

Network InSecurity

By Geoff Shively, CTO and Co-Founder PivX Solutions LLC
And

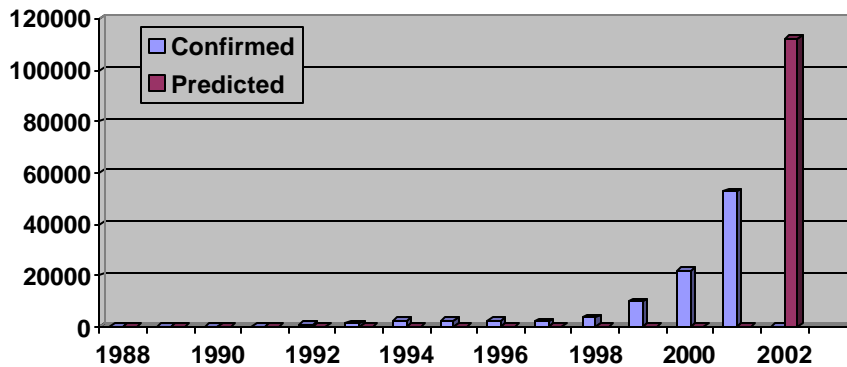
Instructor-University of California Riverside-Cyber Crime and Intrusion Detection

> Foreword

When inter-networks were first created, the concept of cyber crime was far from the focus of anyone's attention. However, such a technical insignificance as inter networks would someday change the world, and it was based on a naive premise of pure trust. This was a trust that no one user would commit any wrong, unethical, or downright criminal acts against or on this medium. This concept, this idea, this thought that now functions as a vital part of most people's daily lives is known as the Internet.

This technical brief will overview the inherent flaws that plague the internet today, making it vulnerable to corporate espionage, money laundering, grand larceny, trading frauds, and worst of all, cyber terrorism. We are in a new time, with old technology and old ideas funding newer technology. To be a success as a technological society, we must re-structure our core infrastructure for the needs and capabilities of today's Internet. A simplistic example is that of AOL Instant Messenger ® software, with a statistic stating that Instant Messenger ® usage is on the rise, with over 100 million users. A typical school day afternoon of trading mp3's and chatting, can turn into a backbone capacity of over 75%. Not only are we ill-equipped to handle such large masses of traffic, but this leaves us open to smaller attacks on the core infrastructure that would result in a more grandiose affect than it would at a lower backbone capacity. Therefore, there are currently millions upon millions of Instant Messenger™ software clients that remain insecure and a constant real time threat to corporate and home networks worldwide.

The Internet has grown exponentially in the last decade, as has the Internet Security, or 'IS' industry. Security services and products have risen to a multi billion dollar market in 2002 from a million dollar market in 1989. As you can see, the growth has been exponential to say the least. The chart below confirms the rise in *reported* domestic incidents.



Source: FBI and CERT January 2002

Please note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time.

Many InfoSec industry professionals predicted that in 2002 the amount of cyber security incidents would almost double. As the numbers prove you can see they did more than double. Currently, researchers and security analysts are stating that they believe we will see another large increase, possibly up to five fold.

> Firewalls

What is a firewall? The actual definition of a firewall states that “*A Firewall is a configuration of hardware and software that acts to enforce a security policy for a network.*” All too often, a firewall is simply a device that users and administrators ‘must have’ for network protection and security. Unfortunately, having a firewall installed doesn’t guarantee security. In fact, it often gives it’s users a false sense of security. Most have heard that the Internet is full of hackers, crackers, and criminals taking advantage of every opportunity to steal your information, and destroy your computer or network. Most of us have also heard that the all-in-one solution to this problem is a ‘Firewall’. The concept seems to be so comforting, and the term so impressive, but this is not the reality. Sadly, this is the train of logic that most network administrators use when laying out their security policy. Ironically, if you refer to the definition of a firewall, it reads that a firewall *enforces a security policy*, meaning that for one to work, you must have an idea, or know what you want it to do for you, down to the finest hair. Hacking, cracking and the anomalous traffic perpetrated by cyber criminals is a moving target. If a network administrator was to have established a lock tight set of firewall policies today it would likely need to be updated tomorrow. Again, without an appropriate security policy in place that takes into account the myriad of variables and has dynamic features to accommodate the constantly changing variants and exploits, it is almost useless.

