Global Information Assurance Certification Paper

Cyber Citizenship for the Home User

Kenneth Walter, May 9 2002, GSEC v.1.4

Cyber Citizenship for the Home User

Introduction/Exec Summary:

"Always-on" home computer Internet access has become common; a "boon" to the education and e-commerce communities, providing benefits in "instant" communication, financial transactions, news and reference resources, and supplements to our entertainment.

This "boon" in communication also carries a burden: home systems are usually not secure. Home users lack the resources and experience to secure their systems, and hence, they are typically open to attack. In fact, many home users choose to ignore the risks associated with Internet connection, and assume that Internet crime is only associated with teenage "hackers" attacking large corporate networks.

Reducing crime is a matter of education. We cannot expect the threat to disappear. However, through education we can expect to see a reduction in the risk of criminal activity. And, through vigilant reporting, we can expect to see the reduction of the threat as would-be criminals find a productive niche in society easier to procure.

Similarly, the Internet community can benefit by reducing the most common Internet vulnerability, that of the unsecured home or small office system. By removing easy targets, it becomes more difficult for the amateur hacker to participate in computer security crime. Computer theft of identity, financial, and access information becomes laborious. And the pawns available for distributed denial of service (DDOS) attacks become fewer.

Main Thesis:

Many home users are attracted to the ease and speed of cable Internet Access. The problem is, most are unaware of their exposure to Internet hacks and subsequent dangers therein. Specifically:

- The frequency of reconnaissance occurring daily on a typical broadband cable network.
- The ease at which hackers, once in, can gather personal or private data.
- The possibility that a remote control program could be installed and not be detected.

Because of the pervasive lack of secure systems, the Internet Community is subject to additional forms of computer crime, such as distributed denial of service (DDOS) and remote controlled hacking. Often, the owners of DDOS pawns are unaware that their system participated in an attack.[1] It is for the good of the home user and the Internet

Community, to reduce this opportunity for crime, by removing the vulnerabilities that make it so easy.

Threats and Vulnerabilities

Before launching into solutions, home users must become aware of the problem. Some are simply unaware that other people can intrude on seemingly private conversations. Others believe that their activity is insignificant and therefore of no account to others. Still others evade the issue of security citing costs, or justify that other people with more resources can police the network. This last sounds all too familiar to IT security professionals, who often struggle with these same issues in the corporate or government environment.[2] Home computer systems are very much affected by, and in turn, have an impact on the larger network we all know as the Internet.

It may be helpful to explore some background to the problems as well as the principles of security, and how that applies to the home user.

First, lets consider the threats currently on the Internet. The Internet, by design, is a source of information. It allowed researchers from distant points to collaborate. Over the years, access points as well as access tools have evolved and abounded to allow any individual to access, and possibly to download, data from another node. In fact, common web browsers are built to retrieve data.[3] [4] This means that World Wide Web (WWW) users can literally download pages of information every time a link is pressed.[5] Data retrieval happens so frequently, and often automatically, that people fail to remember that this external data is stored on user's local systems, benign or not.

Electronic mail (a.k.a. E-mail) is another very common tool used to pass messages amongst people and machines. This tool was once thought protected from virus activity.[6] [7] But human factors, automation tools, and default software installation have conspired to make this tool vulnerable. Recently, E-mail has been the delivery method for some of Internet history's more notorious attacks. [8]

Where do these attacks come from?

It is popular to blame modern teenage hackers for ills of the Internet. In fact, hacking has been around over a century. And much has been documented of phone system hacking, "phreaking", and abuse since 1870.[9] For the Internet, this anti-establishment culture grew from the merely curious, or adventurous hacker who found it fun to break into academic or national defense systems, to serious vigilante groups bent on maintaining freedom of speech from "big brother." It showed up in popular movies such as War Games (1983) and Ferris Bueller's Day Off (1986). Congress enacted the Computer Fraud and Abuse Act (CFAA) in 1984 citing the disturbing discovery of unauthorized access of patient records at a Cancer Institute in 1983.[10] [11] Cases of corporate insider attacks also appeared in the mid 1980's.[12] Many corporate attacks still "go unreported

because companies want to avoid negative publicity"[13] To be sure, teenage hacking still exists, but these other forces also threaten Internet integrity.

Today, a whole host of would-be threats appear by merely connecting a node to the Internet. These threats could be corporate competitor's seeking information to increase market share. They could be foreign nations of terrorist groups wanting to destroy or disrupt national or local systems or infrastructures. They could be a local grass-roots organization seeking support through propagandizing their cause. "They" could even be insiders who carelessly leave the door open for just anyone to walk through – even though such access is privileged and potentially damaging to the organization.

Who'd want to attack me?

The home user system is just as vulnerable to Internet attack as any organization. As I like to tell my clients: "There are people who have nothing better to do today than eat potato chips and break into systems." Why? They do it for fun. They do it because they can.

Breaking code or breaking into computer systems has become "cool." It wins points among hacker peers. Besides, there are potential advantages. Home systems are easy access to credit card or financial data, and can provide launching point for other attacks. Both of which are valuable on the black market. Home user attacks thus provide potential income and disguise for other attacks. And these are the "just for fun" attackers!

Currently, reconnaissance scans occur daily on any given network. These probes could be benign, or precursors to possible attack. Numerous articles are written about attacks and tools needed to prevent intrusion, but the average home user may not know what an intrusion is. The National Security Telecommunications and Information Systems Security Instruction (NSTISSI) defines intrusion as the "unauthorized act of bypassing the security mechanisms of a system."[14] But what if there are no security mechanisms? Is it still trespassing? Incident documentation suggests that would-be attackers look for holes before launching serious attacks. And why not? Why waste resources breaking in on a system, when portals exist practically inviting entry?[15] For evidence of snooping, we need look no further than our own local firewall or IDS. Below table is extracted from a sample 14 hour Zone Alarm Log. Particularly disturbing are the number of unassigned source ports used and the frequency of Sub-Seven probes.

From a sample Zone Alarm Log 2002, April 7 09:22 to 23:27 unexpected packets which might be probes showing destination port range	
86	Total
1	ICMP
1	unassigned port 65368
1	unassigned port 12345
2	FTP port 21
3	NETBIOS Session Service port 139
7	unassigned port 27374 (Sub-Seven)
24	HTTP port 80
47	NETBIOS port 137

Virus, Worm, and Trojan Horse reports abound. The Computer Emergency Response Team (CERT) Coordination Center handled over 52,000 incidents in 2001 alone.[16] It is a safe bet that this method of intrusion will continue for the foreseeable future.

Okay, so they got in. So what?

Once a would-be attacker gains access to a home system, what would they find? What is the threat? Of course the one threat we all think of is losing our data. Some still remember the days when hard drive crashes were common. {Though the technology is better, this threat still exists.} High-risk viruses and worms can cause similar damage, often leading to unrecoverable systems. Some businesses never recover financially due to such computer systems disasters. Little is known about the impact such loss is to the average home user. Certainly damage is done, and most home users I've known simply bite-the-bullet and move on.

But what if the data is not lost, but stolen? What potential impact then? Certainly, some would liken it to losing a wallet: Do we know what was lost? Credit card numbers, identification, home address, pictures, bank account numbers... All are but a few items of privacy concern. Corporate espionage can also occur from the home of an unsuspecting employee.

Some attackers are not interested in data theft or deletion. In fact, to do so would expose or remove the asset so useful to them: Remote control of a home system. Why would attackers want that?

In the words of a popular software vendor: "Remote Control can simplify application support."[17] Applied adversely, attackers can use available software management tools to supply and update programs not installed by the legitimate user. This means that agents, and other software *can be installed undetected* that can use resources to scan and attack other systems. Having remote control of some other system minimizes impact and evidence on the attacker's system. No extra systems, nor addresses, need to be purchased. And the attacker can sit back comfortably and watch remote systems exploit Internet vulnerabilities. Notice also, that the blame for a successful attack is first pointed at the remote system's owner, who then has a burden of proof.

Risk Management

So the threat exists to home users. It exists through human greed and idle hands, which like nothing better than to gain access, notoriety, credit card information, or similar, by theft or subversion of carelessly left data and open doors.

I think most Computer Security professionals will agree that there is no such thing, as "a 100% secure computer system" (even if turned off, it can still be stolen). So Risk Management really becomes a *balancing of resources and impact*, where each computer user has to determine "what's an acceptable level of risk?" Since most home users have not reviewed their vulnerabilities, nor considered the threats significant, this decision is made by default: home systems are typically left wide-open to visitors.

How can the home user reduce the risk of Internet use?

