Global Information Assurance Certification Paper

Can Computer Security Be Achieved?

Daniel Cleary
GSEC Certification Paper
Version 1.4c Option #1
1/1/2005
Track #1

Can Computer Security Be Achieved?

ABSTRACT:

The idea of computer security has been around for a very brief time. This has a lot to do with the fact that the world of computers has only been around for less than a hundred years. “Real” computers, in the way that we see today have only been around for about fifty years. The first networks began appearing in the late seventies early eighties. Even when these networks began appearing they were very small networks funded by the government with the main purpose of connecting colleges across the country to share resources and data. During this time access was limited as were the speed of the lines and amount of data available. In short, there was little worth gaining unauthorized access into, and very few people even knew of its existence. Since the mid-nineties the number of computers and networks has skyrocketed. With this increase has come the age of computer security. Due to the amount data, bandwidth and potentially profitable or interesting material on lightly protected networks and computer systems, the world of security is booming. In an effort to increase revenue software companies across the board have stuck to the adage, “sell now, patch later,” which is the root of a substantial number of vulnerabilities and threats. “Indeed, the current maxim among software companies appears to be ship now, patch later—a policy that has produced a software infrastructure riddled with security holes.”(Alderson) The blame generally lies on Microsoft, but in reality the only reason Microsoft has become the biggest target is mostly related to its widespread use and monopolistic licensing and compatibility policies. "The real weak link is humans, not the bugs in Microsoft's software."(McCue) The future seems to be full of more and more computers and with every increase in security comes an increase in the ability of people to take advantage of this ever growing number of computers. Even if security in computer systems could be secured with better programs, patches, anti-virus and IDS systems there will always be a huge security gap…..people. Now and in the future the weak-link in computer security is and will be users. No matter how secure a computer is, it cannot stop a person from sharing a password or intentionally compromising a system. The number of security events increases with the increase in the number of users and systems. The question becomes, Can we truly create a secure computer environment as long as people are running the systems?

The art of social engineering is an old game with a new name. What social engineering basically amount to is the modern day equivalent of a "matchstick man" or con man. In general social engineering involves building a level of trust with someone in order to get that person to divulge information they should or would not normally reveal. A man named Kevin Mitnick is a renowned "hacker" who was imprisoned and recently released into the computer security field. By his own admittance he is and was never particularly adept at compromising phone or computer systems. What he was good at was compromising people by gaining their trust. "Gather as much information about the target as possible, and use that information to gain trust as an insider. Then go for the jugular."(Mitnick) Social engineering can be as small as an employee pleading with a co-worker to borrow a password because they forgot theirs and feel embarrassed asking for a new one "again." Something as simple as this can be considered social engineering due to the fact that the employee is using the trust they have built with the co-worker to obtain their password. The unsuspecting co-worker could be unwillingly setting themselves up to take the fall for their friend's malicious actions. It is in people's nature to help others and to trust, most often people just think they are being nice and doing the right thing by helping people they know and trust. This act of trusting others is rooted in the fact that for 99% of the time people are not out to deceive you. This 1% is what social engineers take advantage of. Social engineering does not need to solely in person or over the phone but instead is growing through email. Email expands the ability of con artist to exploit the small possibility that someone might fall for the con. Traditional methods of social engineering are often time and resource consuming. In addition these forms of social engineering are inherently risky since the culprit actually has to insert him or herself into a place they are unauthorized to be. With email, con artists are able to target a large number of people quickly and inexpensively making it an ideal means of doing "business." This method of attack also limits the attacker's exposure to traditional forms of being traced and identified. This form of attack grants the perpetrator nearly complete anonymity, which means that he or she can attack without the fear of being caught. The number of email-based scams has skyrocketed in recent years. Often it is the nature of people again that lands them in trouble. One form of email scam is based around the premise that you have won something but must do something to receive your prize. Usually what you have to do to receive your prize is to send a certain amount of personal information to the con artist in order to "verify" your identity. The con either uses this information by itself, or uses it to later extract more substantial information. Another prevalent form of social engineering is called "reverse" social engineering. This form of attack preys on our greedy nature; people are often willing to divulge substantial amounts of personal information in order to receive a relatively useless or worthless prize. Reverse social engineering is pulled of by advertising a service such as PC repair and once inside the social engineer does his damage. A new email scam is spreading like wild fire and is called phishing. Phishing is a way in which the true location of a hyperlink is hidden; therefore it is easy to impersonate a legitimate website. You receive an email from someone who you think is your credit card company. The email says you need to verify your

