages" which has customers phone numbers using facebook sending complains and phone numbers.



Microsoft YouTube Channel hacked

Computer giant Microsoft's official YouTube channel appears to have been hacked Sunday morning. All of the official videos, including recent ad campaigns, have been removed from the account. In their place are short clips soliciting advertisers, not surprisingly, as the channel has some 24,000+ subscribers.

As of 1:30 p.m. ET, four videos have been uploaded to the account, all time-stamped within the past two hours. A fifth video, most recently uploaded, seems to have been removed. The video, "Garry's Mod - Escape the Box," featured what appeared to be an animated gunman shooting at the inside of a construction box.



Interview

with **Dr. Sherif Hashem**

Senior Advisor to the Minister of Communications and Information Technology for CyberSecurity, and the Executive Vice President of the Information Technology Industry Development Agency (ITIDA), Egypt



Moataz: Can you introduce yourself to SECURITY KAIZEN Magazine readers?

Dr. Sherif: I am the Senior Advisor to the Minister of Communications and Information Technology for CyberSecurity, and the Executive Vice President of the Information Technology Industry Development Agency (ITIDA), Egypt. I am also a Professor at the Faculty of Engineering, Cairo University, Egypt (on leave). I had received a B.Sc. in Communication & Electronic Engineering (Distinction with honor) and an M.Sc. in Engineering Mathematics from Cairo University (Egypt – 1985 & 1988), and a Ph.D. in Industrial Engineering from Purdue University (USA – 1993). I had also completed the Senior Executive Program at Harvard Business School (USA – 2001). I am currently responsible for e-Signature, cyber security, and Intellectual Property Rights (IPR) protection for software and databases. Dr. My responsibility includes setting the framework for establishing and operating the Egyptian Computer Emergency Response Team (EG-CERT) at the National Telecom Regulatory Authority, the Egyptian Root Digital Certificate Authority (Root-CA) and the Software IPR Office at ITIDA

Moataz: What are the benefits that ITIDA provide to Information Security Community specifically, not the IT sector as a whole?

Dr. Sherif: ITIDA is the main anchor for E-signature in Egypt, and it hosts the Root PKI Certificate Authority (Root CA) for the country. The Root CA links the 3 private e-signature certification service providers (CSPs) as well as the governmental CA run by the Ministry of Finance, thus providing an integrated infrastructure for PKI services and e-signature applications in Egypt. Such an infrastructure is essential for establishing and protecting the digital identities of individuals as well as organizations, which paves the road for a more interactive Egyptian information society with enhanced quality of life. The PKI infrastructure is also essential for advanced and secure e-government and e-business applications. The Root CA also provides a gateway for cross-recognition of PKI digital certificates with other countries, thus facilitating and empowering e-business applications with the international community. The establishment and the operation of the PKI infrastructure involved a comprehensive training and skills development programs for professionals working at ITIDA and with the private CSPs; which not only enhances the security of the operation of the national infrastructure, but also provides opportunities to export advanced PKI services to the Arab and African Regions. Since its establishment in 2005, ITIDA has organized, supported and hosted several events and workshops, such as the ITU Arab Regional CyberSecurity and Digital Identity Symposium held at the Smart village 18-20 Dec 2011.

Moataz: Can you give us an overview, status and progress of the e-signature and Root CA projects?

Dr. Sherif: The Root CA was launched on 28 September 2009, and the three licensed private CSPs have been linked to the Root CA shortly after. ITIDA has also provided a grant to develop an Egyptian Smart PKI Token. The company that won the grant developed two PKI tokens: with and without biometrics (finger print), which are currently available in the Egyptian market, and are also being marketed abroad. ITIDA has been lobbying for the deployment of e-signature and PKI applications with the e-Government Program, and with key stakeholders in various sectors, including of course the ICT Sector, the banking sector and the Stock Market.

Moataz: you were the pioneer in establishing CERT in Egypt; can you please give us a quick overview about CERT and the role of EGCERT in Egypt Security life?

Dr. Sherif: The Egyptian CERT (EG-CERT) was established at the National Telecom Regulatory Authority (NTRA) and started its operation in April 2009. Operating on 24/7 basis, EG-CERT has about 16 professionals who provide high level monitoring and security incident handling support to key stakeholders responsible for the ICT infrastructure in Egypt. EG-CERT also assist in providing expert reports to courts in major cybersecurity cases, such as the international Phish Phry case that was uncovered in October 2009. EG-CERT has supported several stakeholders within the government,

and the ICT and the financial sectors in dealing with a variety of security incidents, including DDOS attacks, hacking and web defacement. It is worth noting that in 2009-2010, the NTRA launched a national comprehensive cybersecurity training program provided through the well known SANS institute, resulting in the certification of 179 ICT professionals across 38 entities in the governmental sector, ICT and CSP companies, banking and financial sector, and academic institutions. Of course, EG-CERT's staff are among the graduates of that program, with some of them receiving multiple SANS certificates with high scores.