Let's look at the other side of the Risk equation. Subject specialist Mr. Hinson tells us that Risk is a product of threats and vulnerabilities and impact (R = V x T x I).[18] A similar assertion is made in the SANS Security Essentials course (R = T x V).[19] We cannot directly control Internet threats. However, we can control vulnerabilities. Vulnerabilities exist in all our computer systems:

- Open system and default shares
- O.S. flaws & ignorance
- Flaws in software and human factors
- Careless leaving of identification and/or financial data
- Misunderstanding/misrepresentation of software claims/purposes

The folks at Computer Consultants of North Alabama (CCONA) have listed explanations of common computer system vulnerabilities.[20] The following summary contains quotes and paraphrases directly from their excellent page. Home users are encouraged to review this and similar pages. www.ccona.com/networksafe.html

"Most software, including operating systems and applications, come with installation scripts or installation programs." These automated tools are used to setup software quickly, "with most useful functions enabled, with the least amount of work…" This means that more components are typically enabled than any one person needs. These unneeded or unknown components are often not maintained, leaving open vulnerabilities for attackers to use. Sample programs, scripts, and standard directory locations are also tools used to compromise computer systems and networks. Software patches can also be vulnerable to bugs and errors, especially if rushed to market without complete regression testing. Some applications or operating systems, including network devices, have built-in or default accounts, and even default passwords.

The Impact

Vulnerabilities such as these provide access to the common, unprotected home or small office system (a.k.a. SOHO system). If unprotected, they represent a risk to other, especially larger Internet entities, such as corporate, military, or government organizations. These institutions, though most have implemented security policies and procedures, may still be vulnerable to the dreaded Denial of Service (DOS) attack. And

because so many unprotected systems exist on the Internet, the threat of large scale, remote controlled attacks cannot be avoided.

Distributed denial of service (DDOS) tools "allow a single attacker to multiply the effectiveness of an attack."[21] Whether used to flood (and thus deny access to), or used to otherwise compromise a system, DDOS tools can be an effective means to run thousands of hosts against an intended target. The tools have evolved[22] to where remote "handlers" are used to further hide the original attacker, and agent software can be configured to update itself. Further complicating detection are new methods, such as resource depletion and smaller bursts of packets that "can be used to slow down or crash servers."[23]

The exploited hosts of DDOS handlers and agents "are not really addressed by operating system vendors"[24] and most agent detection tools are beyond the means of home and small office users. To quote University of Washington Senior Security Engineer Mr. Dave Dittrich: "There is still a large class of highly populated sites, such as broadband and DSL providers, whose customers' systems can easily – trivially, and without any fear of discovery in some cases – be used for setting up massive DDOS networks."[25]

To help alleviate this problem, the answer lies in Defense In Depth for the Home User.

Defense-In-Depth for the Home User

This might seem an impossible task. Layered computer security for the home user? Considering that many of us have been known to lose our wallet or lock our keys in the car, how can we ever hope to achieve adequate data security for the home Internet user?

One answer is two-fold: First, provide education in terms people can relate to. Second, provide reasonably low cost solutions using non-vendor-specific tools.

Why would we want to do that? To reduce the threat epidemic that mires technology advances and sucks up huge budgets and human resources that could be better spent. *We, the IT community owe it to ourselves to reduce the risk of computer crime*. Computer crime has grown from the rare malicious software time-bomb from a disgruntled employee in 1980[26] [27] to the estimated multibillion dollar losses in productivity and diverted resources to counteract computer theft and vandalism today.[28]

- The threat of virus, worm, or Trojan horse infection is high
- The threat of attackers seeking access control or data theft is high
- The threat of DDOS is now high due to the availability of easily compromisable systems on the Internet

Some threats will not be reduced except through enforcement, conviction, and forced justice.[29] Other threats can be reduced, by removing the vulnerabilities that attracted

such danger, much as cleaning up spilled food reduces the attraction to ants. Thus, some of our security problems facing the Internet community today can be mitigated, simply by making vulnerable systems less inviting.

Defense in Depth is simply a concept of multiple layers. The reason many space missions succeed is NASA's adherence to this concept. It means having a backup in case the backup system fails also. A person may put five deadbolts on their front door, but they may have neglected to lock the back window. So to be effective, Defense-in-Depth's first tool must be education: an awareness of the threats and vulnerabilities.

Education of Home Users

The Internet has become our own mass media. Search engines now replace timeless encyclopedia references and trips to the library. Well-placed public-domain web sites can now provide "instant access" for users seeking certain words. The incentive for seeking such sites must be provided by more traditional means: public news media, word-of-mouth, radio, and organization newsletters. In fact, the corporate newsletter may be the ideal medium, and corporations have some vested interest in protecting employees of identity theft, and itself from potential attack via known or unknown compromise from an employee's home system. Most, larger, organizations already have computer security and use policies in place regarding the corporate network resources. Often, these same organizations may not recognize that "home computer security is a key aspect of corporate network security."[30]

The CERT® Coordination Center's current trends report[31], located at http://www.cert.org/archive/pdf/attack_trends.pdf is a good reminder that vulnerable *home systems can provide backdoor access to organization's computers.* This and other industry reports should be enough to justify attention and funding for employee computer awareness training. Policies and training can be put in place to protect both the organization and personnel from most unwanted incidents. Preparedness for computer incident response (CIR) makes good business sense. And it is common to overlook employee home systems as a source of vulnerabilities.[32] Compromised home user machines are "used by intruders to launch attacks against other organizations."[33] Adequate staff and CIR teams should be maintained to assist enterprise and any related employee incident. The business need, to pre-establish a computer security incident response team (CSIRT) and associated policy, is well documented.[34] Organizations simply need to recognize that employees are part of the organization. To quote West-Brown, management needs to "understand that the problem is a business one and not a technical one."[35]

In my professional capacity, I perform an informal survey of home users with cable Internet access, and ask what protections they have in place. Only one in 20 indicated router or firewall protection at home. Most admit that they have none, and are surprised to learn that they are at risk.

The reality is that *most home Internet computer lack adequate protection*.

Here are some of the statistics:

Reported	1995	1996	1997	1998	1999	2000	2001
Incidents	2412	2573	2134	3734	9859	21756	52658
Vulnerabilities	171	345	311	262	417	1090	2437

Source: The CERT® Coordination Center http://www.cert.org/ http://www.cert.org/stats/ April 2002

These and other reports and surveys[36] support Mr. Dittrich's claim of a large market vulnerable to intrusion, and capable of being setup as massive DDOS network.[37]

Home Internet users also lack some motivation and corporate example. Mr. Hernan, of CERT's Vulnerability Handling Group, makes a point that we, the users (including large organizations), send a clear message to technology vendors that "security is less important than functionality or even appearance." He concludes that "Security products certainly help, but they are not a substitute for secure programs and protocols." And "Unless [people] behave like security really matters…[we] will not be secure."[38]

Since beginning research for this paper, the National Cyber Security Alliance (NCSA) has stood up its www.staysafeonline.info Web site to provide consumers "with tips, alerts, safety checklists, protective measures, and other information to promote safe and responsible computer use."[39] NCSA reports over 2 million visits in its first month and this bodes well for the education and awareness of the Internet public. The site encourages every American to take responsibility to protect their systems and thereby protect the nation's Internet infrastructure from on-line intruders. Cisco Systems, Inc. reports that "NCSA is a cooperative effort between industry and government organizations to foster awareness of cyber security through educational outreach and public awareness."[40] With the support of its members from leading IT private sector companies, it promotes computer safety as part of home security.

This is an excellent example of a cooperative effort to provide awareness of Internet threats and vulnerabilities. Such high-level attention from major organizations *highlights the importance of home user education for the benefit of the Internet at-large*. Though certainly encouraged by the events of September 11th, I am convinced that this kind of effort would have occurred anyway, based on our previous review of incident trends. NCSA cooperation is to be applauded and expansion encouraged throughout our global Internet community.

Principles of Security and Tools for the Home User

Once open to the idea of Risk Management on home systems, tools must be provided that are accessible, affordable, and easy to understand. "Toolboxes" may be assembled based on the Principles of Security as taught by the SANS Institute.[41]

The Principles of Security include four basic tenets:

- Know Thy System
- Principle of Least Privilege
- Defense in Depth
- Prevention is Ideal but protection is a must

The following paragraphs expound on what these mean to the home user:

Know Thy System

It is unreasonable to expect the average home user to know everything about the personal computer system installed at home. Part of the education process is to encourage users to be aware of their computer systems and what constitutes "normal" operations. But that doesn't have to be hard. In some cases, this is just an awareness of what kind of data may be stored, or shared, on your computer system.

We used the analogy of a person's wallet earlier. What happens if that wallet or purse gets stolen? Wouldn't it be nice to know what credit cards documents, licenses, and passwords were in that wallet or purse? One instructor I know advises people to make Xerox copies of everything in a wallet, front and back. That way a record exists of the missing items, and better, the important numbers are available for easy reporting. We can do the same thing for our home systems, including PDAs, simply by making a backup.

Backup

Numerous methods exist for data and system backup. These include well-known commercial tape backup products and the simple "copy to floppy" method taught in schools and Internet cafes. What is important across the board is to keep it simple. The K.I.S.S. principle allows users to protect themselves from agonizing loss, by making backup routine. Today, Re-write-able CD's are popular and we can expect DVD technology to follow suit. In fact, CD/ROM recorders are recommended by SANS's Emergency steps.[42] Specifically encouraged is the "burning" of an image backup to aide in both the rebuilding and the forensic investigation (and collection of required evidence). Although this gets harder as storage sizes keep pace with technology, CD imaging remains a common tool among CSIRTs for now. Complete, tested backups enable Configuration Management, which requires a baseline from which all measurements are taken.