Current firewalls have rule sets and “if” statements so that when an attack comes in from some cracker, the firewall can take the steps needed to block that attacker and any other unauthorized service from entering the network. This is all necessary, of course, but it often precipitates situations like, for instance, when it detects/perceives an attack that is not really an attack, and thus blocks a service. As a result, a client’s web site or server farm is down until a technician can personally come out, conduct a thorough investigation, and subsequently reset everything. This can take hours even for the biggest of companies. And, there are significant costs associated with downtime. According to the Association of Contingency Planners the cost for every hour of system downtime ranges from \$89,000 per hour for airline reservations to \$6.4 million per hour for financial institutions.

Lastly, firewalls can only detect and protect an incoming downstream data line, leaving the internal network traffic untouched, and unseen. Let me take this into the physical realm for a moment. If you were to spec an alarm system for your brand new BMW™ M5, would you choose one that only protected the cabin, leaving the engine unprotected, though the engine bay is the easiest place from which to disable any alarm? You would choose an all encompassing alarm system that covered every exterior panel, to every interior switch or button incase something failed during the moment of truth. This same ideology applies to the cyber world even more so, due to the fact that someone could break into your network, take information worth one hundred BMWs, and leave without starting an engine, or sounding an alarm.

> Intrusion Detection

Many problems plague the existing hardware and software IDS. First off, they are prohibitively expensive. Enterprise software systems go for upwards of \$100,000 for a one-user license. But no matter how expensive, you still need a security expert to monitor it, and must rely upon the software manufacturer for security updates. In many cases, old bugs are exploited during an attack, but once you go after a big time name, like Microsoft®, you have to have the most current exploits and tricks at your disposal.

Additionally, IDS and monitored firewalls monitor the Internet connection on the same line that it is protecting. A rather inefficient method that uses half of the bandwidth for the actual service they are protecting, and the other half to mirror the data and send it to the remote monitoring system.

Though you may have covered all of these bases, and you have a bright and shiny new intrusion detection system it's still not enough to keep out a determined hacker. Let's also assume you have a highly paid administrator, capable of reading and processing thousands of flags a minute. We will assume you have an ample amount of bandwidth to support the needs of offsite monitoring, though with all of these things, you still must have a reactive solution, as well as a proactive one to keep your network afloat. Without these two key elements, your network will not stand a chance against a single skilled cracker, or an army of them pre-programmed to infiltrate and destroy your precious IT investment and its underlying data and the customers and employees ability to access it.

There are web sites that specialize in posting security flaws and exploits, like www.rootshell.com and www.securityfocus.com. They post the latest and greatest security holes as soon as they are discovered. Again, you must have an administrator who has the time and resources to be diligent enough to check these sites, participate in IRC's, download the patches and then to install them, all while continuing to do the other required functions of his or her daily job. In an environment where IT expenses and labor costs are being watched like hawks by CFO's and Wall Street alike, most companies are hamstrung in this critical area.

> True or False

Another key problem is that routers, firewalls, and most intrusion detection devices are true on a network, and can be attacked themselves. This allows the entire network to be disabled from an outsider, no matter how redundant the network. MAC stands for *Media Access Control address*, which means that a MAC address is the physical address of a device connected to a network; which is expressed by a 48-bit hexadecimal number. This number, the MAC address, can easily be spoofed, or cloned by another user on the network segment.

With the ability to easily discover a machine's true MAC address, there is the same ease of execution in spoofing and cloning a MAC address to produce a variable network Armageddon. If an attacker decides to spoof a machine's MAC address, they take on the identity of the spoofed machine. The MAC that once belonged to that machine is now assigned as a unique identifier on the attacker's hijacked machine once two machines are using the same addresses. When cloning a MAC address, for the purpose of re-directing the traffic, the attacker will receive all of the raw traffic that was once intended for the now cloned machine. This data could have been on its way to an enterprise level server that may be housing credit card transaction logs, patient medical records, vital

accounting data, or simply personal files. As a frame of reference, a common network intrusion detection system or a robust firewall all possess a MAC address of their own, which can be spoofed or cloned at will, taking the unit that routes all traffic to your network offline as though it does not even exist.