Moataz: Many Security Professionals are wondering why, till now, EGCERT doesn't have a website or a published phone number to contact them in case of a cyber incident or a security query?

Dr Sherif: EG-CERT will launch their website soon, but in the meantime they can be reached through the NTRA.

Moataz: Why CERT is under the NTRA? Are they only focused on telecom sector? What about the other sectors like banking, oil & gas..?

Dr Sherif: EG-CERT is the first cornerstone towards a comprehensive approach for national Critical Information Infrastructure/CyberSecurity Strategy. Such a strategy will cover critical sectors, including the ones that you mentioned above.

Moataz: Does EGCERT or any other entity in the government have clear Security Awareness Program targeting public users like university students, different government employees and others?

As mentioned above, this needs to be part of a comprehensive national strategy

Moataz: In your opinion, why the Egyptian Government websites were attacked so easily during the 25th of January Revolution and do we have any kind of Audit on the government's sites?

Dr Sherif: Governmental websites are hosted by a variety of providers (in-house, ISPs, etc.), and in some cases the providers and/or the developers do not pay enough attention to security concerns, which makes some websites vulnerable to cyber attacks. As I mentioned above, we need a comprehensive cybersecurity national strategy. Moreover, we also need to enhance/amend the regulatory framework relating to operational requirements for public and governmental information systems.

Moataz: I received many comments from the Egyptian Security Community that they don't feel the progress of Information Security in Egypt. In your opinion, is that because of the lack of publications about MCIT achievements in that field or because of the lack of achievements itself?

Dr Sherif: As I mentioned above, MCIT has launched the CERT (at the NTRA) and the PKI ROOT CA (at ITIDA), and has supported a comprehensive national cybersecurity training program for 220 professionals in 38 entities in the government, and the ICT and the financial sectors. MCIT and its affiliates (ITIDA, NTRA, NTI, ITI) have also supported and organized several events and training workshops, such as Hacker Halted (by EC Council) and other worldwide leading cybersecurity specialists. We understand that cybersecurity threats are increasing and the expectations of our cybersecurity community are also growing. So as security professionals, whether in the government or in the private sector or in the academia, we need to increase our coordinated efforts to further the national cybersecurity agenda, and to expand our outreach to the general public, and to lobby with decision makers in all sectors.

Moataz: In the last couple of months, there were a lot of discussions regarding the electronic voting and its security, what is your opinion about it and is it doable in Egypt or not?

Dr Sherif: The use of ICT in the voting process will definitely enhance the citizen's experience and facilitate participation in the democratic transformation in Egypt. In this regard, ITIDA hosted a group of about 100 ICT professionals to analyze the worldwide best practice and advise the government on a comprehensive approach for ICT-enhanced voting. Several meetings took place in March through April 2011, with over 40 contributed documents exchanged and analyzed. The final recommendations were presented to the Cabinet of Ministers, and some recommendations were taken into consideration. However, we still have a long way to go and there are many opportunities to further enhance the voting process using ICTs, whether inside the polling stations or in the case of remote e-voting for expats.

Moataz: Today, Egypt and the Middle East had a lot of Hacking incidents, why we don't have a big competition to the security community to challenge their skills and get them to the white hat community instead of the black one especially for the teenagers?

Dr Sherif: Great idea! I suggest that you take the lead, and let us know how we can support this initiative.

Moataz: What is your opinion about security kaizen magazine and Cairo security camp initiatives especially after conducting the first capture the flag competition in Egypt?

Dr Sherif: I enjoyed the security camp, at least the part that I attended. I also like the idea of the competition. Keep up the good work!