Establish a Base Line

Base-lining a home system need not be so stringent. However, the choice of what, how much, and how to backup, really hinges on the convenience provided should a disaster occur. Backup is basic insurance. No one product can be the catch-all, so no one product will answer for all users. Let's leave method choice to the home user and explore the benefits and pitfalls of backup.

With a backup, should a person become aware of an intrusion, steps can be taken to minimize the damage. Law enforcement and financial institutions can be contacted if necessary. And, compromised systems can be reloaded with a minimum gnashing of teeth. All this is good, provided the backup is valid. Let me explain:

Recovery Testing

Having a complete backup is rare. Data changes, and keeps changing even during the backup. Every organization including the home can expect some data loss, simply because data backups are not real-time.[i] Also, and more importantly, Know Thy System also means knowing that the backup is recoverable. Has recovery ever been tested? "Some organizations make daily backups, but never verify that the backups are actually working.[43] So the practice of home fire drills can actually be extended to the home computer system, simply to validate that procedures work as expected. Home system owners therefore benefit from routine backup and periodic recovery, by knowing that most of their data is recoverable.

Intrusion Methods

Besides knowing what and where personal data is, the home user should also be aware of how intruders might intrude. Lawrence Rogers of the CERT Vulnerability Handling Group, recently wrote two colorful articles on this subject.[44] In them he describes security leaks and computer break-ins in layman terms. The first refers to knowing what kind of data is available (e.g. private) and how easy it is to unwittingly divulge tons of "intelligence" to a potential attacker. Merely asking a question on the Internet discloses lots of information, some of which may show vulnerabilities. The second article requires us to test our human memory: Do we know for certain what activity is normal and what might be suspicious? Would we be aware of computer break-ins, even if the clues were highly visible? Both articles call on our awareness of our systems. Exactly what vulnerabilities exist? These would be the open shares, backdoors, and software flaws we mentioned earlier.

---

[i] Unless a form of disk mirroring, or RAID system is implemented. Even then, the data is not truly protected as it is not physically removed from the original source, and can be similarly compromised.

Software Flaws

How can we know software flaws? We didn't write the computer programs used on our systems. Even if we did, we would not know exactly how separate programs interact together until we test them. And that means to baseline what is normal. It also means we should look for "consumer product recalls" commonly known as "patches" in the computer world. It also means a little homework, in researching current evaluations of Operating Systems. Getting second opinions, like going to the doctor, can be comforting. And, it can be very revealing.

Sources for Information

User groups, bulletin boards, and Internet forums have all evolved from the need to discuss topics with others with similar software, situations, or interests. Independent watch dog groups and researchers have contributed, like "Consumer Reports", to improvements in software, hardware, and policies in the computer arena. Many sites are supported through advertising. Some are thorough and produce references for their findings. Other advice must be weighed as to its validity. So how do we find accurate, current information?

One recommendation might be to subscribe to two or three automated email notices of general patches and Internet Security watch groups, like CERT[ii] and The SANS Institute.[iii] Again, K.I.S.S. is required as too much information may cause all to be ignored. Besides, not all patches and upgrades are bug free. First consider the implications of upgrades before mechanically installing software you don't know. Make a backup.

Privacy Practices

Home users should also know what constitutes poor privacy practices and human factors that contribute to security failures. Social engineering plays a large part of corporate and government espionage. That can be said for home systems as well. Have you joined a supermarket club, redeemed rebates, or entered a drawing this year? In the process of gaining some benefit, we have relinquished some information that may be useful for marketing demographics. Which can be good or bad depending on how it is used. This information could be used to ask further questions, and, often as not, we comply. Professional thieves have learned to use this method to find easy access to our homes. So have professional and amateur hackers.

[ii] The CERT® Coordination Center http://www.cert.org/

[iii] The SANS® Institute http://www.sans.org/

Most of us believe we are exempt from such manipulation. Read Mr. Roger's *Friend or Foe* article again.[45] The simple truth is, we all give out potentially sensitive information. This is one reason that Public Key Infrastructure (PKI) encryption has become so important to many organizations. CERT has documented cases where people were fooled into giving away their password. "While this advisory may seem very trivial to some experienced users, the fact remains that MANY users have fallen for these tricks (refer to CERT Advisory CA-91.03)."[46] I am always amazed the many times in my own professional career, when people have given me their trusted password, unasked for, whether I was their system administrator or not.

This does not mean we should stop trusting fellow humans, it just means we need to be aware of common fallacies and who has access to our data, really. I liken this to knowing who walked through your office today, who borrowed the company vehicle last, and just not leaving the keys in the ignition.[47] Which brings us to the principle of Least Privilege.

Principle of Least Privilege

Humans have a sense of ownership. For various reasons we become stewards of God's gifts to us, including the numerous tools that we have invented to ease our burdens and to entertain us. For some reason, we are concerned about who: takes our toy, borrows our car, or walks through our living room. Yet, many people leave the "doors" to their living room computer systems wide open, never imagining that someone might actually pass through.

The Principle of Least Privilege is "taking the keys out of the ignition." It requires that an entity be given no more privilege than necessary to perform a task. People are given access rights. Machines are given governors. This principle has far-reaching effects when applied. It means that a software program does only the function it was purchased to do. It means that only certain users have rights to change certain files. When applied, it can mean knowing exactly under what circumstances a person or program can modify important records.

How this applies may be different at home that in the corporate environment. Organizations may want separation of duties, and accountability of data base changes. They also may want to maintain productivity, and so restrict corporate access to non-productive Internet sites and games. Parents want to protect their children from foul language and pornography, and may have an unwritten policy restricting access to immoral subject matter. The principle is the same.

Usually, the Principle of Least Privilege is only partially applied. Why? People are human. People want the flexibility and freedoms to make needed changes immediately. Businesses crave the "new", the "flexible", the "just-in-time", and "added features" marketed to solve problems. At home, the "system administrator", "security manager",

and "user" is often the same person. Software companies want their product to appeal to many people, not just a few. So added features are included in products to make them more flexible and marketable. Often, this principle is not applied because end users and installers simply do not "know their system" enough to customize the installation.

Significant benefits are available by applying the Principle of Least Privilege.

- When minimum software is needed, there are:
  - Lower software requirements, which decrease costs, and funds are available for other purposes
  - Fewer processes used, increasing system performance
  - Fewer vulnerabilities exist, increasing system and data security
- When applied to human access to computer systems:
  - Greater physical security is achieved
  - Greater accountability for changes ease error detection and reversal if needed
  - Greater productivity, as systems are more likely to be used for business
  - Reduced liability, as pornography and insider attack options are limited
- When applied to network access:
  - Fewer open portals, reduces opportunity for cyber crime
  - Better metrics available, to increase knowledge of system resourcefulness ("who used what and why")
  - Greater security, as it reduces risk of catastrophic events such as data deletion, intrusion, or theft

Basically, a thorough review of the Principle of Least Privilege applied to systems, provides better input to "know thy system" better.

Here are several recommendations to assist applying the Principle of Least Privilege at home:

1. Review Your Needs.

Discuss among all the users of the system(s), exactly how they want to use the system(s). Security applied for games is vastly different than security applied for banking accounts. Know Thy System (and users) is the first step in applying the Principle of Least Privilege. Write this information down for your records. This is effectively your "Home Computer Security Policy" until you decide to change it. This should be reviewed from time to time (as should all computer security systems).

2. Restrict Physical Access

No system is safe if someone can walk away with it. Add a simple bicycle lock. Secure your home. Check for windows where the computer system may be visible. Check for backup tapes or similar, laying out where people could easily walk away with them. Don't forget non-human disaster prevention. A system beneath water pipes or on the

floor near the water heater is a bad location choice. Humidity, temperature fluctuation, and pets are other considerations that fall under physical access.

3. Consider Access Times

There may be times where you don't want the kids accessing the system (midnight or study hours for example). Logon restriction during system backup is also appropriate. And consider who has access to change firewall or other administrative settings. Some operating systems provide account lockout restrictions that can be applied here. Or, use physical access controls to prevent abuse or to monitor access. Any hardware store can provide lock boxes for wall outlets that can be applied to both system and to network access. More specialized access tools may be appropriate depending on the situation. Look for keyboard and mouse locking drawers from office furniture stores. Some of the software tools we discuss later also include features at this level. The Zone Alarm personal firewall, for example, includes an Internet Lock feature. This can be configured to "lockdown" all network activity after 2 minutes of inactivity or when a screen saver activates.