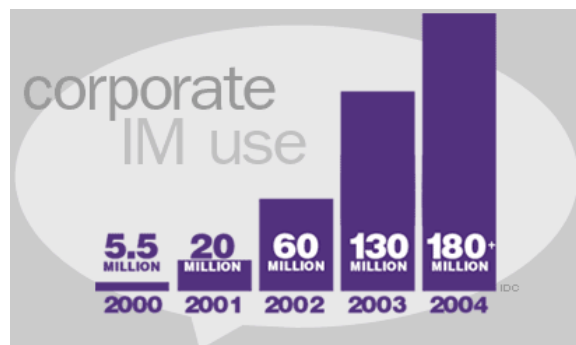
This is obviously a severe problem, and could be catastrophic if an attacker automates the process of spoofing addresses, taking down your key routers, firewalls, and servers within a matter of seconds. This problem has yet to be addressed by a single security company, leaving this inherent security flaw wide open, thus leaving your key infrastructure and valuable corporate data completely vulnerable without a fix in sight. An ideal solution would be to create a device that lacks not only a MAC address, but an IP address as well. A device such as this would be 'untrue' on a network, and thereby it would become undetectable, un-spoofable, and un-clonable. This eliminates the risk of any attacker(s) spoofing the MAC, thus breaking a core link between your network and the internet.

> Attack Origins

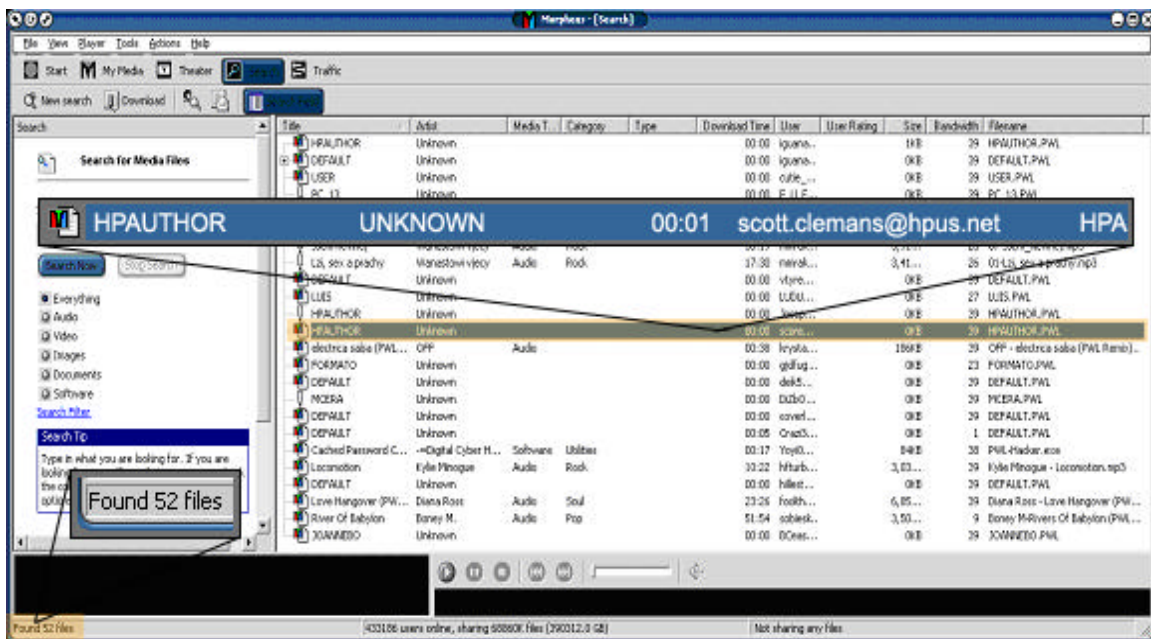
All too often, system administrators and employees alike assume that any cyber attack on them will originate outside of their network, and worm its way on in. This is why most companies outline a standard firewall and/or intrusion detection system for their security policy, completely overlooking internal traffic. In reality, over 30% of substantial attacks come from the inside of the target network. Thus rendering your grandiose firewall and intrusion detection systems to sit and "twiddle their virtual thumbs" as your network is brought to its knees.

Internal attacks can come from many places; sometimes even the most insignificant of software applications running on an employee workstation can leave a gaping hole in your network. For example, AOL Instant Messenger™ software is used for chatting, file sharing, and many other personal functions on a daily basis by more than 100 million users. These users are not only teenagers talking with their friends, but corporate employees and workers using this application to chat and share files while at the office. The AOL Instant Messenger™ client software is riddled with holes like a piece of Swiss cheese. Many pre-made programs lay waiting on malicious www and ftp sites to be downloaded and executed against vulnerable systems. If one of these systems happens to be inside your 'secure' network, any attacker with 5 minutes of experience, a free program, and 2 clicks of a mouse is able to bypass your world class security measures. Once an attacker has control of an internal workstation, he or she can execute any malicious code, or run any insidious program to ruin your network and its contents without being seen or heard by security devices. Sadly, that same busy network administrator and even a CIO have no idea how many instant messaging programs are downloaded onto employee's desktops and laptops just sitting there with an open invitation into the company's network.