Best Practice

Constructing mature information security awareness and educational models

Information Security is defined as protecting information and the systems that hold and support them directly from unauthorized use, access, disclosure, disruptions, modification and destruction. Any organization irrespective of their size and number utilize the following mechanisms for practicing and improving their information security posture. The mechanisms utilized are People, Process and Technology

The only common factor as seen from the diagram is that people manage both process and technology. Therefore every employee permanent, temporary, contractor, business partner, vendor etc has information security roles and responsi-

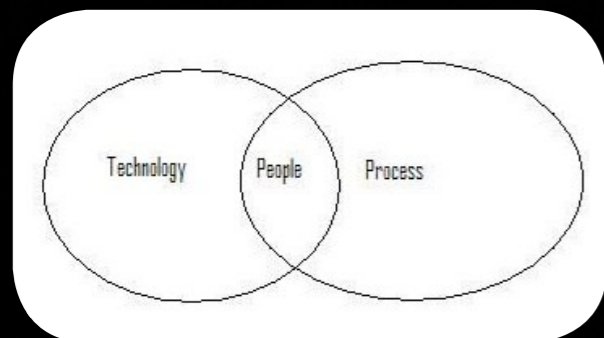


Figure 1

bilities to be fulfilled. It is therefore imperative that the entire workforce receives sufficient and good quality information regarding security responsibilities. Information security awareness is extremely critical to any organization security strategy and supporting security operations. In spite of the importance of making end users aware of their roles and responsibilities in reference to security only 64% of US organizations, 48 % of UK organizations and 59% of Indian organizations conduct security awareness programs in spite of the many regulations that make it mandatory. Many of the security incidents that resulted in Millions of dollars in penalties and loss of reputation could have been prevented by proper security awareness and training. This paper not only focuses on end users but also on the technical users and the senior management which are generally missed out.

What value does information security awareness and education deliver? Having a comprehensive and mature information security educational program will result in better health of the organization in terms of security as well as the organizational health. Let us now tabulate some of the risks that involve people factor and involves people which can be prevented by effective awareness programs.

Risk Seed	Threats	Medium of threat	Impact
Human Resources	Social Engineering	Phones, Instant messengers, posits.box mugging	Loss of Customer intimacy.
Human Resources	Password disclosure	Risk Seed	Loss of reputation, financial penalties.
Human Resources	Insecure software coding leading to various vulnerabilities.	Internal development environment	Loss of CIA and can also lead to Financial impacts

From the above table it is clear that Security awareness and training needs to be imparted to all members of the organization. Let us now see how an information security awareness program is constructed.

Pillars of Information Security awareness and education:

Right People, Management Commitment and Information security policies form the pillars of an effective security awareness and education program.

Information security policies:

Have well articulated and updated information security policies in place that support the vision and mission of the organization. Keep them current in line with the evolving threats and have a review every month by an Internal IT team. Have this review circulated to the senior management. This will ensure that the policies are updated and are being viewed by senior management thereby generating buy in.

Management Commitment:

Get Management Commitment before going ahead with a plan such as this. A mature enterprise wide security awareness program increases the security posture as well as the internal communication posture of the organization which will help foster cross functional effectiveness' and bring in a healthy working culture. Highlight to them the above advantages and get their nod. Getting their nod also sends positive signals across the enterprise that the management is seriously committed to improving and maintaining security.

Right People:

This is the number 1 ingredient for any organizational success. Having the right people on the team makes all the difference for making any plan/strategy highly successful. Always hire people by conducting a good background check for positions that require no experience. When hiring for senior/mid level positions make sure that people are cross checked across on all areas such as Education, Employment, Previous Employer References, groups, conferences, publications, personal history and check if they are committed towards excellence. This forms the ground for building the plan.

Form a team:

After having the right people on board, you will have to form a Core Committee involving and comprising members across the various business units. The team structure is very vital for success and is discussed below in greater detail.

Core Committee members:

The core committee members should comprise heads of members of all business sections. This will ensure that their support is there which is very vital for a successful awareness program. The CISO/Corresponding person who is responsible for security should also be part of the Core Committee.

Security Awareness Champions group:

Security awareness champions group should be formed which will include senior members across the business. People to be included in this group should exhibit at the least the following qualities:

1. Knows the business: The person selected as awareness champions should have a sound knowledge on business process. This will be very vital when mapping security risks with new process/policies/strategies of the organization.
2. Competent in their selected field: The person selected should be competent in his/her chosen field. This will ensure that he has the respect of his team members and peers which will be very effective for putting forth ideas in place.
3. Respected by peers: People chosen as awareness champions should be respected by peers in their respective departments. This will ensure team commitment as a person of such caliber will have his voice heard and respected across his team members.
4. Effective Communicator: People should exhibit effective/extraordinary communication skills. These people should be conversant and fluent in one or more languages. Examples include a person conversant in English and fluent in his native language say (Arabic), this will ensure that the diversity factor in organizations has been taken care of.

Security Awareness focus Group:

This group should consist of members across departments who are committed towards excellence and are keen to add value to the organization. These people should have the option of getting promoted as awareness champions as part of their commitment towards information security awareness.