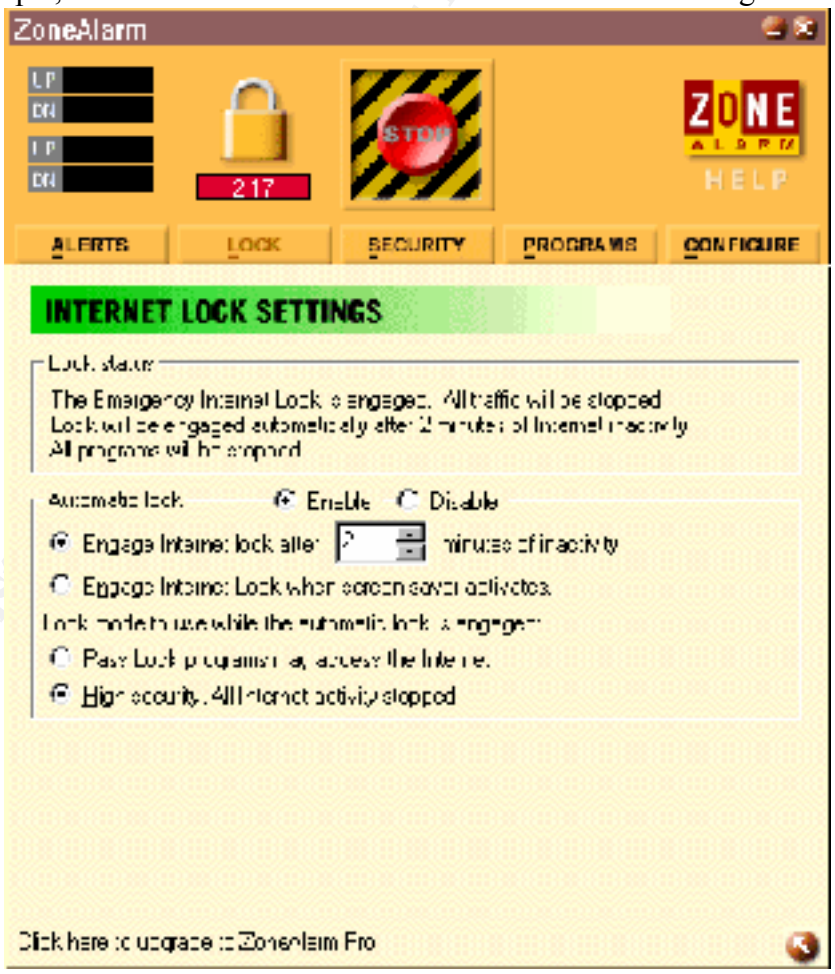


Image of ZoneAlarm Internet Lock Settings

4. Check Operating System features

Many Operating Systems (O.S.) have tools embedded to help restrict access. But most home system versions are not robust enough to really protect. In Microsoft Windows 95,

98, and ME for example, users can bypass user login. If user separation is important, (i.e. you don't want your spouse, in-law, or children to see your recent Internet activity) then you should consider a more robust login security through an NT, Linux, or a Mac O.S. This brings us to O.S. vulnerabilities and "features." Recall that software is often installed with default options. Operating Systems are no exception. So update and lock down your O.S.

The following locations are provided as sample only, and are not endorsed as valid sources for software patches. This list was produced using a simple web search to show possible locations of various operating system patches and upgrades.

http://windowsupdate.microsoft.com/
http://www.apple.com/macosx/
http://www.microsoft.com/downloads/searchdl.asp?
http://catchup.cnet.com/catchup/cu/index/index.html
http://www.linux.org/info/
http://www.slackware.com/
http://www.redhat.com/software/linux/
http://www-1.ibm.com/servers/aix/os/
http://www.apple.com/macosx/upgrade/softwareupdates.html
http://www.opensource.apple.com/projects/darwin/
http://www.software.hp.com/HPUX-RDMP/
http://www.software.hp.com/RELEASES-MEDIA/
http://www.uniqsys.com/services/softadmin/softadmin.html
http://www.sun.com/solaris/
http://www.sun.com/solaris/liveupgrade/
http://www.cisco.com/public/sw-center/sw-ciscosecure.shtml

Once updated, you must re-evaluate all your security settings. Major changes can undo all previously applied patches and restrictions, so that systems are no longer protected from intruders or data leaks. And for Gosh Sakes, turn off unrestricted shared resources. All too often home (and corporate) systems are installed with default shares turned on. And even in Windows NT, the entity "Everyone" has access to all resources. Change permission settings to these "open doors." Lock your personal file cabinets.

5. Remove Unused Software

As discussed above, most applications come with added features. If you don't use these features, turn them off. Many installation packages allow for some customization. Read the manual. Remove any samples or unknown features. Software can always be re-installed or features added back later if necessary.

6. Check for Leaks

Be aware of Internet tools and how they work. Some applications (telnet and FTP) transfer data "in the clear." That is, the data, including any access passwords, may be

visible by a third party. Programs that use Internet Relay Chat (IRC) may be vulnerable. Check the advisory listings for information concerning your particular software suite.

Personal firewalls, network routers and other tools can be used to prevent data leaks, and provide positive control. We'll explore these tools further in the coming section.

Defense In Depth

As discussed above, Defense in Depth is the concept of multiple layers. Single layer security can and will be compromised. Computer engineers learn early that there is always more than one way to accomplish a task. Likewise, computer attackers learn about different vulnerabilities and choose the most likely path to accomplish their goal: the compromise of the target system. There is no single defense that can stop computer theft short of not owning a computer. And that option limits the availability of the Internet, arguably the most useful tool yet invented. Just as individuals and businesses must protect themselves from harm, home computer owners must be vigilant that their systems are not used as targets or accomplices in a crime.

Here are several recommendations to assist applying Defense in Depth at home:

1. Apply Physical Security
Much application of physical security was discussed in the previous section. Additional notes may be to apply multiple layers of physical security: an additional lock, for example. Home burglar alarm systems and components have become readily available. In fact, some homeowners and businesses use a second computer to collect data or control premises security. Computer cameras, video, and related software have become mainstream for archiving and photo enthusiasts. Why not use these tools to help protect other computer systems and data storage cabinets? One basic idea here is to apply physical separation from an apparent threat. It does no good to have your physical security system stolen.

One terrific idea[48] applies to physical separation by function: Rather than purchasing separate computer systems for games, banking, and Internet surfing; use removable hard-drives (each bootable to it's own O.S.) to create different security postures depending on function. This cost-effective approach limits access to sensitive information and can make security configuration less complex.

Physical separation also applies to backup strategy. Place a backup of really important information in another house, a desk drawer at work, or in a safety deposit box. We never *plan* for a flood, fire, or tornado to destroy our home systems and all the backups along with it.

2. Avert Disasters
Did I mention backup? Backup comes in many forms. In fact, that's what Defense in Depth is: backup for the backup in case the backup fails. Protect from Disaster means being prepared in case of an emergency, such as power failure, flood, fire, and funeral. Backups are our insurance should a bad event happen. It is a good idea to save your work-in-progress often, to insure against the one time someone kicks the power cord.

Power failures used to be a huge problem with computers. With technology advances, outages occur less frequently (except in California) and systems are more likely to recover easily. But the risk is still there. A power failure can still mean your home computer system may not recover from "the crash." That is why power filtering and battery backup remain a basic component of system security. A power strip is not enough. It may not contain the necessary surge protection from power spikes. Check it. Be aware that power fluctuations may not always be visible. Power brown-outs, noise, and minor surges all produce dirty electricity which can shorten the life of a computer system. Not all system power supplies can filter or withstand such surges and can pass it on to the components that hold your data. Which is why I recommend uninterruptible power supply (UPS) systems.

Not all battery backup systems are uninterruptible. The marketing rhetoric on this subject is a challenge to wade through. But the difference of a few microseconds can make the difference between a saved file and a hung system. Power users are reminded to purchase a UPS to size. An overloaded UPS may do more harm than good. Finally, all wire input must pass through surge protection. A power surge or spike makes no distinction from a telephone wire or network cable, or power cable, or printer cable.

3. Have a Backup Plan
Even if you never look at it again, create a plan should something go wrong. All military organizations create emergency procedures for any number of situations. Home users may not need that level of detail, but it is helpful to have an evacuation plan in case of fire. Likewise, a checklist or simple plan will save time and frustration, should an event affect your home computer system. This may be as simple as listing the number of your local computer guru or cousin who helped you setup your system.

It is better if you have personally reviewed and filed procedures for Data Recovery, for alternate Network Access, and for recovering a valid log for law enforcement to investigate in case of Intrusion. These need not be detailed, but a simple review of steps required to restore data from backup, for example. How to check logs, and an alternate method to access the Internet, may prove invaluable should the need arise. Be prepared.

4. Secure Passwords
One of the easiest tasks for hackers these days is to crack passwords. "Cracking" is not really the word anymore, as automated tools are now available for hackers to simply "look up" likely passwords, using dictionary association. In any organization, there is

bound to be a few people who use simple words, birthdays, pet names, car names, or place names as their password. Home users are no exception. What with all the clubs, ATM PINs, cell phone PINs, and Internet shopping accounts, the password game has gotten real complicated. Most people I know have more than 10 passwords. We users want simple passwords, so we can remember them, but that's a bad choice. People have been known to carry PINs with them, place logon information on a yellow sticky near their workstation, and even share their password.[49] Having easy-to-guess, or easy-to-reach passwords are a bad idea. Let's look at why.