Learning to fear peer to peer file sharing programs is essential to your network's survival. Starting with Napster™, on to Gnutella™, then Open Nap™, and now on to KazaA™ (aka, Morpheus), p2p file



sharing programs are here to stay, regardless of what the MPAA, or RIAA have to say about it. As soon as one is banned, another one is created by a 16 year old high school student and it will pop up in its place with the same overwhelming patronage. Regardless of what the program creators have to say, these utilities are created to share and trade media files, such as .mp3, .mpeg, .avi, .asf and more. Users from all around the world connect and share the files as part of a 500,000+ Gigabyte file database online 24/7/365. Recently, security consultants with PivX Solutions, Newport Beach, CA discovered a major flaw in 2 of the leading p2p programs. Morpheus™ and KazaA™ do not filter search results for confidential system files, administrator passwords, e-mail, address book, registry files, and even financial information. The image below shows a search for '*.pw!', revealing 52 unique file names, with an astounding 846 default passwords and duplicate file names. This means that 846 computer systems are using default logins, and only 52 have custom names such as 'billjoe 12' or 'marrycool86'. A very interesting result has been highlighted, with some further investigation, there seems to be a user on the Hewlet Packard internal network. The actual e-mail address has been changed, though the original was valid, and respondent. Inside corporate, government, and seemingly insignificant home network



users constantly run these utilities, and with over 481,728 users online sharing 76297kfiles (424912.0 GB), there may just very well be a vulnerable user on your protected network revealing sensitive data to millions of users. This is just another example of how an internal attack may occur, and sometimes through the most unlikely of sources.

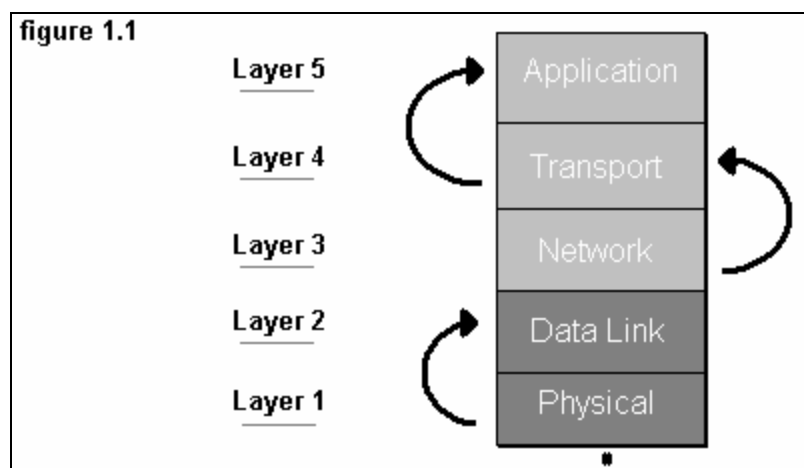
To eliminate this seemingly obvious problem, a good system administrator will have to specify a system or systems that are capable of sniffing traffic from multiple network segments, both internal and external. Once a system such as that is implemented, they must feed the raw traffic to a processing center that can search for anomalies, attack signatures, or any subtle changes in network structure. Also, due to the amount of bandwidth that is necessary for duplicating raw traffic to be processed, the system that will do the handling, sorting, and final processing of this massive flow of data must be

nearby. Lastly, the selected system which is used for tapping into network segments should not cause added latency, or be attackable itself, as that would only create more security problems.

> Software or Hardware

Most security products on the market today are either a complete hardware, or complete software system, both with their own set of flaws. By nature, embedded hardware devices are limited by both their processing power, and their storage capacity. First off, a firewall has a constrained amount of power to perform thousands of tasks and secondly checking legitimate traffic becomes amazingly strained when under attack. Some systems become so strained from a simple Denial of Service or distributed Denial of Service attack that they cease to function. Under this set of circumstances the attacker denies your customers, clients, or partners of the service you provide. Either he or she takes the target server down, or the firewall itself will shutdown because it cannot process the flood of data being feed through its ports. This is a 'no win' situation for the owner of the target system or service, though the problem is apparent. The problem lies within the hardware doing the processing and storage confined in fewer than 5 rack units.