IT awareness group:

This group will cater specifically to the Information Technology department. This will include senior members within the department and will keep a track of training requirements needed by the departmental people. This group will also measure the success of the trainings given to IT personnel. Formation of the team and team members should be done involving HR, Customer Service, IT and other sections and should have the approval of 3/4 of the core committee members. A sample hierarchical chart is given below for a reference. (Fig 2)

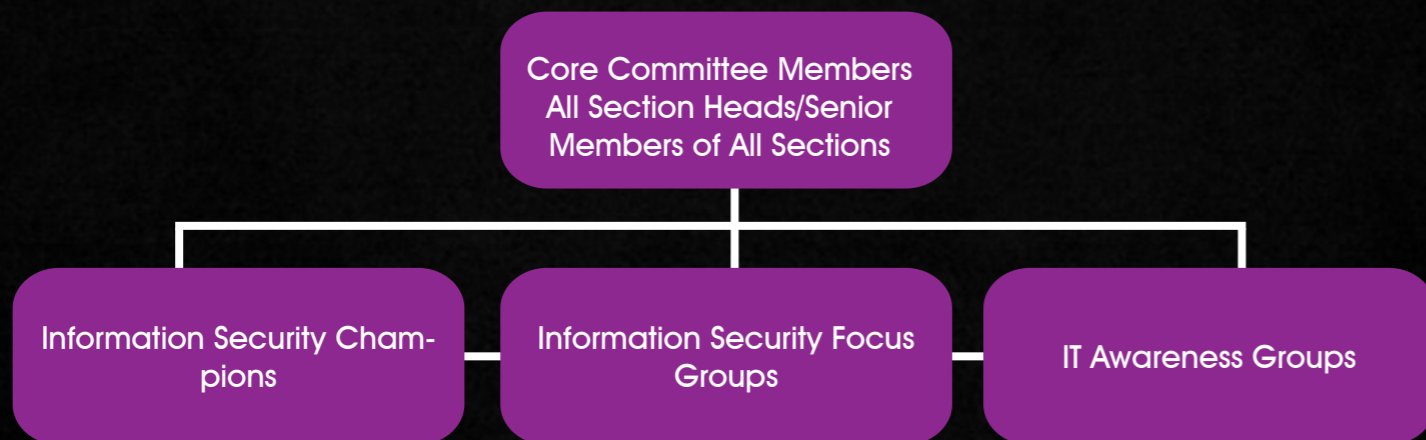


Figure 2



End user Security awareness Model: Figure 3

Identify Needs:

Not all users are equal. This phase will also identify the training needs of each and every individual mapped to their responsibilities handled by them. Training needs are assessed vis-a-vis responsibilities and impacts that can be caused by the responsibilities. Map responsibilities to system exposure, impact, and training needs. A simple matrix that can be used is shown below.

Since we go by the saying not all users are the same, the knowledge of each and every users in terms of security awareness, system expertise and computer knowledge are assessed individually through pre-assessment questionnaires developed by the Information Security Awareness champions. The information security awareness questionnaire should be prepared keeping in mind the normal end user to the advanced user. IT specific assessment questionnaires should be prepared for IT personnel and their knowledge on various domains tested periodically. It is recommended to use web based assessments through the organization intranet portal site for easy collection and improvements. This will also help us analyze gaps and improve knowledge levels of users. Based on answers collected and personal interviews with people classify their training needs and knowledge levels. Have them documented as per the sample format given below. The basic purpose of the sample report is to organize the article and provide an idea and is not intended to be comprehensive.

Needs Assessment Report:

Employee ID	Responsibilities	System exposure	Impact	Training Needs	Knowledge Level
1234	Payroll Processing	Fair	Loss of Confidentiality and integrity	Basic	Advanced
5678	Solving customer related issues through Phone calls, Emails and Service desk system	Good	Loss of availability, social engineering that could lead to financial impacts and loss of reputation.	Advanced	Intermediate
891	Floating purchase tenders	Fair	Poor quality equipments, leading to financial loss	Intermediate	Basic

We will describe clearly on what it means by basic, Intermediate and advanced.

Basic Training: Primarily for users whose ignorance can cause the least impact on the organization and their resources. Impact causes negligible financial loss and zero loss of reputation and integrity.

Intermediate Training: For users whose ignorance can cause some damage to the organization and its resources, but does not cause much financial loss and does not damage the reputation of the organization.

Advanced Training: For users whose ignorance can cause significant financial loss and damage of reputation thereby affecting customer intimacy and credibility.

Develop and Deliver: After doing a need assessment. Plan, Develop and Deliver security awareness and educational programs across the enterprise. Each process has been described in detail below.

Develop: This step involves gathering available training resources such as people, content and development of training material. The training material should be developed with the following points in mind by the security awareness champions and security awareness focus groups.

- *How do we want users to react/follow?*
- *What skills do we want the users to learn and apply?*
- *Will this content reach out effectively?*

There is series of materials available that requires to be imparted to each and every person in the organization, based on their responsibilities and level of knowledge that is needed, the scope of which is too large to be discussed here. IT service champions in consultations with focus groups must ensure that necessary areas have been taken care of. Classify topics required for each level.

Training Needs	Topics	Delivery Method	Schedule/Frequency	Audience
Training Needs	Review of Security policies and acceptance	Face to Face	New hires and Annual	Everybody
Basic	Laptop Security	Face to Face, Bulletins	Quarterly	Laptop users
Basic	Incident Management	Face to Face, Bulletins and handbooks	Bi Monthly	Help Desk Users

After comprehensive designing and planning, deliver the plan to the end users based on their training needs that have been assessed through various mediums that are available in an organization. The training plan and methods should be ratified by Core Committee, awareness champions and focus groups. General topics ranging from basic to intermediate can be given by Information security focus groups\Awareness champions whereas advanced topics should be delivered solely by information security champions selected from the IT department.

Evaluate and Improvise: Ideally after delivering the content, the end users must be evaluated under controlled environment to check if they have comprehended the topics properly. A post assessment report template has to be prepared to see if the outcome of the training is as desired. The Assessor must also get inputs from the candidate to see what can be improved in terms of content, presentation etc. All collections if done online will be easy to comprehend and deliver better results in future. Benchmark the current performance and continually improvise it for matured results.

Sample Assessment and Improvisation Report Template of Content and Assessor:

Presenter ID	Content	Delivery Method	Remarks of candidate
1234	5678	Webinar	Points can be split further which will help us comprehend better.
1234	5678	Face to Face and Webinar	Webinar was good but the presenter gave fewer examples in relation to password security.

Sample Candidate Assessment and Improvisation

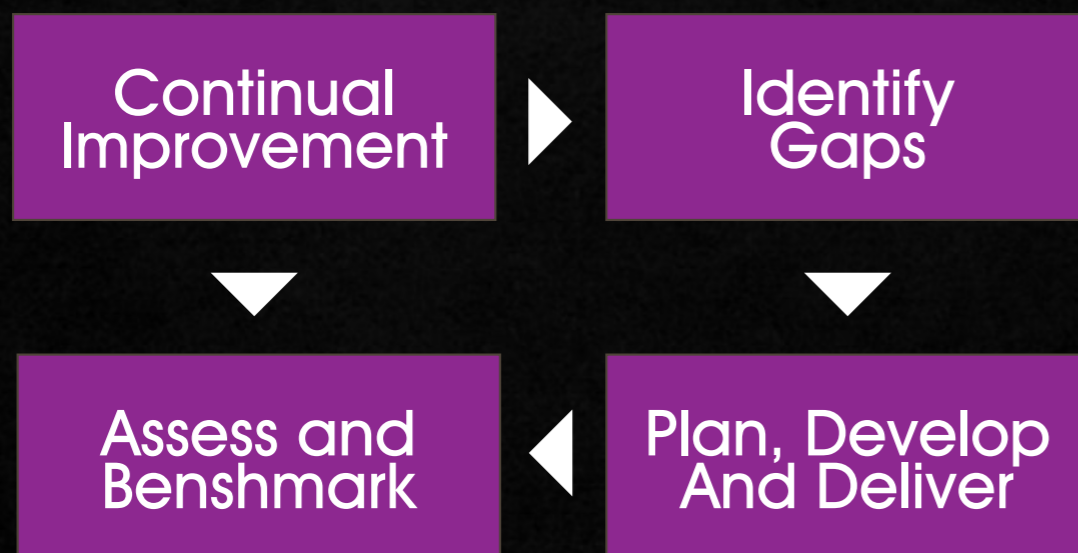
Template:

Employee ID	Topics	Password policy	Performance Score	Performance and remarks
1234	Wireless Security	Webinar	60 percent	Average performance, need to have a one on one session to make him excel.
5678	Password policy	Face to Face and Webinar	80 percent	Optimum performance must educate the user through bulletins and targeted Email to help him Excel. Next examination to be conducted next month same date.

The post assessment reports are stored in a repository accessible to all the security awareness champions, Core Committee members and focus groups. This will ensure that continual improvisation happens on a regular basis. The security champions can also develop a Department Based Grading system to check which department performs best and recognize them through internal newsletters. This will certainly improve the organizational health in terms of security and performance.

Information security education does not end with End users as is the case most organizations do, their own IT department also needs to be educated on a continual basis to keep them updated with the latest compliance regulations, evolving threats. The process has been described above.

Security Awareness Model for IT personnel: Figure 4



Identify Gaps:

The CISO/IT manager and the Information security personnel must conduct regular audits on their department people to check if they are equipped with the knowledge to handle evolving threats, knowledgeable on new standards, current trends etc. A “needs assessment” is conducted through needs assessment as described for end users.

Invest in Education materials: The organization must invest in good quality educational materials that are available for IT people such as ISSA, ISACA, ISC2, IEEE etc. By Investing in these journals and educational materials the organization is certainly bound to increase the learning curve of their IT people which will result in better codes, process improvements etc. These journals pave the way for identifying an effective needs assessment.

Plan, Develop, Deliver, Assess and Improve: After conducting a “needs assessment,” check to see whether internal people are qualified enough to fill the gap or not. If so prepare content and plan delivery methods for educating them. In some cases it becomes necessary to bring in external expertise to train our people. In such cases depending on budgetary constraints train the senior members/a group, and retrain them asking them to train other members. This way knowledge is resonated throughout the organization. Document the training, assess those using internal feedbacks and keep them improvising continually. IT based security educational needs must be done bi monthly for better quality to keep in line with evolving threats and regulations.

Conclusion

Information Security awareness and education is continuous and continual. With proper management support, right people, good team formation and involving all business units in the process we get their commitment which will ensure a successful security awareness and education to one and all in the organization going beyond security education and awareness to increasing cross functional effectiveness and organizational health.

References

http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_report.pdf
csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.



Vinoth Sivasubramanian

I am a founding member of ISSA UAE and a working committee member of International Cyber Ethics. CEH, ABRCCIP, ISO 27001 LA,

Enhanced Mitigation Experience Toolkit (EMET)



Everyday software vulnerabilities and their exploitation threaten the user information system and computing experience. Often, common applications like word processing, media players, browser and its extensions are used to reap the rich benefits for personal and professional productivity, becomes the target of these threats. A significant problem lies in the way these vulnerabilities are exploited, which requires no user interaction, as they get downloaded and executed simply by visiting a malicious website or opening a malicious downloaded document. A normal user wouldn't have any clue of what components of the browser or the running application is being exploited either for installation of malware for vicious purpose or for propagation of malware to other systems.

User and Enterprise rarely patch these third party products due to numerous factors like lack of availability of tools, half cooked or broken patching process, lack of security governance and organizational culture. The frequency of zero day attacks is on raise for the client side applications according to various vulnerability intelligence companies worldwide including IBM X-Force Threat reports. According to SANS report "The Top Cyber Security risks" the un-patched client-side software is on the top priority number one from the rest of the risks. It is interesting and frustrating to note that some of the vendors haven't patched the zero day vulnerabilities reported two years ago according to SANS report.

It is a well known fact that signature based Anti malware detection and removals technology products are losing the war as these technologies can't keep up with the wide variety of malware and its variants being produced on daily basis. The only solution which holds promise is to address these vulnerabilities at the very heart of the operating systems to counter various attacks exploiting the underlying operating system mechanisms. Microsoft recently released "Enhanced Mitigation Experience Toolkit" (referred to as EMET) version 2.0.0.3 in November 2010 for its fleet of client and server operating systems including Windows XP, Windows VISTA, Windows 7, Windows Server 2003 and 2008.

At the time of release, EMET was not supported by Microsoft. For the enterprise environments EMET's MSI format can be deployed either manually or by existing software deployment delivery mechanism/tool.

The success of EMET really depends on the acceptability of this tool in the user community and its wider deployment. The demand for its support forced Microsoft to support the EMET. Also, much needed feature for the success of this technology in enterprise market segment would be manageability of EMET by the group policy, without which chances of EMET deployment in enterprise market are dull. EMET will be another layer of defense in the defense in depth strategy in near future to mitigate or in worse cases delay exploits being successful on the target systems.

EMET mitigation tool looks really nifty due to the controls offered at the very root of the exploits taking on the Microsoft platform like stack overflow and address randomization. EMET offers mitigation techniques such as dynamic Data Execution Prevention (DEP is enabled by default on IE8), Structured Exception Handler Overwrite Protection (SEHOP), Heap Spray Allocation, Null Page Allocation, Export Address Allocation Table Access Filtering and Mandatory Address Space Layout Randomization. EMET kit offer granularity up to the single process. For more details of this mitigation tool and how does it work, please refer to EMET user guide (see the reference list at the end of this article). It will be prudent to enrol browsers, Acrobat Reader, flash players in the EMET to prevent exploitation of this application while surfing web sites.

Supported systems

EMET 2.0 supports the following operating systems and service pack levels:

Client Operating Systems:

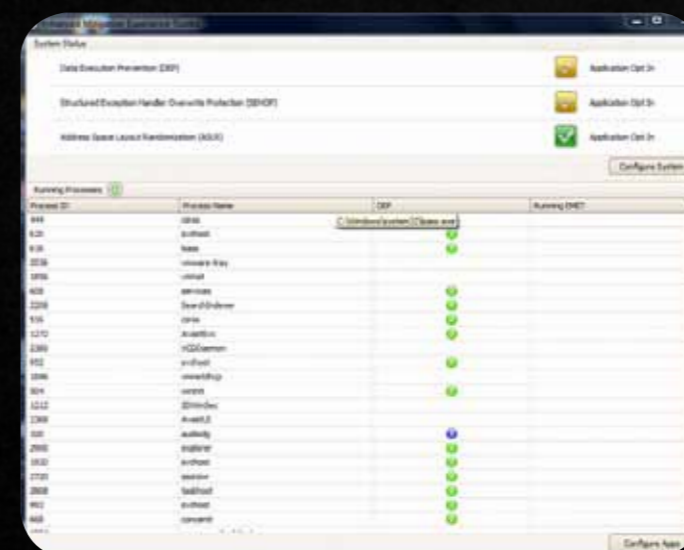
- Windows XP service packs 3 and above
- Windows Vista service pack 1 and above
- Windows 7 all service packs

Server Operation Systems:

- Windows Server 2003 service pack 1 and above
- Windows Server 2008 all service packs
- Windows Server 2008 R2 all service packs

Configuration of EMET

EMET can be configured using the graphical interface or by the commands.



Listing 1 - Main EMET configuration windows with the options per process and system wide configuration.

After you install EMET, you will need to specify how much protection to provide. Click on the configure system button as shown in listing 1. This will open a new window as shown in listing 2.

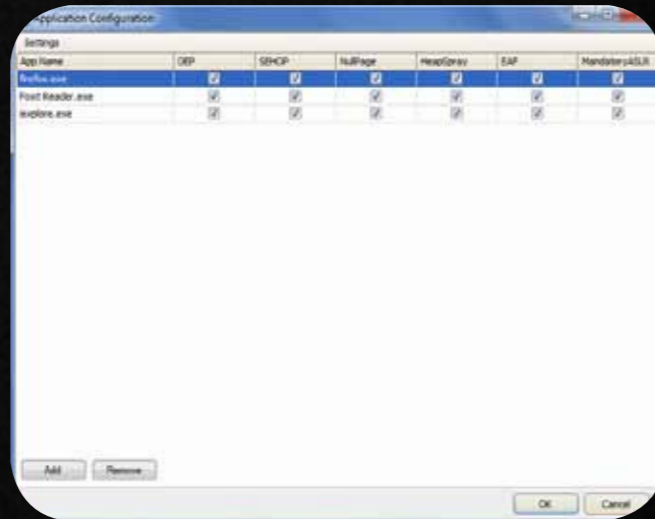


Listing 2 - System configuration

Next click on the configure application button and screen in listing 3 will come. In this, you can add application by clicking add button, this would protect the added applications. Finally, reboot your device for changes to take place.

Listing 3 - Application configuration

EMET is really a good control initiative at the fundamental causes of vulnerabilities in Microsoft products and promises another defense in depth layer for protecting the information systems. As user acceptance and demand for EMET raises, we will see further development of these tools for its integration via group policy. It will be good to see this tool being fully supported and managed via group policy in near future. Needless to say, this mitigation needs to be tested for deployment in the production environment as it may break existing application compatibilities therefore production implementation will require extensive testing before it can be deployed. Again, EMET could serve as another layer in the defence depth strategy.



References

- IBM X-Force Threat Report - www-935.ibm.com/services/us/iss/xforce/trendreports
- Microsoft Security Report - www.microsoft.com/security/sir/default.aspx
- EMET mitigates Adobe Acrobat Reader exploit- www.itwire.com/business-it-news/security/41804-microsofts-emet-mitigates-adobe-acrobat-reader-attacks
- Here is the video from the EMET developers- <http://technet.microsoft.com/en-us/security/ff859539.aspx>
- EMET user guide - http://blogs.technet.com/cfs-filestoragefile.ashx/_key/CommunityServer-Components-PostAttachments/00-03-35-03-78/Users-Guide.pdf
- Some proof in support of EMET preventing exploits on IE 6,7 and 8- <http://blogs.technet.com/b/srd/archive/2010/11/03/dep-emet-protect-against-attacks-on-the-latest-internet-explorer-vulnerability.aspx>
- More proof of Acrobat reader zero day exploits being blocked from execution- <http://www.ditii.com/2010/09/10/enhanced-mitigation-experience-emet-2.0-toolkit-blocks-adobe-reader-and-acrobat-zero-day-exploit/>
- Download link in case you wish to try EMET on your lab or home devices - www.microsoft.com/downloads/en/details.aspx?FamilyID=c6f0a6ee-05ac-4eb6-acd0-362559fd2f04



Naveen Sharma

I hold the CISSP, CISM, SANS GCIH and FCNSA certificates. I work for a top tier managed service provider in Sydney, Australia

مجلة عرب هاردوير ARABHARDWARE

مجلة تقنية شهرية للمبتدئين والمحترفين



- هاردوير
- سافتوير
- العاب
- هواتف
- شركات ومؤسسات
- وغيرها من الأبواب الشيقة

الآن في الأسواق

لمزيد من التفاصيل زورونا على

<http://magazine.arabhardware.net>



Cairo Security Summit

Cairo International Conference Center

26-29 APRIL

@ **CAROICT** 2012

International Telecommunication, Information Technology Trade Fair and Forum of The Middle East and North Africa

The Spring Of Technologies
From Dreams To Needs

Topics:

- **Track 1:** Mobile and Smart device Security
- **Track 2:** Vulnerability & Incident Management
- **Track 3:** Cloud & Database Security
- **Track 4:** Enterprise Security
- **Track 5:** Web 2.0 Security
- **Track 6:** Defensive Tools & Techniques
- **Track 7:** e-Commerce Security - Emerging trends and strategies
- **Track 8:** Hackers and security
- **Track 9:** Security of the National Broadband Network
- **Track 10:** Global Security Challenges

In Cooperation with:



24 Menouf St., off Orouba St., Heliopolis, Cairo, Egypt

Tel. : + 20 (2) 269 10792/3/4/5/6/7
Fax : + 20 (2) 241 59852

Join our group on



"Cairo ICT 2011" معرض مصر الدولي للاتصالات



securitysummit@cairoict.com



www.cairoict.com

Are you prepared to handle Cyber Security Incidents?

(CSIH)

CERT® Certified Computer Security Incident Handler

First Half - 2012	Creating & Managing Computer Security Incident Response Teams (CCSIRT)*: Jan 29 - Feb 1	Information Security for Technical Staff (ISTS): Apr 1 - Apr 5	First Half - 2012
	Information Security for Technical Staff (ISTS): Feb 19 - Feb 23	Creating & Managing Computer Security Incident Response Teams (CCSIRT)*: May 20 - May 23	
	Advanced Incident Handling (AIH): Mar 18 - Mar 22	Information Security for Technical Staff (ISTS): Jun 3 - Jun 7	

*: Courses CCSIRT & MCSIRT must be booked together
All courses include 5 stars coffee break & lunch



DRI page @ SEI:

www.sei.cmu.edu/partners/digitalrisk

Registration: www.digitalriskintelligence.com/register

info: training@digitalriskintelligence.com

Trainees should bring their laptops be able to run the labs

SPECIAL PRICES - CONTACT US

Rules of Usage:

- The Coupon is valid only from 1/1/2012 till 30/4/2012
- Coupon is valid only for one user
- The Coupon is valid only in the printed copy of security kaizen magazine not the online one
- You have to bring the coupon to the training center after cutting it from the magazine
- The Coupon is valid only in the following Authorized Training Center:
 - 1- Arab Security Consultants*, Nasr City, 02-22732620, Register online (<http://www.asc-egypt.com/ec-council-egypt/ec-council-course-registration.html>)
 - 2- NEN (6 October ,Nasr City ,Maa'di ,Mansoura ,Zagazig ,Assuit ,Suhag ,Ismailia ,Protsaid ,Arish) * Management Building : 6 October, Tel.:+20 (2) 3830 0048*





2day adv. 01000255359

الأُن العدد السنوي لمجلة سيكويريتي كايزن

أول مجلة متخصصة في أمن المعلومات في الشرق الأوسط

WWW.BLUEKAIZEN.ORG

SecurityKaizen

All EC Council Courses

30%
Discount
on..



- CEH
- ECSCA / LPT
- CHFI