Login authentication has been the basis of computer security since its foundation. Yet all one needs to login as someone else is their login name and the password. Most organizations make it real easy to guess a login name. Usually it is the same or similar to a person's email address name. Worse, default operating systems often display the last user logged in by default. This means half the login is already known. So guessing a valid password is all the hacker has to do, *to gain access as that person*, to access accounts, change data, or make financial transactions. Once in, the game is over, the attacker can easily place remote access tools or agents that open the backdoor for frequent re-entry. Attackers may not tell us they broke in. They may continue to use our identity, or use that system as a tool to attack other sites.

To make identity theft more difficult, we must secure our passwords. One method is to make the password harder to guess. Instead of using a word or simply numbers, use a "password phrase" instead. That is, use the 1st , 2nd, or 3rd letters of every word in a phrase you make up. Then place numbers and special characters mixed among the letters. Make some of the letters uppercase, some lower case. The resulting combination is a password unlikely to be guessed at using common password tools. The hacker must then resort to time-consuming job of hard cracking. And if the password length is reasonably long (7 or more characters), the hacker may well give up.

Remember that there are people in this world that have nothing better to do than eat potato chips and break code. We must not make it easy for them, or we lose. Strong, secure passwords are basic to protecting our identity. So to review password creation:

- Not a word or name
- Alpha numeric
- Upper and lower case
- Special characters (if allowed)
- Seven or more characters

5. Use Multiple Layers

Use a multiple layer defense strategy for all system and network components. The following examples are typical for a home computer system. Depending on the balance of risk, several tools may be modified or expanded upon.

5a. Virus Protection

Virus protection has been a basic computer system need since computer viruses and related logic first appeared in the wild. For microcomputers (PCs) these started in 1984 with the Morris Worm and 1986 with the Pakistani Brain. Some of us remember when these first appeared and were appalled at the ease with which these viruses spread. Losses sustained during early crisis and the time lag before anti-virus updates, prompted recommendations for multiple anti-virus vendors. Today, detection and updates have dramatically improved. So much activity occurs in the virus arena, that one (1) week is considered too long for anti-virus updates in the commercial world.

For home users, I recommend any regular, current anti-virus vendor. Each has their strengths. Use at least one product, and make sure it covers the software applications that you use. For example, some products support E-mail clients separately. Almost all Anti-virus systems include "memory-resident" modules that continually check system and downloaded files for virus activity. Common examples are V Shield from McAfee, and Net Shield from Norton/Symantec. Above all, subscribe to the automated update. Virus definitions get updated too frequently for manual updates anymore.

All users are reminded to scan all files from external sources. All files, including downloaded E-mail attachments, files downloaded from the Internet, and files from diskette, CD, or similar must be routinely scanned. It only takes once, for a nasty virus or Trojan Horse program to be injected into your system. The extra precaution is necessary because some viruses are smart, and will attempt to disable your Anti-virus system. For more on viruses, worms, and others, see the following sources:

Symantec Security Response
http://securityresponse.symantec.com/avcenter/vinfodb.html
McAfee AVERT Virus Information Library
http://vil.nai.com/vil/default.asp
The CERT Coordination Center Vulnerabilities, Incidents, and Fixes
http://www.cert.org/nav/index_red.html
SANS Institute Security Digests SANS NewsBites
http://www.sans.org/newlook/digests/newsbites.htm
National Infrastructure Protection Center (NIPC)
http://www.nipc.gov/index.html

5b. File Access

All users should have access to all files, not! We covered basic access control under Least Privilege. What's needed here is redundancy, or mitigated risk. If someone did break in, or heaven forbid, steal your computer, you would want further protection. Web site administrators are experimenting with "wrappers" and "sand-box" techniques to contain single system compromises from affecting other systems. While these methods are still too expensive for the average home user, other tools are available that can prevent spread, or further loss from a break in. *Encryption tools* are available to secure individual files or directories.

5c. Computer Access

The biggest set of tools is available for guarding computer access. This ranges from BIOS passwords to the most sophisticated application-layer "firewall." For most computer defense systems, this is the last defense, the castle wall protecting the crown jewels. Let us explore the options.

Install a personal firewall such as ZoneAlarm or Tiny. Currently home versions of these programs are free. Personal firewall protection rates the top of the list. Most network prowlers can be stopped simply by configuring a program to monitor and block unexpected network traffic. When configured properly, a software firewall literally monitors all access to and from your network interface. When misconfigured, even the most expensive firewall can let bad traffic pass. What is bad traffic? Anything that was not specifically requested by the current user may be considered bad. It may contain intrusion attempts, probes, and queries. It may contain benign network checks, or address updates from an upstream server. It may contain a connection attempt from a fellow "gamer" to allow smooth transactions during a game. Bad traffic may even be outbound data being sent automatically, unbeknownst to the user. Each home user's situation determines what is "bad" traffic. Being security-conscious, it is better to consider all traffic as bad unless we request it, based on the Principle of Least Privilege.

Some operating systems allow *configuration of an outbound "access list*." If available, this list can be set by IP address, and can limit or delay certain kinds of traffic to other inside or outside systems. This is important mitigation if one home system is compromised. Expected or limited privilege controls can prevent a problem from growing to be a disaster. This is also a consideration for using *different local administrator passwords* for multiple home systems. These can be kept in a safe somewhere, but will foil an intruder who guessed right on one system from compromising the rest.

Some system owners *lock the BIOS* or basic input/output system control on their system. This is a good idea, IF you have a good memory. BIOS configuration does not change much, but when needed, you could be locked out of your computer completely. But BIOS also allows one to change boot-up options, possibly by-passing some O.S. authentication. So balance this decision on risk and physical exposure. See Least Privilege for more.

Operating system choice is a decision that affects exposure to vulnerabilities. Some O.S. are based on Least Privilege and provide security accordingly. Most home O.S are designed to be as flexible as possible, easy to use, and come with installation strategies that are nothing short of exposing. Any system that automatically connects to a manufacturer's site is bad news. Beware of "easy to use." That phrase usually indicates one or more vulnerabilities that may expose the user to some harm for the sake of convenience.

For a new home or SOHO computer system, it is generally a good idea to start up the system isolated from the network. Close as many openings as possible before connecting to any network.

Software choice also determines exposure to vulnerabilities. Extra features, sample scripts, sponsored or "bonus" programs, all increase the likelihood of compromise. Use multiple layers when applying the principle of Least Privilege to software. Be aware of the function for which the software was purchased. Be careful of additional features, which may not receive adequate inspection or regression testing before inclusion. Remember that "default" installation may include "features" you know nothing about. Remember K.I.S.S. (keep it simple). *Turn them off*.

Network browsers (Netscape Navigator and Microsoft Explore) likewise contain added "features." Connecting to a manufacturer website by default exposes your computer to any script or defect that may currently infect that website. *Use "blank."* If you must default to a website choose one that you trust. Remember that all web browsing is "trust." Web pages contain scripts that can control actions on your computer. Most provide the "active content" and "eye candy" that makes the Internet so interesting. But web sites are not immune from attack either, and a hacked site could contain unfriendly code.

To minimize such exposure, *turn off features like Java Script and Active X*. Some sites won't work as intended. It may be good that some sites won't work as intended. Not all sites are a benign as we would like. To be sure, Java Script and Active X type programming are great tools. Web surfing may seem "both safe and anonymous. It's not."[50] That is a security risk the user must make an active choice about. Don't let someone else choose exposure for you. For different levels of exposure*, consider separation by function* ideas mentioned earlier in physical security. Different levels of exposure on the same computer expose all the users on that computer to the risk. Consider this risk before reducing the level of security open on your browser application. An excellent resource exists from The World Wide Web Consortium (W3C) for "Client Side Security" and other related web concerns. See WWW Security FAQ at http://www.w3.org/Security/Faq/wwwsf2.html.[51] Although W3C specifically disclaims its contents, the material provided by Stein and Stewart is commendable. I recommend all web users review the information available there to better understand Internet risks.

Do you have your own website? Then you have probably been exposed to numerous articles on vulnerabilities and associated risk. Web sites make easy targets because they must open portals for browsers to enter. They are built to allow complete strangers access information. Apply Least Privilege here in Depth. Here are a few tips worth noting for website and webpage owners. *Develop web content off-line*. Separation of public and private data areas is important, any slips during development or changes could expose sensitive data.[52] Burn and *use a CD-ROM* as the actual content source for web

page data. That eliminates the ability to modify content, a significant source of entertainment for early hackers.[53] Be very conscious of the exposed open ports and ensure additional countermeasures are installed to *monitor changes in files and attempted permission changes*. If handling visitor passwords and private information, apply procedures to mitigate risk. Privacy policy and records become important during any litigation regarding your site. For more, see the World Wide Web Server Side Security FAQ at http://www.w3.org/Security/Faq/wwwsf1.html.