The other option is a software security solution available to administrators looking to secure their investment. Software systems too have their fair share of flaws; not surprisingly software security solutions are even more insecure and riddled with their own natural flaws. Within software security, you have many layers that come before the application layer. What is known as the 'Physical' layer comes before all else, and passes traffic off to the 'Data Link' layer which passes it up to the 'Network' layer and so on. As you can see, there are 4 layers that traffic and its contents pass through before it is even denied or permitted access for processing and routing. Any skilled cracker will simply take down the system by attacking one of the lower level layers.



Not only does a software security suite rely on the hardware it is installed on, it relies on what other applications or services are running on the same machine. With hardware, you get a set configuration that the operating system runs on, though with software, configurations are never the same. This usually leads to unpredictable behaviors and low performance marks; which is something you cannot afford in the area of security. Besides the fact that both hardware and software systems can also be taken down by

MAC spoofing or cloning as previously discussed, they can also be taken exploited with their own vulnerable features. Black Ice™, by Internet Security Systems® was discovered to contain a large Denial of Service vulnerability within its latest version. This software firewall happens to be one of the leading applications on the market, though is now equipped with a security vulnerability, is susceptible to one of the most common attacks. An ideal security device would be one that encompasses the pros of both the software and hardware units, though they seem to be few and far between.

> Insecure By Nature

As you can see, the current status of network technology is grim at best. Everyone from the Government to small businesses is at risk of a complete and total IT meltdown. This will continue as long as black hat hackers search for new security holes and backdoors as a “hedonist searching for that perfect pleasure”, quoted from Giraffe, a reputable white hat hacker attending DefCon 8 stated. As long as security companies continue to build on old technology the problems will continue as will the hacking - unabated. A new company has emerged with a new technology to help secure today's internet, leaving the old ideology and methodology being used in current security systems to be spoofed, cracked, hijacked, or ignored.

A company to provide the next generation in IT security is PivX Solutions™, and the technology is known as LLEDH (Low Level Electronic Data Handling). LLEDH is a way in which to take traffic from a network segment without actually being seen as a true device on the network. Once the device can take electronic data without being true, it is unseen, and can now take advantage of many other benefits of being truly invisible on a network. PivX Solutions has this revolutionary approach and process before the US Patent and Trademark Office as a patentable methodology.

> Implementing LLEDH

As PivX Solutions™ developed LLEDH; PivX has also developed a system which is powered by LLEDH technology. This system is known as Invisiwall™, the first truly invisible hybrid network security system. Using hardware and software technologies together, improves processing power, scalability, capacity and response times making for more than just a secure infrastructure. Furthermore, Invisiwall™ does not add latency to your network and will not disrupt the constant flow of traffic through a tapped segment.

> Invisiwall.Technical

Invisiwall™ is not just a device, but an entire system as shown in the image below. There are 3 main points that make the system what it is. 1) The Invisiwall™ device; a custom device which is used to invisibly copy traffic to point number 2, leaving it untouched, and to continue on to its destination. 2) AI and Attack Signatures Engine; this point is where all copied traffic is examined for anomalies, attack strings & signatures, suspicious patterns, or probes. 3) This is the Detection and Response point; this is where actions are taken via API to the firewall if any problems are found.

Due to the huge amounts of traffic moving over high speed networks, and the need for raw packet duplication, the processing and monitoring jobs are performed within the physical plant of the data center at a PivX local Network Operations Center (INOC). The

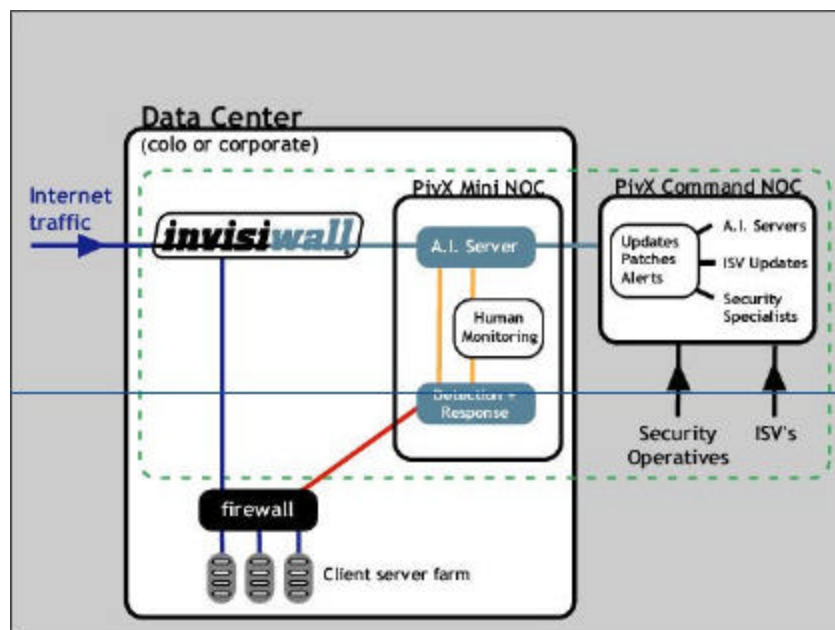
device acts as a splitter that sends a carbon copy of the network traffic on a dedicated third line maintained at the NOC. There, professional security experts use custom software to monitor, log, and analyze the traffic and actions occurring on the subscribed line. The PivX solution eliminates the problem of false detection, as well as determines which firewalls are deploying false offenses that ultimately lead to costly down time. PivX security specialists will have rules-based scenario plans for specific attacks and attempts, enabling them to immediately respond to any such occurrence.

Humans and Artificial Intelligence United – Invisiwall™ is far more discerning than current technologies, most of which use simple programs that react when something happens, with a singular offense sometimes blocking out innocent users. Invisiwall's artificial intelligence (AI) programs run on dedicated servers, and typically on what would be deemed supercomputers. Thus they are able to process more than 100 times faster than standard embedded firewalls. The Invisiwall™ model has real people monitoring the integrated AI engine—they are plugged in to a worldwide network of real time security specialists who are constantly on the lookout for anything that is the least bit suspicious.

Around the Clock Local NOC – Invisiwall™ will be the only intrusion detection service on the market offering absolute 24/7 reliability, support, and monitoring in a custom built secure NOC. This is also known as the INOC.

Around the Clock Corporate NOC – Not only is there a team of people 24/7 locally, but there is a constant staff at the corporate NOC where all local NOCs are monitored from based on a condition level similar to Norad's DefCon system.

Fully Scalable – With the Invisiwall™ product, PivX can stack up to 95 devices for multiple Internet connections with customized monitoring, service, and support contacts to accurately match client needs.



> Network Insecurity Conclusion

In conclusion it is clear to me and many of my InfoSec peers, fellow University Instructors, Professors, and the hacking community that the word "Network Security" is a myth. It should, in fact be called "Network InSecurity". Until an entirely new approach is taken to defend these critical systems and their precious data, the "bad guys" will continue to win this war. Make no mistake about it, this is a war! Many of these hackers and crackers honed their skills playing video games and they graduated to virtual games like "Action Quake II" where they played for hours if not days on end. A major problem is this: network administrators are fighting a war against an enemy that is well equipped, nameless, faceless, elusive, and whose weapons are getting more sophisticated every day. The network administrators, however, are fighting this war with a hodgepodge of cobbled together solutions, which are not acting in concert, they are not sufficient to deter their enemies; in fact, the enemy can see their defenses before they take an offensive move. Furthermore, the defenses being deployed by network administrators are reactive at best and due to budget constraints which neither their army nor their weapons of defense are capable of protecting them.

> Contact

Geoff Shively, CTO PivX Solutions

//: Physical

2808 Lafayette

Newport Beach, CA 92663

//: Internet

e-mail: geoff@centrifugepartners.com

URL: <http://www.invisiwall.net>

//: Telephony

office: (949) 673-7385

home: (949) 673-7075

fax: (949) 673-7042

cell: (949) 254-3744

List of Acronyms

ARPA	Advanced Research Projects Agency
CERT/CC	CERT® Coordination Center at Carnegie Mellon U
DARPA	Defense Advanced Research Projects Agency
IDS	Intrusion Detection System
FTP	File Transfer Protocol
WWW	World Wide Web
IETF	Internet Engineering Task Force
IP	Internet Protocol
p2p	Peer to Peer
NOC	Network Operations Center
AIM	AOL Instant Messenger®

I would like to thank the following people and organizations for their support and contributions to this White Paper:

CERT (Computer Emergency Response Team) at Carnegie Mellon University

CSI (Computer Security Institute)

FBI

Dr. Mark Songer-Former Forensic Science Expert FBI, Current Director FSTI

Verdeen and Andreana Weiner

Rob Shively-CEO PivX Solutions

Centrifuge Partners

University of California-Riverside