The False Sense of Security

Daniel Dumitreasa

SANS GSEC Practical ver. 1.4b
August 25, 2003

Contents

Abstract

Many people will generally agree that by having a false sense of security is overall much worse than knowing what level of security good or bad can be expected from any situation ahead of them. Obviously, this way of thinking may vary widely from a careless gambler to a responsible IT security manager.

Following, I would like to invite the readers to look at some of the widely spread IT security misconceptions that are creating a false sense of computer security to a huge number of IT users, from business managers to home computer users alike.

In spite of its broad title, because of its original purpose and the limitations imposed, this document is far from exhausting the proposed subject-better suited for a more ample work-and will only aim to offer a representative sample of the most common security misconceptions in this age of Information Technology.

Nevertheless, I hope this to be yet another invitation for reflection on this topic and to help raise computer security awareness on a larger scale.

Introduction

In opening, I will start by saying that this paper does not seek to be an IT security scaremonger of any sort. Rather, it aims to be a warning signal for all sorts of contemporary IT users intended to help them better understand the limited security of their IT assets, at this moment in the industry, and to enable them to choose the best way to deal with this fact of the computing life.

It has been said many times that “information is power” by the virtue that being better informed in life allows one to better choose the life navigation strategies and gives one a bit more power in front of this largely unpredictable world of ours. This is even more so in the IT world changing at a pace much faster that what we are used to.

It is commonly accepted that the security subject in general, and the IT security matter in particular, are essentially part of the business component at either the corporate or personal level, as it is all about risk assessment and mitigation strategies.

The bottom line is that when we will be better able to understand the risks involved in a life situation --and in the Information Technology in particular-- then we will be in a much better position to choose the best tradeoffs and strategies for staying in the race.

The danger for those users self-indulging in a false sense of IT security (which is simply not there) will become more significant for them as their dependence on the Information Technology will increase.

Increased Interconnectivity

Due to the impressive value brought by the wider human connectivity facilitated by the Internet technology, the acceptance of this new technology (together with all the benefits and its financial profits) has increased at a very fast pace. Unfortunately, the business drive is very much concerned with the expansion as a priority, while taking way too little into consideration some business protection aspects like the security matters.

The problem that has suddenly arisen is that the number of IT security incidents has increased almost proportionally with the number of the new Internet connected users. Based on an interconnectivity technology still in its infancy –at least as much as security is concerned -- the ever increasing number of Internet enabled users are now able to reach a much wider number of sites and people over the net.

The software technology, also not yet mature enough and always ridden with a myriad of software glitches--“features” for them or “bugs” for the rest of us--is still sold, in most cases, without any guaranties from the part of their creators and merely providing some best effort support plans.

That is, the ever full of glitches software industry–driven by lower costs and faster production cycles--is suddenly facing a wider Internet audience exposure and, inevitably, its security shortcomings are much faster discovered, publicized and exploited than ever before.

Therefore, while the IT technology has changed rapidly, the human mentality has not always kept pace with it and some people are still not realizing the business implications created by the wider exposure of this “yet not enough secure” connectivity technology.

In many cases, the IT business owners are looking at the benefits versus the losses--brought by the new wider interconnectivity--and are considering many security-versus-connectivity tradeoffs in the way they run their business.

While this is all right in principle, the main issue here is that many of the IT users and business owners are still very much underestimating the security vulnerabilities of their IT assets. Therefore, they may accept some wrong trade-offs, putting their company IT infrastructure at risk and their business in a position to be adversely affected by such network security related problems.

The reality, not anymore shocking for most of us, is that there is no such thing as a 100% security guarantee possible for an interconnected computer system or an infrastructure. Even more, today we may almost guarantee that any computer system or network infrastructure connected to the Internet, directly or by means of other proxy connections, may become vulnerable at a certain moment in time when the right number of software bugs will concur such as to allow a certain malicious intruder to penetrate it.

As they say, there is just a question of time until the software created to provide the business functionality--and rarely tested exhaustively for all the imaginable network attacks--will have a new vulnerability found and exploited in a context of some few security management trade-offs.

The majority of us do not know how to pick pockets or open locked doors and windows, but the much-specialized pocket thieves and burglars have spent quite a bit of time improving their trade. Likewise, the determined hackers will be able to find some exploits much faster than the businesses that they are praying upon can eliminate them.

This is also more possible today than in the past because the technology that is interconnecting us, in a faceless and less personal fashion, is enabling the hacking community to share security intelligence and exploits much faster and more organized than before, and therefore empowering them to be more informed and effective in their network attacks.

The message here is that it is just a matter of time until the next security vulnerability will surface in the software used for business, on the server, on the firewall or the router and especially in the end-user workstation.

Then, when that time will come, it will be just a question of chance for a hacker to be there to exploit the vulnerability and for the business owners to pay the price of their security trade-offs strategy.

The Laws of IT Security

Based on either a simple ignorance or maybe some crass misconceptions in the IT security field, a network safety feeling may determine a user or a business to exchange sensitive information with a third party over the Internet, while using a proprietary email encryption algorithm with no user passwords. Furthermore, their workstations may be directly connected to the Internet and one of them may not have a patched Operating System but may be using an up-to-date virus scanner.

Therefore, they may believe that their communication is at the same time confidential (because of the label “encryption algorithm”) and that therefore their information cannot ever fall in the wrong hands. In such a situation, they will exchange unreservedly some confidential information that may be intercepted by a third party, and may be exploited for their fraudulent uses directly or corroborated with some other information.

This type of security incident may be caused by either their ignorance of some security laws or an overestimation of the security protection offered by certain technologies.

From the ancient Roman law system, the lack of knowledge of a public law was never an accepted excuse for trespassing it. The jungle law is not much different and often the price paid for ignoring it is much dearer than for the other cases.

In a similar way the security laws of the Internet jungle are also punishable, if ignored, by business disruptions or downtime at best, or by information loss, data corruption or leaked into the wrong hands and thereafter usable for fraudulent exploits on the expense of the rightful owners.

The laws of IT security, much like the laws of science, are in continuous discovery and refinement, and various people and groups have attempted to formulate some of them. For the readers' convenience, we will reproduce some of them below, but probably many others in the industry may come up with their own definitions.

As an example only, the people at Microsoft–a company considered by many to be responsible for much of the IT security-caused grief on the planet--have started some sort of Security Essays series published on their TechNet web site.

On that publishing space, while attempting to capture some laws of IT security, Scott Culp--Microsoft's Security Response Center Manager-- and his team have listed their "Ten Immutable Laws of Security" [1]:

If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
If a bad guy can alter the operating system on your computer, it's not your computer anymore.
If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
If you allow a bad guy to upload programs to your web site, it's not your web site any more.
Weak passwords trump strong security.
A machine is only as secure as the administrator is trustworthy.
Encrypted data is only as secure as the decryption key.
An out of date virus scanner is only marginally better than no virus scanner at all.
Absolute anonymity is not practical, in real life or on the web.
Technology is not a panacea.

Then, after they have considered another dimension in the play (i.e., the point of view) they have formulated also their "The Ten Immutable Laws of Security Administration" [2]:

Nobody believes anything bad can happen to them, until it does.
Security only works if the secure way also happens to be the easy way.
If you do not keep up with security fixes, your network will not be yours for long.

It does not do much good to install security fixes on a computer that was never secured to begin with.
Eternal vigilance is the price of security.
There really is someone out there trying to guess your passwords.
The most secure network is a well-administered one.
The difficulty of defending a network is directly proportional to its complexity.
Security is not about risk avoidance; it is about risk management.
Technology is not a panacea.

Then, viewed from another angle, here is yet another set of security laws as proposed by Ryan Russell and collective in [1]:

Client-side [i.e., “end-user computer”] only computer security does not work.
One cannot securely exchange encryption keys without a shared piece of information.
Malicious code cannot be 100 percent protected against.
Any malicious code can be completely morphed such as to bypass signature detection.
Firewalls cannot offer a 100 percent protection from an attack.
Any intrusion detection system (IDS) can be evaded.
Secret cryptographic algorithms are not necessarily secure.
If a key isn’t required, one does not have encryption but only encoding.
Passwords cannot be securely stored on the client unless there is another password to protect them.
In order for a system to begin to be considered secure, it must undergo an independent security audit.
Security through obscurity does not work.

While we may or may not agree with all of them as being accurate or even having a law-like status, we should reflect on their wisdom as many of them are or may be quite near to the reality.

The false sense of security

Experience has shown that many IT managers and system administrators tend to indulge at times in a comfortable false sense of security by falling into some security traps or ignoring some of the above security “laws.”

However, the home users are also, for most of the time, indulging in the comforting feel of computer security because, it is certainly preferable to considering the cold reality facing their lack of expertise and the ever-increasing complexity of the software they are using.

Anyway, as the acknowledged security risk levels are rather a part of the business management, the business risk accepted is often different from the technical security risk posed by a certain security situation. Therefore, many managers will argue–sometimes rightly--that a technical security risk may not always constitute a similar level of a business risk for a certain company.

While this is certainly true in many occasions, the problem here is to understand properly all the ramifications of the business risk introduced by certain security vulnerabilities.

Following, I will try to explore briefly some of these computer security myths, commonly circulating in the IT community.

Technology Myths

SSL Protection Myth

Many of us have already encountered many Internet sites that are trying to reassure us about their security just because they use SSL. Prosise C. and others are looking in [10] at the SSL trust issues and their wrongly assumed blanket security. We will review some of their comments here:

We are often seeing advertisements like "Your transactions are protected by SSL." What is it suggested by that? Do they imply that the SSL protocol will protect also the web server and application?

Here it has to be clarified that SSL has not intended to secure the operating systems or even the web application, but merely to secure the data in transit. Sometimes, as we may see later, even this last aspect may be questionable. However, the SSL protocol by itself does not eradicate or mitigate any vulnerability on the web server or application [10].

As expected, at the server end of an SSL tunnel it will always be the same class of web server programs, applications, CGI scripts, or back-end databases as on any regular, non SSL-enabled web site. However, many users, IT managers and administrators may assume that the SSL-enabled web servers are automatically secure because SSL uses strong cryptography. In reality, the SSL-enabled web servers are vulnerable to the very same attacks that may affect the regular web servers.

Lack of Regular Auditing and Constant Monitoring

While the useful encryption feature of SSL offers the much needed traffic protection, it does also create problems for the system administrators trying to use the currently available vulnerability scanners or intrusion detection systems [IDS] to audit or monitor their SSL transactions.

The IDS will monitor the network traffic for unauthorized activity and will attempt to flag any policy trespasses, but in order for it to function, the IDS must be able to view all traffic. The problem is that the SSL encryption renders the HTTPS traffic unusable for inspection.

Subsequently, while there are many security scanners that audit the regular web servers for known vulnerabilities, such scanners may not check also the SSL-enabled servers. The SSL-enabled servers may very well have the same web vulnerabilities as the regular kind, but unfortunately, some security scanners may not be able to audit them.

The lack of network monitoring combined with the missing vulnerability auditing leaves the SSL enabled servers unprotected by the audit component of the security maintenance.

The SSL traffic protection solution

Now, let us examine the security protection potentially offered by the SSL traffic itself.

Many SSL users are under the impression that by using SSL traffic encryption their confidential data exchange with the SSL-enabled web site is secure and nobody could eavesdrop on this information exchange.

Like in many other instances with so many good ideas, the practical result depends on the quality of the implementation.

Depending on the level of encryption [cryptographic algorithm strength and the key used], the traffic may still be decrypted (at various degrees of speed) in a certain useful period. Then, if the respective SSL product used by a certain web site has some not patched known vulnerabilities, its protection strength is as good as the chance for a hacker to find it and exploit its vulnerability.

SSH Header Protection

Many of us may have been, at least at a certain point in time, under the impression that an SSL connection encrypts the entire information exchange and whatever is sent through it, is always secure as long as it is using a strong encryption algorithm.

This is, again, not necessarily true and depends very much on the web site development work.

That is, because the SSL header is not encrypted and if the web developer chooses to store some user related information (like the user name, account, transaction steps, site navigation info) on the web query line, that information will be sent visible in the web page HTTPS header even if the rest of the message is SSL encrypted. Therefore, somebody listening to the SSL web traffic may collect some information like the user name and account, site navigation details, etc., even when the rest of the SSL message is encrypted.

Cryptography Protection Myths

Quite often, we may see some product advertisements offering VPN solutions based on their proprietary encryption [i.e., non-standard encryption algorithms], or even using some already known insecure algorithms with rather short keys [like DES].

While the proprietary encryption algorithms may claim to provide a certain cryptographic strength, more often than otherwise, these algorithms have not been reviewed by the cryptographic community and may very well be prone to some conception or implementation errors that will render the product useless when discovered by a hacker.

Other times we may even hear about products using some IETF standards like IPSec, and someone may automatically consider them secure because of the good publicity of the standard. Quite often, many may just overlook the fact that the standard protocol also allows for bad implementation choices like some weak authentication and weak cryptographic algorithms.

Anyway, an uninformed IT manager may be very happy to buy and implement an extranet VPN solution just because it is based on the IPSec protocol, and may easily overlook the fact that it may use a weak set of encryption policies or even a weak authentication method for the IPSec pairs.

Well, like always, the devil is in the implementation details.

More often than not, the employment of some strong cryptographic algorithms may not always provide an overall reliable encryption solution.

While it is rather easier to discard some solutions based on published weak cryptography, regular computer professionals and often even security professionals, tend to believe that a product using any reputable strong cryptographic algorithm with a long enough key is always a secure solution.

In reality the situation is not that clear cut here either.

Bruce Schneier very well addresses this in [8] :

“Strong cryptography is very powerful when it is done right, but it is not a panacea. Focusing on the cryptographic algorithms while ignoring other aspects of security is like defending your house not by building a fence around it, but by putting an immense stake into the ground and hoping that the adversary runs right into it. Smart attackers will just go around the algorithms.

A cryptographic system can only be as strong as the encryption algorithms, digital signature algorithms, one-way hash functions, and message authentication codes it relies on. Break any of them, and you've broken the system. And just as it's possible to build a weak structure using strong materials, it's possible to build a weak cryptographic system using strong algorithms and protocols.”

Further, there may be no better ways to put it as he says it so admirably:

“Building a secure cryptographic system is easy to do badly, and very difficult to do well.

Just because an encryption program works does not mean it is secure. Functionality does not equal quality, and no amount of beta testing will ever reveal a security flaw. Too many products are merely "buzzword compliant"; they use secure cryptography, but they are not secure.”

Basing the security of a system or network only on the encryption solution, it is certainly just another case of indulging in the dangerous FSS [False Sense of Security].

Secure Email a PKI Solution Myth

The Public Key Infrastructure [PKI] technology is usually about the digital certificates obtained from a commercial or corporate certificate authority [CA]. This technology, like many other new security ideas, is sometimes much hyped as another panacea for our security problems.

Like any other aspects on the security front, this PKI technology is also not the only proper security mitigation response as it may have its own share of actual or potential flaws.

It has been said many times that security is a chain only as strong as its weakest link. The security of any CA-based system is based on many links and they are not all cryptographic. In this case people are much involved throughout the entire [certificate granting] chain and will weaken the solution.

The very good paper by Ellison and Scheier [9] discusses many of these potential PKI risks.

Basically, the main issues of the PKI technology are related to the following aspects:

The person issued with the certificate is indeed the one who says it is.
No certificate could be issued fraudulently to a person [not being the one the certificate claims to be].
It should not run the danger of a confusion of digital identities when the names are identical or almost.
The PKI certificate should be only used by its legitimate owner.

Many times, because the users will prefer the convenience before security and the commercial CAs will prefer to maximize revenue before anything else, many shortcuts may appear in the process.

As such, the users may not use any passwords to protect the certificate (actually its private key), and therefore it may be used by anyone controlling the computer system storing the certificate. In addition, the Certificate Authority may issue the certificates over the web without properly verifying the user’s identity, etc.

From the above major points will stem many questions like:

Can the CA (Certificate Authority) be compromised through theft of signing key or even corruption of personnel?
How did the CA signer know the information being certified without meeting the person requesting the certificate?
How does the CA make any evident difference between people with the same or slightly different names such as to clearly avoid confusion and to cut out fraud?
Can the certificate issuer guarantee that the key holder controlled the associated private key?
Does the software application agent check for key or certificate revocation?
How well are the computers at both ends protected?
Is the encryption code itself protected from tampering?
Are private keys protected by password, and if so, how strong?
Are they used in tamper-resistant hardware or merely in software?
Can a physical passer-by sign something with the signer's key or tamper with the software or public key storage?
Can a virus or Trojan horse make use of the certificate instead of the legitimate user?

From all the above we may realize that neither this technology can be considered as always safe to rely upon, because of its many human factor implications.

IDS Protection Myth

The Intrusion Detection System is generally an useful method to spot known network attack patterns--like a virus or a worm code--and could also detect unusual traffic patterns that vary from the statistical normal.

The problem that appears with IDS is that if an intruder will craft a special attack code, not yet present in the IDS collection of signatures, that attack will not be noticed by the IDS. Sometimes it is only required to change some few bytes in the entire code for the pest pattern such as to not match anything in the IDS stored collection.

The other problematic aspect of the IDS solution relates many times to its maintenance and log review procedures. If the tool is poorly tuned to the local network conditions, it may produce a very big list of false positives that will quickly tire the log reviewers and will make them trust less and less the log contents. Unfortunately, in the sea of false alarms there might appear, at times, some correct alarms about some encountered real attack patterns. The usual problem may be that the boring human log review may be done irregularly and the real pest patterns spotted may be lost through the big number of false alarms.

These two aspects are making this solution, while useful in some cases, certainly not fully reliable to protect a network. Recently, the Gartner Group has released some research reports looking at the ineffectiveness of IDS.

Firewall Protection Myth

While much has been discussed in the media about the firewalls, it should be clarified that while very useful, they can protect the network from only certain types of attacks as well as providing some useful logging.

Unfortunately, for many users, administrators and IT managers, a reputable firewall solution --at the gate-- may let them believe that their network is securely protected against any network security problems.

Briefly, we will now look into some of the aspects that will adjust to reality this myth also.

First of all the firewall cannot protect the network against anything coming from inside the network. Disgruntled employees, physical security access to network devices and computers, internal modems dialing out to external network, unauthorized wireless networks, pests (worms, etc.) brought on various media (floppy, CDs, etc.) are among the things that a firewall cannot protect against, but will still affect the internal network.

About the dangers coming from the malicious inside employees, the Gartner Group has published quite an interesting report [5].

While leaving aside for the moment the above issues, even the traffic that may pass through firewall may produce some serious security problems.

For example, a legitimate HTTP connection starting from the inside to an outside IP address may be allowed by a firewall. However, it may not be initiated by an actual user but by a Trojan horse program just downloaded on the user's PC.

Any user with an Internet access may potentially download a new virus or Trojan horse in such a way to not be detected by the IDS system and to be allowed by the firewall coming as the normally allowed HTTP traffic.

Then, while the company may have its email, DNS and web server protected in a DMZ, any legitimate traffic to these servers will be allowed by the firewall. Nevertheless, in case such allowed traffic may take advantage of a recently published vulnerability in the mail server or any of the web servers, the situation becomes hot. An intruder may first take control on a DMZ host through the firewall allowed protocol, and then initiate a communication from the DMZ to its remote base over some traffic that may very well be allowed by the firewall.

After taking control of the web server [in case it falls to an exploit over HTTP], an intruder may use it as an attack base for all the servers on the same subnet or on the internal network. All that may happen while maintaining the HTTP channel communication with the external intruder's site.

In another case, if the web application is connected inside to a back end system [database, etc.], depending on the way the application has been developed, it may also allow for attacks –like SQL injection, cross site scripting, etc.- that will be perfectly allowed by the firewall. Using these types of attacks, a skilled hacker may directly affect the integrity of the data on the backend system, without even penetrating the network.

There may very well be also some other direct attacks of the firewall itself from outside or maybe penetration attacks using some improper firewall configurations with more relaxed rules than the business needs would dictate.

The human factor in the firewall configuration and maintenance issues has been known to produce insecure configurations, caused by some too relaxed or obsolete rules, typos, IP address mistakes, etc.

In conclusion, while the firewall cannot be guaranteed to always fend off all the external based attacks, it certainly cannot defend against the inside originating threats. A good discussion on this subject may be found in [1].

Secure Web Application as the Last Frontier

When all the above aspects have been cleared, resolved or at least mitigated, one of the last defense frontiers will remain the application itself. This part, quite often ignored, is about the attacks on the web application conducted by using some legitimate web input form but filling it with unexpected data for the web application.

This class will include anything from the web related buffer overflow type of attacks to the more subtle forms of attack by SQL injection and cross-site scripting. These may come independent and in addition to any other web technology related vulnerability.

All of these attacks are rather well known attack techniques, but this fact does not appear to reduce their spread in the field.

There may be quite some few companies using expensive firewalls and network defense methods to protect the access to their financial data, just to have their back-end financial data altered through an SQL injection through the front web site. Even worse, this access may go via the regular web channel using the SSL protocol, and may not be logged by the firewall or even detected by any IDS [because of the encrypted traffic].

However, if the responsible manager does not know about them, it may not hurt him for a while.

People Traps

Next, I will briefly explore some other security misconceptions widespread in the corporate world and relied upon by so many IT and security managers.

Trusting the Inside Network and the Insiders

Some IT managers are proudly stating that they trust their internal users, and therefore they do not consider protecting their IT assets from the “internal threat.” Just like this, they will step into the trap.

The Garner Group research [5] does report at large about the potential inside malicious employees and their costs for the company.

However, even if the personal integrity of the internal users will not be discussed here, the state of the computer technology, the lack of users’ knowledge and the potential variety of network backdoors are (see the Firewall-related section above). This situation may just have a “Trojan horse” code passing through the gate and attacking the prized IT assets from an inside vantage point.

Trusting People and Not Technology

Probably quite a few of us have heard at times system administrators or IT managers saying, “We do trust these people or those external partner companies, so we should allow them to connect to our network unrestricted.”

Well, we may trust the people’s integrity individually or as a company, but this trust should not be confused with trusting their systems, networks and the technology they are using to connect to our network.

Simply put, they may fail to be well defended on their own against network intruders (because of their lack of knowledge, financial or human resources, recent destabilizing changes and events in their organization, etc.), and somebody using their systems (and even maybe their credentials) may benefit from this trust and fraudulently access your network.

There is a perennial degree of confusion between the human integrity trust notion and the network security trust and many times this may prove dangerous for the IT side if not carefully controlled.

Well Established Security Policies

It is not unusual for an IT manager to develop a sentiment of security when his organization has adopted and published a collection of security policies relative to their IT operations.

Nevertheless, once again if relying solely on a security defense like this one, the false sense of security is just a small step away.

Even the best people are not machines, and they may make mistakes in the procedures used, which may lower the security of a network. Therefore, without a policy enforcement plan–in addition to the policy adoption--or at least a regular audits program, the security of a network cannot be really maintained.

Other Security Administration Myths

In order to conclude this sample of security traps, misconceptions and myths, I will just mention briefly some other favorites:

A network intruder may not be always after defacing a web site or produce havoc on the network, but this does not mean to be somehow less dangerous. Chances are to be exactly all the contrary.

Regardless of the big amount of money invested in security defenses in a company, by not maintaining it continuously (patches, audits, policies, etc.), in a very short time it will stop returning what was expected out of it.

In an organization made up of a mix of some security conscientious people and some security-ignorant others, the lower denominator will often set the security practice level.

Conclusion

If whatever you have read above did not make you reflect on the very poor condition of the computer security in this IT age, then please also note that most software bugs are discovered, sometimes, long before publication.

This situation happens in order to allow time for a cure and its deployment before the exploit is published. However, that will tell us that at least some people have already discovered the vulnerabilities and it is only reasonable to presume that not only the good guys may be part of this group.

This fact should also tell us that, right now, there should be already a good collection of not yet published software vulnerabilities, discovered by some few and used maybe only for their own interest.

At the same time, in their rush to add new functionality and improve the Internet user experience, many Internet enabling software companies are releasing code (for some fancy graphics or multimedia support, etc.) that can be often exploited.

Are we facing a computer security risk every day while browsing the Internet? The response is, for the moment, yes, certainly we are!

Can we absolutely trust our computer systems? Not really, and if we will do it, we will just kid ourselves.

Are the home users doing enough to protect their information stored on or exchanged through their computer? Certainly not, because the issues are more complex than ever and the average computer users are just left in the dark at the mercy of the software manufacturers offering cryptic products with no guaranties of any kind and especially not security.

Will we soon win the race against the insecurity of our computers? Difficult to say right now as long as the main software industry interests do not appear to be really seriously focused towards the security of our computing experience in a much similar way to the film industry's interests for quality movie productions versus more revenue from any kind of products.

However, as the last of the "Ten immutable Laws" of security states: Technology is not a panacea" [2] and we should never expect a quick security solution from any unilateral approach to fix it.

References

[1] Russell, Ryan, and collective. "Hack proofing your network" Second Edition". Syngress Publishing Inc., 2004, Chapter 2: "The Laws of Security".

[2] Microsoft TechNet. "The Ten Immutable Laws of Security". Microsoft Security Essays, URL: http://www.microsoft.com/technet/columns/security/essays/10imlaws.asp

[3] Scott, Culp. "The Ten Immutable Laws of Security Administration". Microsoft Security Essays, Nov. 2000. URL: http://www.microsoft.com/technet/columns/security/essays/10salaws.asp

[4] Bradley, Tony. "Internet/Network Security", URL: http://netsecurity.about.com/cs/generalsecurity/a/aa061403_2.htm

[5] Mogull, Rich. Gartner Group Research. "Danger Within" in "Security in a world without secrets". URL: http://security1.gartner.com/section.php.id.3.s.1.jsp

[6] Fisher, Dennis. "Open Source: A False Sense of Security?". eWeek- 30 Sep. 2002. URL: http://www.eweek.com/article2/0,3959,562220,00.asp

[7] Schneier, Bruce. "Why Cryptography Is Harder Than It Looks", URL: http://www.counterpane.com/whycrypto.html

[8] Schneier, Bruce. "Security Pitfalls in Cryptography", URL: "Security Pitfalls in Cryptography". URL: http://www.counterpane.com/pitfalls.html

[9] Prosise, Chris and Shah, Saumil Udayan. "SSL: A False Sense of Security". URL: http://www.zdnetindia.com/techzone/resources/security/stories/28863.html