Update software versions and apply patches necessary to secure all home systems. As mentioned previously, software is often shipped before all bugs are known, and some are virtually impossible to discover in a lab environment. "Field testing" as it is commonly known, is required to mature a program to withstand scrutiny. Often, patches and upgrades fix one problem, only to expose other vulnerabilities or "features" attackers can use. Shrink-wrapped software has even been known to contain viruses. It sure keeps security people on their toes. Best to *keep apprised of software patches* from vendors and third-party user groups to ensure the latest, best-fixed version is installed. "Because vendors are concerned with getting their software to customers as quickly as possible, they sometimes sacrifice security." "As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required..."[54]

5d. Network Access

The most basic protection available to home users is to pull the plug. This is effective, but not really efficient. "Air-gap" systems do exist to protect internal networks (Intranet) from external networks (Extranet or Internet). Few home users can justify such separation tools. IT Professionals certainly need a certain-level of home network protection.[55] So do executives, telecommuters, and the rest of the general Internet public. Especially as we respond to the call of Cyber Citizenship by fighting the threat of DDOS. To that end, here are several tools and comments that can be combined to provide reasonable, affordable protection from most Internet intrusion.

Install a hardware firewall. This could be a simple router with access lists applied, a personal computer with two interfaces setup to emulate a router, or a full blown commercial device with all the bells and whistles (literally). A home marketed "router' with network address translation (NAT) currently costs between $85 and $150 in the U.S. NAT is a great feature, but does not cure intrusion. Network Address Translation was proposed as a way to handle internal addressing. See original Request for Comment (RFC) for more. (RFC#1631)[56] It did not take long to see the security benefits of using non-routable addresses, so this has been marketed. NAT is recommended, but it is not a panacea.[57] Remember that Defense in Depth requires multiple layers, as "field testing" for products continue. A better router/firewall may include stateful packet inspection (SPI). SPI is a method where the firewall actually keeps track of outgoing data (packets) and only allows expected traffic back in. For more on stateful packet inspection, see Lisa Senner's Anatomy of a Stateful Firewall in the SANS Reading Room.[58]

Beware of wireless technology. While the convenience is a great feature, it is also convenient for someone else to snoop your network. Wireless simply has no controllable physical perimeter. For more, see Ken Hodges' wireless paper in the SANS Reading Room.[59]

Detection is a Must

The icing for computer security is "Prevention is Ideal, but Detection is a Must." Ideally, we'd all like to prevent computer crime. But computer crime does happen. No system, nor home for that matter, is 100% safe. Accidents can and do happen, as do break-ins, theft and other crime. The goal here is detection. If some entity, somehow, managed to bypass all our layered security, how would we know? Aside from broken glass and tire marks in the lawn[60], it would be more helpful if we had a video security camera that could help solve a break-in.

Having dependable logs, for example, would be helpful for law enforcement as well as providing a level of scope for the intrusion. When available, logs can show exactly when the system was compromised, what vulnerability was used, which system or files might be affected, and maybe where the attack came from. Access to this kind of information is critical to a CSIRT in quickly assessing the damage, aiding law enforcement investigation, and getting an organization's systems back in business. Similar tools and logs can be used at home for the same purposes.

Here are some ideas to apply the Detection principle at home:

Install Intrusion Detection. A software-based intrusion detection system (IDS), like BlackIce or similar, is ideal for exposing compromise and logs. Some have firewall features, which can also help reduce exposure. It is okay, even recommended, that detection overlap already covered features as part of Defense in Depth. Should one firewall fail or be misconfigured, the second firewall or IDS can detect the compromise and minimize the exposure. Some IDS software currently markets for under $40.

Log everything. Good logs are essential to exposing compromise details and enabling fast, efficient response. Investigators use logs for forensics as well as evidence if needed during prosecution. You want the logs as accurate as possible. Logs with gaping holes are not very useful. Attempted attacks and "successful" attacks can help justify resources spent on security. They can also reveal areas where security may still be weak. Don't worry about getting too much data. That can be sorted out later. See Appendix for More on Logs.

Logs provide metrics. Programs can be used to graph logs into usable forms that show trends and exceptions. Used in this way, logs can be very revealing. Log sorting and reviewing is not an easy task, use available tools to automate the process of sorting,

filing, and archiving logs. Look for syslog() programs or use WallWatcher.[61] For more tools like these, see Practicallynetworked.com.[62]

Notification tools are essential. No home user is going to review the entire log every day too look for patterns or exceptions. Commercial organizations use automated tools to check logs for specific words, events, or "triggers" that can signal a human for intervention and further review. These may pop up a window, play a sound, send E-mail, or even page or call a cell phone with an automated message. These tools are mature enough that prices are now affordable for the home user for some basic features, or they may be included with your firewall or IDS.

Closing Summary:

The Principles of Security can be applied now. The toolbox is full. Most of the security measures may be put to use without any purchase at all. Some may require minor expenditures, probably a tiny fraction of the price paid for the home computer system.

All security measures require an awareness of Risk and the associated threats and vulnerabilities. The motivation for action is quite clear:

- Home computer systems are generally not secure
- Computer crime threatens our data, and our identity
- To protect ourselves, Security Measures must be applied
- By applying security, we reduce risk for the Internet-at-large

Let's review our toolbox. It contains four drawers:

- Know Thy System
- Least Privilege Principle
- Defense In Depth
- Detection Is a Must

Here are all the tools discussed that are available to the home user. Not all tools will be used at the same time. But most will be applied, and new ones will be discovered:

- Know Thy System tools:
  - Learn about the computer system
  - Observe "what is normal"
  - See exactly what is where – Show file extensions and detail view
  - Build a Baseline – Make a Backup
  - Test backup recovery and steps
  - Learn about flaws and "back-doors"
  - Get the word about current threats and new tools
  - Be aware of privacy concerns and social engineering

- Principle of Least Privilege Tools in the Toolbox:
  - Review home system user needs – Write the policy
  - Restrict physical access – Who can see or drip on my keyboard?
  - Configure access times - Use timers and "locks" both software and hardware
  - Limit login rights and shares as much as possible
  - Check access rights and shares routinely
  - Remove extra programs and unused "features"
  - Take control - Look for "leaks"

- Defence In Depth Tools in the Toolbox:
  - Education, awareness, and training – Take a class
  - Physical locks and alarms and camera – Keep it from "walking"
  - Lock the BIOS in public areas
  - Separate system functions with removable hard drives
  - Place second copy of backup at another location
  - Save often
  - Filter all power through surge protectors or UPS systems
  - Make checklists
  - Use good passwords

  And the other drawer of Defense in Depth Tools:
  - More than one virus protection method – Be vigilent
  - Apply Least Privilege to files and accounts
  - Install software firewalls on all systems – strongly configured
  - Add an outbound access list
  - Adapt different passwords on each system and change them seasonally
  - "Lock-down" your web browser, too much Java (and X) is no good for you
  - Be considerate – Do not expose other users by bypassing security

  And Important Defense Tools for Programs and Internet:
  - Change or upgrade the operating system when needed
  - Secure before using – Close the door before driving down the superhighway
  - Remove "default" software features – When in doubt, turn it off
  - Auto-update virus signatures
  - Insert a NAT router
  - Download and configure software firewalls
  - Add a second hardware firewall if you can
  - Use a firewall with Stateful Packet Inspection

More Tools for Web page hosts:

- Build it off-line – Test it off-line too
- Use CD-ROM for content
- Install Trip-wire and other monitoring tools

- Prevention Ideal, but we also need tools for Detection is a Must:
  - Install a backup alarm, the IDS, to verify other tools
  - Log everything
  - Use tools to automate log checking and archive
  - Configure bells and whistles to alert you before damage is done

Wow, that's quite a toolbox. Remember that no system is 100% safe. Do not expect to apply all the tools available. Too many locks make the system hard to use. The focus of Cyber Citizenship is crime prevention. Rather than ignore the risks, be attentive to them and take steps to minimize your vulnerable spots. As more Cyber Citizens apply these tools to their systems, it becomes tough for would-be criminals to pose a threat.

Awareness and motivation are key to reducing crime on the Internet. As users protect their private information and systems from theft and invasion, computer crime is averted. A benefit for others appears as fewer systems can participate in distributed denial of service (DDOS) networks. So practicing Cyber Citizenship truly helps defend the Internet. Defense in Depth for the Home User makes it possible to protect both our personal systems and data, and other organizations.