account information due to a security issue with your account. The email provides a link that has the name of your banks webpage, and the webpage looks identical to your banks page. However, the page is fake and when you enter your information it falls directly into the hands of the perpetrator. This form of social engineering takes sort of a shortcut. The social engineer in this case skips having to earn your trust because you all ready have trust in your credit card company. This makes the task a lot easier and many times more effective. The numbers of ways you can fall victim to social engineering are too many to count. The scariest thing about social engineering is that no matter how secure a computer system is it can be compromised easily by a user having the appropriate access falling victim to a social engineering based attack. Corporations use policies to enforce the rules and regulations that they wish to implement. Policies are a start but for the most part are underutilized and users are not properly trained on the policies in place. So printing out policies and giving them to employees is not enough, people need to understand and follow them. You can reduce the number of incidences through training and possibly by instating penalties, but as long as there are people sitting behind the computers there some of them will be conned.

For many employers the biggest threat to there computer and network security comes not from the outside, but from within. Again the major issue here is trust. Employers, for the most part, trust their employees not to do anything to harm their organization. This is often a weak-link in the chain of security; internal users can pose the greatest threat whether they act maliciously or otherwise. Most companies devote most of what little money they have for security on the external threat. They put firewalls, IDS, packet-sniffers and anti-virus in place to ward off attacks from outside of their network. There are two basic types of attacks that come from within, the intentional and the accidental. Depending on the severity either one can be equally damaging but the intentional attacks tend to do more damage. The accidental attack from an insider; whether it be an employee, consultant, or volunteer can be extremely hard to detect and prevent. When a person has legitimate access to a network or computer it is hard to determine whether that person is doing their job or downloading mp3's slipstreamed with Trojans and key-loggers. The best example of this that I know comes from my own personal experience. At the place where I work a woman approached me to say that she opened an email from an unknown source. This goes against a well known company policy, but did not surprise or worry me much at first. She then continued to tell me that she opened a link and proceeded to download and install a program that did not appear to "do" anything. The only reason she brought it to my attention was due to the fact that since that time the hourglass was spinning on her computer even when she was not working. Upon further investigation I determined that she had downloaded a Trojan, which installed two key-loggers that luckily could not connect through the firewall. When I asked her why she had done something that she was repeatedly trained not to she simply stated that she was curious where the email came from. This employee was not only trained repeatedly, but due to HIPPA regulations knew that an infraction could cost her or the company thousands of dollars. This type of behavior may mean job security for me, but it

also strikes a blow to the idea that security can be achieved. “End-users are still the main cause of virus infections in the workplace, as they continue to open suspicious email attachments and use online file-sharing and instant messaging services, according to experts.”(McCue) Employees can be trained, reminded and disciplined but curiosity, carelessness and just plain stupidity can lead to catastrophe. The other more troublesome threat is a malicious inside employee. This can be any person in an organization with access to computer and network resources, from the CEO to the janitor. One of the most major threats inside a company actually comes from the cleaning staff, and with good reason. Cleaning staff often has access to most every part of an organization, have this access when no one else is there, and often are paid so poorly that they are easily bribed by competitors or other employees. Another internal malicious threat is the disgruntled employee. Whether the employee is underpaid, underappreciated or just out for money this type of attack can be the most devastating to an organization. One example from my own experience involves an employee who got wind of her termination before her computer and network access were revoked. This employee proceeded to erase every bit of work they had done from their hard drive as well as all the departments’ work from the network drive. The network drive was successfully restored but the company lost thousands of dollars in work done by this employee on their local machine. It was also believed that the person caught wind of their termination by unauthorized permissions this person had to their bosses email. The permissions were in place for so long without anyone reviewing them, they had full administrative privileges on the network and there for the ability to read anyone’s email. In addition users generally have direct access to the hardware they use every day, unsupervised. With the advent of USB flash drives it is easy for an employee to plug in a 1 GB flash drive and download the company’s entire customer database. The biggest problems with these devices are that they are almost undetectable due to their size and unlike floppies they have the capacity to transfer major data files under the radar. “The problem of “rogue modems”, unauthorized modems which individual users have installed can still be an extremely dangerous threat to an organization’s security.”(White) Most companies today still use modems in one form or another. Often these devices are given little to no attention because the network administrators are too busy worried about the firewall and the high-speed connection tied to it. The majority of corporations have very little money to spend on technology, especially when the bottom line is concerned. When the funds are limited, security is often pushed to the back burner so that the money can be spent on other things. Security is usually an afterthought and gets little attention and even less money.

The final problem that comes into play in an organization of any type is one relating to passwords. Passwords and their policies/enforcement are the nemesis of every network administrator on the planet (slight exaggeration). It is plainly clear that passwords which are long, complicated and contain special characters are key to ensuring computer security. It is also clear that people cannot seem to remember or use passwords that are long, complex or use special characters. “Asking users to recall a single password and userid for one

system may seem reasonable, but with the proliferation of passwords, users are increasingly unable to cope."(Sasse) Passwords are sort of a catch twenty-two. If they meet the required prerequisites for being secure they are most often too hard to remember and need to be written down.

> If the password is more complex and non-intuitive (a random combination of letters and numbers), the user may have trouble remembering it, and this may lead to writing it down – often keeping it in a prominent place such as the top desk drawer or even on a sticky note stuck to the monitor. Users may also share their passwords with other users in an informal work environment. Even when users exercise reasonable diligence, hackers can often use "social engineering" to persuade users to divulge their passwords by posing as tech support or administrative staff. (Shinder)

In my eyes once a password is written down, whether on paper or digitally, it looses 90% of its effectiveness. I feel that this is the case because once a password is written down it becomes available to people who would have had no chance of getting it otherwise. The next problem with passwords becomes the shared password or group passwords. A shared password is one that is shared among co-workers when each has their own. The main reason this occurs is for the simple fact that people forget their passwords and don't wish to bother having it reset so they simply ask to borrow a co-workers. Group passwords are used when a group of people all need to have access to the same systems and it easier for the company to assign one or two passwords for everyone to use. The problem with both of these is that it allows users to access computer and network resources without any one really knowing who is actually accessing these resources. Anonymity in an organization is the worst thing when it comes to security. An administrator needs the ability to know accurately who is accessing what resources and when, this way if something wrong happens it is clear who was responsible. With the ever steady progression of technology the time it takes to crack even a complex password is steadily decreasing. While two years ago it would take 24 days to crack a complex password it now takes 24 hours. This time will only decrease, meaning that even the most secure passwords will be vulnerable.

The next real threat facing the apprehension of any real computer security is the threat from external sources. There are a few basic forms of an external threat can take; malicious compromiser, curious compromiser and the ever insidious competition. The malicious compromiser, most often known as the "hacker", enters an unauthorized computer system for the sole benefit of him or herself. Often these attacks are pursued either to achieve financial gain or simply for recognition. These compromisers can target an organization directly for various reasons, but more often than not choose to attack a network based on the ease of attack. The ease of attack can be determined by running port scans against a wide array of networks looking for weaknesses, once a perceived weakness is found the attacker will begin penetrating the system. This method of scanning actually works in favor of the organizations that have

even the most minimal security for the simple fact that it there are more often than not easier targets to pursue. The next type of attacker, the curious compromiser, is often the more elite in the computer underworld. This person often knows the ins and outs of computer systems and picks their targets carefully. More patient and skilled than the average “hacker” this type of attacker will slowly but surely gain information about a system through appropriately timed and crafted attacks to avoid detection. The only thing saving most corporations from this type of attacker is their growing obscurity and lack of desire to do harm to an organization. “They don't have a malicious intent, though they may have a lack of concern for privacy and proprietary information because they believe the Internet was designed to be an open system.”(Quittner) The final and most troublesome external threat facing corporations is the threat from competitors. An organizations competitor will often do any thing they can to learn as much information as they can about an organization. This frequently means that a competitor is willing to devote large financial resources to the procurement of information. Competitors have been known to hire “hackers” and current employees to do their bidding. This can lead to the divulgence of company secrets, as well as a company’s future plans. The world of corporate espionage and hackers for hire has become more prevalent in recent years due to the rise in connected systems. It is often cheaper for a company to hire a hacker to break in and steal trade secrets that it is for the same company to invest in its own research and development. Imagine if you owned a software company and spent 2 years developing a product only to have stolen and sold publicly before you even had the chance to market it. This type of attack can be detrimental to the affected company and extremely lucrative to the competing company. It is clear that the external threat to an organization can seriously affect the ability of that organization to achieve a secure computing environment.

One of the major factors affecting computer security is not whether we can secure systems, but whether we can use the systems once they are secure. If a password is complicated enough to be secure, but can’t be remembered or written down, usability is lost entirely. Secure systems can be designed. With the use of secure ID cards, biometrics, voice recognition, RSA tokens and other means security to a certain extent can be achieved. “The more secure a system is, the harder it is to use. The harder it is to use a system, the less secure it will be.”(Krause) What prevents this from becoming a reality comes from many factors. The first and most ruling factor becomes cost, the implementation and use of any one or combination these technologies can quickly eat up an entire organizations administrative costs. The second factor to consider is risk assessment, what is the likelihood that any of these attacks would happen to an organization and what would the real impact be. For instance it would not be worth investing $30,000 in a generator in a building that has not lost power for five years. Another important factor to consider is the fact that people need to use computer systems to do their jobs. It is a tricky balancing act, determining which threats to address and which to ignore is a difficult task. A computer is a tool and if that tool becomes too hard or complicated to use then it becomes a liability to an organization. If security is too hard to use, people with either decide not to use it at all or to simply bypass it. For example, I had the pleasure

of touring a very secure NOCC (network operations control center) and had to pass through several layers of security personnel to reach the actually facility. I was astonished to see two men smoking just outside the secure fire door they had just propped open to go outside without having to pass through security. When attempting to achieve a secure computing environment, the vertex where security meets usability is crucial, and more often then not a very grey line. Elaborate systems may elevate the level of attainable security, but lower productivity to the point where it has a damaging affect on performance. To stay in business a company must remain competitive and no business is going to risk going under for security's sake.

It has become my opinion that it is now and for the foreseeable future unlikely that a truly secure computing environment will come true, as long as people are needed to run computers. Many companies and professionals preach and claim that there are ways to ensure security, but I see their methods and solutions as nothing more than band-aids. They can help, but they just don't do the trick. Due to the nature of the computer industry products will continue to be released now and patched later, and the "hackers" will always be one step ahead of the anti-virus and security industries. I see this task as an unachievable goal, though strides and advances will be made. True security can never be achieved as long as there are people running computers; users are the ultimate weak-link. The ever changing world of technology and computers in particular, does not lend itself to security. With an industry striving to release new software and hardware within a relatively short time frame, there is an inherent disregard for security. In an effort to be competitive and profitable there is an overwhelming abandon of secure practices industry wide. Some major corporations have made strides to improve, but only as the result of countless vulnerabilities and a fear of loosing shareholders. As long as people are using computers for personal or business use there will always be a reason for someone to compromise them, whether it is for financial gain or simple curiosity. Ultimately a truly secure computing environment is not achievable. To err is to be human, but to really screw up it takes a computer.

Works Cited

1. Alderson, David. “The role of economic incentives in securing cyberspace.” November 2004, CISAC Stamford; http://iis-db.stanford.edu/pubs/20765/alderson-soo_hoo-CISAC-rpt_1.pdf
2. Krause, Brian. “Security And Usability” Encentuate; 2004 http://www.encentuate.com/resources/usability.htm
3. McCue, Andy. “Users Still the Weakest Link.” Where Are You?; 5-12-2002 http://www.vnunet.com/News/1137373
4. Mitnick, Kevin. The Art of Deception Indiana: Wiley Publishing, 2002
5. Sasse, Brostoff and Weirich. “Transforming the ‘weakest link’ — a human/computer interaction approach to usable and effective security” BT Technol J Vol 19 No 3 July 2001; http://www.cs.ucl.ac.uk/staff/A.Sasse/ttw.pdf
6. Shinder, Debra. “Passwords: the Weak Link in Network Security.” Windows Security; 5-1-2004, http://www.windowsecurity.com/articles/Passwords_Network_Security.html
7. Quittner, Jeremy. “Hacker Psyc 101” TLC; 1-11-2004 http://tlc.discovery.com/convergence/hackers/articles/psych.html
8. White, Gregory P.H.D. “A Common Weak-Link in the Security Chain.” CSRC; 9-12-1999, www.csrc.nist.gov/nissc/1999/proceeding/papers/p35.pdf