###

Appendices and Notes

Interesting snippets for further study:

In 1989, Tim Berners-Lee created a proposal for a hypertext document system to be used within the CERN community. Although based in Switzerland, CERN members were scattered throughout the globe and project turnover was often high. Collaboration over long distances, getting new project members quickly up to speed and preservation of information in the face of frequent member turnover were the driving factors in the development of the proposed system. This system, which Berners-Lee later named "The World-Wide Web" in October of 1990, outlined several important components necessary to realize the vision and which, in a nutshell, defines the nature of the WWW today.[63]
From: http://www.blooberry.com/indexdot/history/html.htm

The Economics of Information Warfare, 26 March, 2001
http://securityresponse.symantec.com/avcenter/security/Content/2001_03_26.html
An article demonstrating the danger of using only one defense mechanism and describing the advantages of layered security solutions is now available. Description: "A security measure like a firewall, IDS, vulnerability assessment, or anti-virus, when used alone, is not as effective as when those measures are used together as part of an in-depth security solution. Consequently, security measures used piecemeal, make it easier for an attacker to be successful because it lowers his total cost. A comprehensive security solution incorporating a firewall, network and host intrusion detection, vulnerability assessment, and anti-virus, create a security solution that is expensive for an attacker to defeat." Last modified on: Friday, 13-Apr-01 09:17:53

Symantec Contribution to Microsoft Security Operations Guide
http://securityresponse.symantec.com/avcenter/security/Content/security.articles/security.fundamentals.html
"Symantec is pleased to collaborate with Microsoft on their Security Operations Guide. The Security Operations Guide is an excellent set of specific configuration recommendations that if followed will result in formidable security for Windows server platforms. Below is a set of information security articles written by Symantec security experts that expand on key points within the Security Operations Guide…These Symantec Enterprise Security Manager™ policies are free to Enterprise Security Manager™ maintenance paying customers."

- Fundamentals of Information Security (80-20 Rule)
- Defense in Depth Benefits
- Corporate Security Policy
- Microsoft Security Operations Guide
- Review Microsoft's Security Operations Guide.

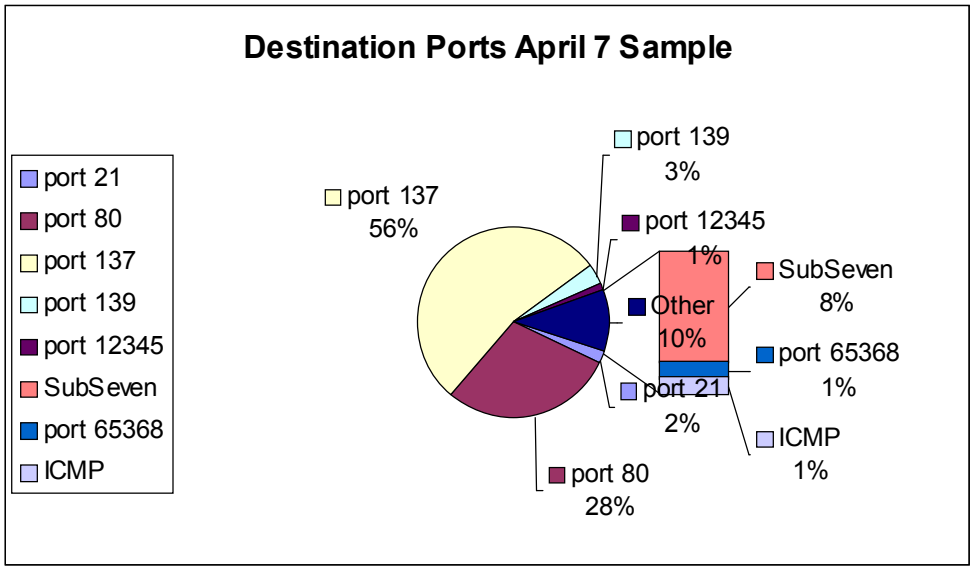
More on Logs.

Many security defenses provide logging capabilities. Capture the data. With a little research and some finesse, you can convert indecipherable logs into usable summaries and charts. GREP or simple cut-and-paste, are readily available tools for the home user. Below is raw data and a useful graph from a Zone Alarm Log sampling from April 7, 2002.

TURN THIS:

FWIN,2002/04/07,09:22:47 -10:00 GMT,10.10.X.X:1034,192.168.X.X:137,UDP
FWIN,2002/04/07,09:25:48 -10:00 GMT,10.11.X.X:1025,192.168.X.X:27374,TCP (flags:S)
FWIN,2002/04/07,09:26:39 -10:00 GMT,10.12.X.X:67,255.255.255.255:68,UDP
FWIN,2002/04/07,09:38:37 -10:00 GMT,10.13.X.X:1822,192.168.X.X:80,TCP (flags:S)
FWIN,2002/04/07,09:40:34 -10:00 GMT,10.20.1X.X:3483,192.168.X.X:137,UDP
FWIN,2002/04/07,09:52:45 -10:00 GMT,10.21.1X.X:2390,192.168.X.X:80,TCP (flags:S)
FWIN,2002/04/07,10:16:54 -10:00 GMT,192.168.X.X:1025,192.168.X.X:137,UDP
FWIN,2002/04/07,10:27:14 -10:00 GMT,10.14.X.X:67,255.255.255.255:68,UDP
FWIN,2002/04/07,10:28:03 -10:00 GMT,10.15.1X.X:4250,192.168.X.X:80,TCP (flags:S)
FWIN,2002/04/07,10:34:25 -10:00 GMT,10.22.X.X:4734,192.168.X.X:139,TCP (flags:S)
FWIN,2002/04/07,10:39:31 -10:00 GMT,10.16.1X.X:1336,192.168.X.X:80,TCP (flags:S)
LOCK,2002/04/07,10:46:35 -10:00 GMT,Netscape Navigator application file,10.30.X.X,N/A
FWIN,2002/04/07,10:52:03 -10:00 GMT,10.23.X.X:1031,192.168.X.X:137,UDP
FWIN,2002/04/07,10:52:24 -10:00 GMT,10.1X.X.X:4478,192.168.X.X:80,TCP (flags:S)
FWIN,2002/04/07,10:59:09 -10:00 GMT,10.1X.1XX.X:2223,192.168.X.X:80,TCP (flags:S)
FWOUT,2002/04/07,11:21:03 -10:00 GMT,192.168.X.X:68,10.31.X.X:67,UDP
FWIN,2002/04/07,11:24:21 -10:00 GMT,192.168.X.X:4592,192.168.X.X:27374,TCP (flags:S)
…

INTO THIS:



Simply by using common applications like WordPad and Excel.

EndNote References:

1 Rik Farrow, Network Magazine Feb 5, 2001
DDoS Is Neither Dead Nor Forgotten (p3,4,5)
http://www.networkmagazine.com/article/NMG20010125S0003

2 Moria West-Brown, CERT Coordination Center, SEI October, 2000
Avoiding the Trial-By-Fire Approach to Security Incidents
http://www.stsc.hill.af.mil/crosstalk/2000/oct/westbrown.asp

3 Brian Wilson HTML Overview
http://www.blooberry.com/indexdot/history/html.htm

4 Kevin Werbach http://werbach.com/ Version 4.0 January 1999
The Bare Bones Guide To HTML
http://werbach.com/barebones/barebones.txt

5 The World Wide Web Consortium (W3C)
http://www.w3.org/MarkUp/ especially http://www.w3.org/MarkUp/#historical
http://www.w3.org/History/19921103-hypertext/hypertext/WWW/TheProject.html

6 Aredridel <aredridel@nbtsc.org> Date: Thu, 4 May 2000
See "It's just -technically impossible- for email to directly carry a virus."
http://www.nbtsc.org/lists/nbtsc-l/archive/msg15185.html.

7 Lincoln Stein and John Steward for The World Wide Web Consortium (W3C)
WWW Security FAQ Client Side Security July 28, 2001 p21
http://www.w3.org/Security/Faq/wwwsf2.html

8 The CERT® Coordination Center http://www.cert.org/
See protective measures and methods of infection at:
http://www.cert.org/tech_tips/virusprotection.html January, 2000
See specific reports on Love Letter virus and Melissa Macro Virus:
http://www.cert.org/about/loveletter5-2000.html May 4, 2000
http://www.cert.org/advisories/CA-1999-04.html March 31, 1999

9 Robert Trigaux, St. Petersburg Times, Jun 14, 1998
The Underbelly of Cyberspace – A History of Hacking
http://www.sptimes.com/Hackers/history.hacking.html

10 Haeji Hong, University of California reprint 1998
Hacking Through the Computer Fraud and Abuse Act

http://www.law.ucla.edu/students/studentorgs/BLT/html/i3-hh.html

[11] Ronald B. Standler
Computer Crime, June 1999
http://www.rbs2.com/ccrime.htm

[12] Rosanna Lee, The Risks Digest Volume 3: Issue 51 September 7, 1986
originally from Chicago Tribune and San Jose Mercury News, Sept 5, 1986
"Computer Sabotage of Encyclopedia Brittania"
http://catless.ncl.ac.uk/Risks/3.51.html

[13] Ibid. Robert Trigaux, St. Petersburg Times, Jun 14, 1998
The Underbelly of Cyberspace – A History of Hacking
http://www.sptimes.com/Hackers/history.hacking.html

[14] National Information Systems Security (INFOSEC) Glossary
NSTISSI No.4009 September 2000
http://www.nstissc.gov/assests/pdf/4009.pdf

[15] The Honeynet Project http://project.honeynet.org
See Statistics: Number of port scans per day
http://project.honeynet.org/papers/stats/ July 22, 2001

[16] Ibid. The CERT® Coordination Center http://www.cert.org/
See http://www.cert.org/annual_rpts
And http://www.cert.org/archive/pdf/attack_trends.pdf

[17] Microsoft Corporation © 2002 article posted December 15, 1999
On Windows2000: Benefits of Remote Application Execution
http://www.microsoft.com/windows2000/server/evaluation/business/terminal.asp

[18] Gary Hinson, http://www.users.totalise.co.uk/~g4ifb/index.htm November, 2000
Rick Assessment Paper "A practical model for risk assessment and prioritisation"
http://www.users.totalise.co.uk/~g4ifb/Audit_papers/Risk_assessment/body_risk_assessment.htm

[19] SANS Information Assurance Foundations 2001
SANS Security Essentials II: Network Security p.1-8

[20] Computer Consultants of North Alabama
Page on Network Security
http://www.ccona.com/networksafe.html

[21] Ibid. Rik Farrow
DDoS Is Neither Dead Nor Forgotten (p2)

[22] Ibid. The CERT® Coordination Center http://www.cert.org/
http://www.cert.org/advisories/CA-2000-01.html

[23] Ibid. Rik Farrow
DDoS Is Neither Dead Nor Forgotten

[24] Dave Dittrich, http://staff.washington.edu/dittrich/misc/ddos
Personal comments on DDOS Conference, December, 2001
http://staff.washington.edu/dittrich/misc/ddos/lockheed.txt

[25] Ibid. Dave Dittrich, http://staff.washington.edu/dittrich/misc/ddos
Personal comments on DDOS Conference, December, 2001
http://staff.washington.edu/dittrich/misc/ddos/lockheed.txt

[26] E. Eugene Schultz Lawrence Livermore National Laboratory
CIAC Incident Handling Guidelines July 23, 1990
See section 3.4 History of Computer Viruses reference 1980 - IBM Trojan.
"All IBM 4341's stopped at 7:30 AM on 11 April 1980. Logic bomb planted by disgruntled employee"
http://escert.upc.es/mirrors/ciac_docs/ihg.txt

[27] Daniel J. Ryan, May 1993
Economic Implications of Information Systems Security Failures
He references the April 11, 1980 IBM logic bomb
http://www.danjryan.com/Econseq_WP.html

[28] Thurston Hatcher, http://www.CNN.com March 12, 2001
Survey: Costs of computer security breaches soar
2001 "And of the 186 respondents willing to detail how much they lost, the deficits totaled nearly $378 million. In 2000, 249 respondents said they lost about $265 million."
http://www.cnn.com/2001/TECH/internet/03/12/csi.fbi.hacking.report/?related

[29] Ibid. Ronald B. Standler
Computer Crime June 1999
http://www.rbs2.com/ccrime.htm

[30] Daniel Crider, November 22, 2001
A 6-Layer Defense for an I.T. Professional's Home Network p1
http://rr.sans.org/homeoffice/6layer.php

[31] Ibid. The CERT® Coordination Center http://www.cert.org/
See http://www.cert.org/annual_rpts
And http://www.cert.org/archive/pdf/attack_trends.pdf

[32] Lorraine Cosgrove Ware, CIO Research Reports
source: *CIO* and *Darwin* magazines
Executive Cyberthreat Awareness Survey, February 6, 2002
http://www2.cio.com/research/surveyreport.cfm?id=73 and
http://www.cio.com/research/cyberthreat_es.cfm

[33] Ibid. The CERT® Coordination Center http://www.cert.org/
CERT® Coordination Center 2001 Annual Report, see CA-2001-20
http://www.cert.org/annual_rpts/cert_rpt_01.html

[34] See SANS reading room papers on Policy
http://rr.sans.org/policy/index.php

[35] Ibid. Moria West-Brown
Avoiding the Trial-By-Fire Approach to Security Incidents
http://www.stsc.hill.af.mil/crosstalk/2000/oct/westbrown.asp

[36] Example reports can be reviewed at
E-Soft, Inc. SecuritySpace.com
Internet Research Reports
https://secure1.securityspace.com/s_survey/data/index.html
Another very interesting report just published 17 April 2002
considering the large base of AOL users is
Rich Mogull, The Gartner Group http://www.gartnerg2.com
AOL's Instant Messenger Compromises Browser Security
http://www.gartnerg2.site/../research/na-0402-0030.asp

[37] Ibid. Dave Dittrich, http://staff.washington.edu/dittrich/misc/ddos
Personal comments on DDOS Conference, December, 2001
http://staff.washington.edu/dittrich/misc/ddos/lockheed.txt

[38] Shawn Hernan, The CERT® Vulnerability Handling Group
Security Often Sacrificed fpr Convenience October 2000
http://www.stsc.hill.af.mil/crosstalk/2000/oct/hernan.asp

[39] Neill Edwards, National Cyber Security Alliance
Stay Safe Online Campaign News Release March 12, 2002
http://www.staysafeonline.info/press/031102.adp

[40] Cisco Systems, Inc. News Release February 7, 2002
Cisco Supports Stay Safe Online Campaign
http://newsroom.cisco.com/dlls/corp_020702b_print.html

[41] SANS ALOHA IV February 2002
Eric Cole on Security Principles
SANS Security Essentials I

[42] Global Incident Analysis Center © 1999 - 2000 SANS Institute
Incident Handling Step by Step: Unix Trojan Programs - Version 2.1
http://www.sans.org/y2k/DDOS.htm

[43] Ibid. Computer Consultants of North Alabama
Page on Network Security
http://www.ccona.com/networksafe.html

[44] Lawrence R. Rogers, The CERT® Vulnerability Handling Group
The Internet – Friend or Foe? Jan 7, 2002
http://www.cert.org/archive/pdf/homeusers/friendorfoe.pdf and
Is there an Intruder in my Computer? Feb 26, 2002
http://www.cert.org/archive/pdf/homeusers/intruder_computer.pdf

[45] Ibid. Lawrence Rogers, The CERT® Vulnerability Handling Group
Is there an Intruder in my Computer? Feb 26, 2002
http://www.cert.org/archive/pdf/homeusers/intruder_computer.pdf

[46] Ibid. The CERT® Coordination Center http://www.cert.org/
See CERT® Advisory CA-1991-04 Social Engineering
Last Revised September 18, 1997
http://www.cert.org/advisories/CA-1991-04.html

[47] Vincent Wallace February 12, 2001
Personal Firewalls: Not Enough p2
http://rr.sans.org/firewall/not_enough.php

[48] Ibid. Eric Cole SANS ALOHA IV February 2002

[49] Ibid. The CERT® Coordination Center http://www.cert.org/
See CERT® Advisory CA-1991-04 Social Engineering
Last Revised September 18, 1997
http://www.cert.org/advisories/CA-1991-04.html

[50] Lincoln Stein and John Steward for The World Wide Web Consortium (W3C)
WWW Security FAQ General Questions p2 July 28, 2001
http://www.w3.org/Security/Faq/wwwsf1.html

[51] Ibid. Lincoln Stein and John Steward for The World Wide Web Consortium (W3C)
WWW Security FAQ Client Side Security, July 28, 2001
http://www.w3.org/Security/Faq/wwwsf2.html

[52] Free Security Tips
http://www.cyberdefenders.com/freesecuritytips.html

[53] Ibid. Robert Trigaux, St. Petersburg Times, Jun 14, 1998
The Underbelly of Cyberspace – A History of Hacking
http://www.sptimes.com/Hackers/history.hacking.html

[54] Ibid. The CERT® Coordination Center http://www.cert.org/
Security Knowledge in Practice
http://www.cert.org/security-improvement/skip.html
Also see CA-2002-03 Solution, "Disable the …. service"
http://www.cert.org/advisories/CA-2002-03.html February 12, 2002

[55] Ibid. Daniel Crider, November 22, 2001
A 6-Layer Defense for an I.T. Professional's Home Network
http://rr.sans.org/homeoffice/6layer.php

[56] See original Request for Comment at
www.ietf.org/rfc/rfc1631.txt

[57] Timothy W. Foreman, November 9, 2000
Network Address Translation – Not a Security Panacea
http://rr.sans.org/firewall/net_add2.php

[58] Lisa Senner, May 9, 2001
Anatomy of a Stateful Firewall
http://rr.sans.org/firewall/anatomy.php

[59] Ken Hodges , September 10, 2001
Is Your Wireless Network Secure?
http://rr.sans.org/wireless/wireless_net2.php

[60] Ibid. Lawrence R. Rogers, The CERT® Vulnerability Handling Group
Is there an Intruder in my Computer? Feb 26, 2002

http://www.cert.org/archive/pdf/homeusers/intruder_computer.pdf

[61] WallWatcher.com
http://www.wallwatcher.com

[62] PracticallyNetworked.com
Tools - Routers & Linux – including logging tools
http://www.practicallynetworked.com/tools/tools_index_pg2.htm

[63] Ibid. Brian Wilson HTML Overview
http://www.blooberry.com/indexdot/history/html.htm

Last Updated: October 19th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive