Global Information Assurance Certification Paper

The Future of Security

Dominic Salemno

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b – Option 1

Summary

The main purpose of this research paper is to provide a general knowledge of current security systems and security systems that will be implemented in the future. This paper provides a good basis for future thought on state of the art technology. This basis includes the details of future enhancements that will lead to a more secure and trusted computing base. Finally, my main point is for this information to be used to make a better impact in the computer security field.

Introduction

"It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be...This, in turn, means that our statesmen, our businessmen, our everyman must take on a science fictional way of thinking."
--Isaac Asimov

Change is inevitable and we cannot change the inevitable. In our constantly changing society, we must continually look towards the future and expect the unexpected. Security as we know it has advanced much throughout history. We know to a certain degree how to handle possible weaknesses in the present infrastructure but as technology changes; we will see dramatic advances and possibly inescapable dangers.

Current Security Models and Methods

In present-day society, there is certain accepted approach to accomplish particular tasks. Many brilliant minds that have received their doctorates at various universities have published widely accepted models to implement computer security. These models have been shown to work and are carefully followed for those who take their security profession seriously.

Computer security methods that are in wide use today developed over time to keep up with the constant demands of newer technologies. As things change and evolve, the computer security methods must adapt to this constant shift. Despite the fact that we are an advanced culture, individuals and organizations implement out-dated procedures that do not take on the new threat. Newly devised techniques are constantly appearing to show different and more efficient

ways of accomplishing large tasks. Many followed some of these concepts in the beginning, but only recently have today's issues brought to light the unavoidable dangers of viewing security as an afterthought. Past professionals in the computer field looked over security briefly during the beginnings of the invention of the computer.

Computer systems implemented separate accounts, each with their own password to gain access to that particular system. Although this policy kept unwanted intruders out of the system, it failed to keep users from disrupting other users. Some systems did not put into place access controls to state what users could do with data not belonging to them. For example, once logged onto a particular system each user had their own personal directory to store files of their choosing. Once a user logged on, he or she could browse through the directories of the system mentioned and access files of other users. Unfortunately, most of the time users had full access to those files.

Computer Architecture and Infrastructure

Current security varies from system to system; depending on the architecture new vulnerabilities or inherent weaknesses may arise. A particular Architecture that is increasingly popular at this time is Intel's x86 series. An architecture described in computer science is not just the hardware that the computer uses but also the software that usually accompanies that particular hardware.

Many people complain about their computer always crashing and they emphasize the need for a new computer. Most people who are unknowledgeable in the area of computers assume that a new computer will have less system crashes. They have a distorted perception because they view the entire computer as the problem. One cannot blame the fact that Intel designed the particular CPU that is in use today. One must blame the software companies that produce the software that we regularly use on our computer systems. The x86 series has been used for many years now. Competent programmers with sufficient experience should understand the underpinnings when writing software for that particular system. Too little time is spent in the educational arena to properly teach what you are dealing with and what you should look for in modern-day computer systems. Most of the vulnerabilities that plague our current structure are easily categorized into three groups (buffer overflow, format string, and input validation vulnerabilities). We know exactly what we are dealing with and yet these things still cause havoc in our current society. Many blame it on lazy or uninformed programmers. Many security professionals that are widely respected are criticizing many corporations and organizations for developing such insecure code.

Software, as we create it, can come to a point of stability even though it is not perfect. Developing good and stable software usually takes some practice and

experience. Unfortunately, because of this basic fact many people will use the basis of imperfection as an excuse. The arguable point here, once stated by Jon Lasser, is that much of the bug-ridden software could have been avoided by using well-known programs to catch human error (StackGuard and FormatGuard).

Protocols

In the early stages of computer networking, the main goal was to get computers to talk between each other efficiently. Early network protocols were not designed with security in mind. Some applications prompted for a login name and password but it sent all of this information as clear text from source to destination. The significance of this is that early LANs (Local Area Networks) broadcasted all their traffic on the local network.

As time progressed, a new invention surfaced called a switch. This took care of most packet-sniffing problems but not all. With security implementations, there is usually a compromise with speed and/or performance. Not only did switching hubs implement security but also improved upon the speed of LANs. The drawback was they were more expensive but over time, the price for small office switches has dropped dramatically. An attack called ARP (address resolution protocol) poisoning allowed for a particular user on a segment to sniff packets destined for a particular host. All broadcast traffic could also be sniffed because broadcast is sent to every host on a segment, hence the name “broadcast.” Once the traffic leaves the LAN and heads out onto the Internet it is very vulnerable, so if you are in Maine and are communicating with a server in California anyone along the way can grab your password.

As mathematics evolved, computer professionals began to notice flaws in the system. Seeing the need for improvements, they developed communications protocols that use encryption algorithms to allow for secure transfer of data. SSH (Secure Shell) is one that was developed and is still very widely used. SSH uses asymmetric cryptography (public key cryptography) to decrease the chance of unauthorized viewing and tampering. Anyone sniffing traffic between two hosts will probably understand the traffic is encrypted but will have no idea what data is being transferred. There are also re-written protocols that use some cryptographic procedure. The same data is transmitted from host to host but the data is encrypted. The sending host forms the data, encrypts it, and sends it on its way. Upon successful retrieval of the data, the receiving host decrypts the data and then acts upon it. If the receiving host does not have the right key then none of this communication will work. One host can verify the identity of the other using this technique. Impersonators are easily caught using this simple security measure.

Operating System Design

Over the years, computer systems developed to allow consumers to choose an operating system based on their needs. The first operating system was supposedly developed by Gene Amdahl and was used on the IBM 704. Since then many operating systems for various platforms were developed. These operating systems have changed dramatically over time to meet the demand of the consumer. Command line interfaces were eventually taken over by graphical user interfaces.

"Only one remote hole in the default install, in more than 7 years!" This quote sits proudly at *http://www.openbsd.org* underneath the OpenBSD mascot, the blowfish. Many claim OpenBSD is one of the most secure operating systems in the world. Theo de Raadt, in the early 1990s, was responsible for the SPARC port of NetBSD. A disagreement with the core team led him to leave the development and start his own project named OpenBSD. The main goal for the OpenBSD project was to produce the most secure operating system in the world. Starting in early 1996 an audit was done on the source code of the operating system. This was not just a simple audit; this was a line-by-line analysis of the entire operating system. This project found a great number of bugs that related to possible vulnerabilities. Any errors they found, whether they were related to security or not, were fixed. OpenBSD's motto is "secure by default," and they claim that this is one of the most robust operating systems in the world. To continue this wonderful service the OpenBSD team provides an on-going audit of the system so they can catch new bugs when new features or software are implemented. The same developers who created and developed the OpenBSD project also created the OpenSSH project, thus producing a powerful way to talk to a remote computer in a secure manner.

Linux arises from nowhere. A young man at the University of Helsinki in his early twenties noticed a small operating system called Minix that was created by Andrew Tanenbaum. This young man's name was Linus Torvalds. He found an interest in Minix but only saw it as a tool for students and nothing else. Therefore, he decided to embark on his own crusade and create an operating system similar to Minix but something that professionals could actually use. After some time Linux has spread and continuing support and development has lead to its vast popularity. Many distributors advertise it as an alternative to the "dreaded" windows operating system. The Linux project gained so much popularity that it caught an eye at the National Security Agency (NSA). The NSA realized its potential, took Linux, and made alterations releasing a new distribution called "Security-Enhanced Linux." They implemented what is known as mandatory access controls within the operating system. The NSA also implemented a wide range of security mechanisms to configure the system to meet a wide range of policies. The new Security-Enhanced Linux still maintains the original terms that the original Linux offered. You can freely download documentation and source code from the NSA's site.

Microsoft started as a small company with the development of an operating system called DOS (Disk Operating System). It was a small command line interface without any security features and only ran one program at a time. It had no security features and you could for the most part only run one program at a time. Microsoft saw the need for a Graphical User Interface after seeing Apple's design. They created a new operating system called Windows.

After the first version was released, they continued development and added new features and made improvements where necessary. Windows was good for stand-a-lone personal computers but in the rise of computer networks, Microsoft saw a problem. They developed "Windows for Workgroups" which was the first operating system developed that offered networking packages. It provided peer-to-peer file and printer sharing. This idea later developed into a need for an operating system to run high-end servers; hence, Windows NT (New Technology) was born. Windows NT 3.1 was their first release and Microsoft continued to develop two different lines of operating systems. They developed one OS for the average home user and the other for high-end servers and the workplace. One of the operating systems was known for being highly insecure while the other had more security options.

Over time, Microsoft wanted to take the best of both worlds and merge the operating systems into one. The first large step into this area was the Windows 2000 Operating System. Windows NT 5.0 was officially named "Windows 2000" by marking it as a "mainstream" operating system. Windows 2000 added the customizability and features of Windows NT with the ease and multimedia options of the Windows 9x series. Later in that year, they released "Windows ME (Millennium)" which Microsoft probably later regretted.

Microsoft claimed Microsoft ME had huge advancements in the areas of multimedia and security but it was really a small upgrade to the previous versions of Windows. A memory leak was later found within the Windows ME operating system, which caused many problems for users. Every company is bound to make a mistake and this was probably one of Microsoft's biggest, because Windows ME did not have any security enhancements at all.

The next operating system and still the one most widely used is called "Windows XP (eXPerience)." This has proven to be a very good move for Microsoft indeed even though there are still problems that crop up. Microsoft implemented an activation feature within the software so one has to register through the Internet, or Windows will not run after a certain period of time.

It did not take long before a few mischievous hackers/crackers figured out how the key system worked and made key generators. Most of the keys generated where from windows operating systems that were not yet sold. Therefore, a user could buy windows XP and when they tried to install it and then activate it, it would tell them that their key could no longer be used. The user had to call

Microsoft and tell them the combination of letters and numbers on the screen and they would give them a working activation key.

When Windows XP was first released there came the issue of a nasty computer bug that resided within Universal Plug and Play. It allowed any person to control another person who was running Windows XP. They could control their entire computer, delete files, rename files, or possibly destroy their entire system. This was patched but not after a little havoc was done. The problem with Windows XP is that it runs a bunch of services by default that are either known to be dangerous or are not used very much at all. Universal Plug and Play was one of these services.

Another service that is widely used to deceive users is social engineering by way of the windows messenger service. A small dialog box would popup on a user's screen with the name of the person sending the message and the message itself. The problem is that there was many programs made that can spoof the address in the messenger service to make it look like it came from a legitimate source. Another problem is that most home users do not have a firewall so their messenger service was exposed to the entire world. Spammers used this to their advantage to deliver instantaneous advertisements to the user's desktop. Mischievous computer users also used this to their advantage. They sent messages telling the user of a problem with the security of their system and to fix this problem would require them to visit a specific site and download the software there. The site contained a software application that would run and release a Trojan horse onto the user's computer. This allowed anyone to control this novice user's computer. Once an attacker had control, they could steal sensitive information contained within files or through the interaction of the Internet. They could log all passwords that were typed, and view the user's screen as if they were behind the computer itself. To date some of these problems have been fixed and other problems have been posted on Microsoft's support site with possible solutions.

Earlier versions of Windows were very unstable and constant BSOD (Blue Screen of Death's) appeared. A blue screen of death is what happens when an unrecoverable event happens in the system. BSODs usually happen due to problems with "Ring – 0" code (hardware drivers) and/or privileged programs. The blue screen that resides on Windows XP actually contains more information about the system crash. Many make jokes about this type of error, hence calling it the Blue Screen of Death. When Bill Gates first introduced Windows 98 live on television the system crashed with a BSOD. There are obvious security issues associated with the Blue Screen of Death. If you sent an oversized packet to a Windows machine, it did not know how to handle it, causing a BSOD. Thus if hackers encountered a Windows machine on the Internet to cause a little mischief this is what was done.

Cryptography

Privacy and security has been a big issue for ages. The first recorded incident of crypto (short for cryptography) was in ancient Egypt when a scribe wrote down the story of his master's life in non-standard hieroglyphics. The scribe used a simple code of hieroglyphic substitution. This was not well known during his time. Later, Julius Caesar used a substitution cipher to aid his army and hide valuable information from his enemies. As time went along more advanced ways of encoding information was developed. The advancements in mathematics lead to harder to crack systems. Most of our valuable information today relies on an infrastructure known as public-key cryptography (asymmetric cryptography) as compared to its close cousin secret-key cryptography (symmetric cryptography). Symmetric cryptography uses one key. The same key is used for both encryption and decryption. As long as both parties have the same key, information can be sent and understood on both sides. The problem with this type of cryptography is key distribution. How do you get the key to the other party safely and securely? There has to be some initial communications before you are sending valuable information back and fourth. If the initial communication is on the Internet then the initial communication must be in clear text, otherwise one party will not understand the other.

A paper written by two individuals helps them invent a new way to communicate. The paper describes using a mathematical function that is one-way and asymmetric. After releasing the paper to the public, they received information back on how to implement such a crypto-system. This system works by using two keys. These two keys are conceivably called a public key and a private key. Each person has their own public key and their own private key. They release their public key out onto the Internet for everyone to see and they keep their private key a secret. The information they encrypt with their private key can only be decrypted with their public key and vice versa. This ensures authentication with another individual over the Internet. The way this system works is by using very large prime numbers; so large that it would take hundreds of years to break them down using today's computing power. As technology advances so does the speed of computer systems. Moore's Law states that the computing power of the world will double each year. We are advancing much in science and technology. To keep information a secret from increasingly fast computer systems people just increase the length of their keys.

Physical Security

You can have the latest software and secure configurations of that software but if someone can enter the room where your server is kept and pull the plug then you have nothing. As most people know, most computer crimes are perpetrated by insiders. Most of these are usually disgruntled employees or corporate espionage. Current technology is progressing in more advanced devices in this particular field. Large companies have badges for every employee. An employee swipes his/her badge into a card reader and the computer system validates that

employee. If the employee is successfully validated he or she is allowed to enter. If not, several other options are usually chosen like an alarm or armed guards holding you until the authorities get to the location. Once inside every other part of the building you want to gain access to, is validated by your badge. Once inside a particular room an employee can login to the computer system using his/her designated username and password. The username is usually their first initial of the first name and the last name. This classic type of security has many problems, what happens if someone steals your badge. This is particularly disturbing if the stolen badge belongs to one of the system administrators or security professionals.

As our culture begins to advance, we invent more complex inventions to handle the new threats that arise. Biometrics is a hot topic in the world of physical security. There are many methods of implementing biometrics. These include: fingerprint, iris, and retina scan, and speech and facial recognition systems. These systems can be implemented and can do a very good job at keeping unwanted intruders out. Using two or more of these technologies is also recommended. Once on the inside a company can have motion detectors in certain areas that are locked and off limits. These types of areas would include backup archives and the server room. Another useful technology is SecurID and/or Boot up USB Keys because no one will be able to power up the machine without the Boot up Key within the USB port. A SecurID implementation is another good option because the key changes every 60 seconds. It would be a great feat for an attacker to gain access to your system.

Future Technologies

As knowledge and technology improve and progress. Science evolves because we ourselves think of things that we would not have realized in the beginning. Will we get to a point where we can no longer advance? I am not quite sure, but the following is what the future of security holds in store for us.

Advances in Security Models/Methods

Protocols

There are many models to look at and, these models must continually adapt to an ever-changing computing field. The methods we use will most likely get more complex. We are not dealing with small amounts of data in this age. There are processing systems that deal with terabytes of information. Methods might also get simpler because our knowledge of things will increase in time.

Advances in Architecture/Infrastructure

The current architecture has helped us look at things at in entirely new perspective because there was a need to make machines that were backwards compatible with previous systems. Bigger leaps might be expected when dealing with future enhancements. I have read a news line not too long ago. This news article described building an operating system that was invulnerable to buffer overflows. Since heap overflows are in the same category it would kill off those as well. As security becomes more of a concern, hardware implementations will start to be built to handle these vulnerabilities.

Microsoft's current project code-named Palladium will implement cryptography within the computer hardware. Palladium's focus is to allow the computer to run in a secure processing mode. The computer will not boot unless it has a proper secure base. The CPU will include newer instructions and changes in the memory controller, and a flash module will be used to hold keys and hashed values. The problem with this architecture is that the user has no control over the keys on his or her system. Whitfield Diffie argues against Microsoft in this particular move, and Diffie states "users should have control over the keys located on their system."

Advances in Cryptography

Cryptography as we know it relies on the slowness of technological progress (Ref 5). If a quantum computer were invented tomorrow, all of the world's secrets would no longer be safe. To think one step ahead many are trying to build a new cryptosystem that is unbreakable. This new cryptosystem is called "Quantum Cryptography." As stated in the article from American Institute of Physics, "You'd have to break the laws of physics to break this code." The secrecy relies on the fundamental laws of physics laid out by Heisenberg's Uncertainty Principle. The principle states "the more precisely the position is determined, the less precisely the momentum is known." (Ref. 6) Upon reading the properties of a photon, this fundamental law always proves itself. Two hosts can communicate securely through a fiber optic line by measuring the properties of the photons. If a third party tried to tap the line in between the two hosts, there would be very little success. You cannot read the properties of a photon without destroying the photon. The intrusion would immediately be identified and communications would probably cease until a secure channel could be setup.

Advances in Physical Security

The future of security relies also on the fact of physically protecting your assets. If you had a competitor that would do anything to remove you from the market, all they would have to do is to place a bomb right near your building and set it off. Now there is no more competition! Providing physical security measures would help you to identify unauthorized intrusions and including corporate espionage.

Biometrics is often used but not quite up to speed just yet. Speech recognition needs vast improvements. If someone were to have a cold, the speech recognition software would inaccurately identify a proper employee as an intruder.

Facial recognition systems take key points of someone's face and obtain a positive identification. This is particularly interesting because an intruder wearing a mask would still be seen as an intruder. They would not have the same exact face structure as the legitimate employee. Even though facial recognition is a beneficial technology, there is a slight problem with this implementation. The user's face has to be prerecorded for a proper identification to take place. There are systems today that implement facial recognition but have a high error rate. (Silicon Spin)

In a matter of time iris scans will take over retina scans for a very good reason. Retina scans look for the blood vessels within your eye. If you are under stress, have a lack of sleep or pregnant, the scan would indicate you as an invalid user or intruder. An iris scan will actually scan the color patterns of your eye for a positive identification.

Hand and fingerprint scanners are very well known and have been implemented for years. They take the lines on your fingers and the identifying characteristics of your hand to authenticate. A perfect scan of a finger is taken into question. A fingerprint scanner looks at particular points within the scan and uses statistical analysis to find a match. (Silicon Spin)

Biometrics is an interesting topic and will probably be one of the sole methods of identifying people in the future. If two or more of the biometrics systems above are used the chances of an intrusion are very unlikely.

Detectors and Sensors have been used for years and are very reliable. Motion detectors can be found in many cities to prevent thefts. Motion detectors will scan for large objects that move in a particular area. They can be adjusted so that smaller objects would not cause an alarm to sound. Heat sensors locate any change in temperature within the room. The average human body maintains a temperature in the 90's on the Fahrenheit scale. A heat sensor would pick up an object within the room that does not conform to the current room temperature and sound an alarm. A heat and motion sensor will probably be combined into one unit in the near future, in order to provide a more efficient security system.

Nowadays many devices rely on touch to accomplish a task. Palm pilots rely on little pens that touch a screen interact with the device. There are touch sensitive monitors that allow someone to navigate the Windows operating system using fingers. This could be implemented on certain types of floors made with particular materials. If any weight were to be pressed on one of these floor panels, this abnormality would be recognized and an alarm would sound.

Conclusion

Advances in science and technology will lead to more secure and trusted environments. Having most or all of the future enhancements equipped within your particular set up would reduce the number of security breaches and intrusions. As these types of technological advances spread, imagine the worldwide impact on society. The criminal rate of the world would drop dramatically. It brings to view the futuristic scene portrayed in the movie “Minority Report.” In this movie, Tom Cruise plays an officer who is appointed to stop crimes that have not happened yet. The individual that would have committed the crime is apprehended and thrown in a prison colony. This is mostly science fiction but it brings to the light the endless possibilities when using a one unified system of dealing with social deviance. Privacy may still be an issue but it always is and always will be debated. Only time will tell of the amazing feats the human mind will accomplish.

Works Cited

Cassidy, David. “Heisenberg / Uncertainty Principle”. May 2002 URL: http://www.aip.org/history/heisenberg/ (13 April 2003).

Daemon News. “The BSD Family Tree”. URL: http://www.daemonnews.org/200104/bsd_family.html (11 April 2003).

Kwiat, Paul and Thomas Jennewein, Nicolas Gisin. “Quantum Cryptography”. URL: http://www.aip.org/releases/2000/release03.html (13 April 2003).

Lineback, Nathan. “Windows History”. URL: http://members.fortunecity.com/pcmuseum/windows.htm (9 April 2003).

McClure, Stuart and Joel Scambray, George Kurtz. Hacking Exposed: Network Security Secrets and Solutions, Third Edition. Berkeley, California, Osborne, McGraw-Hill, 2001. 324.

National Security Agency. “Security-Enhanced Linux. URL: http://www.nsa.gov/selinux/index.html (11 April 2003).

OpenBSD. URL: http://www.openbsd.org/security.html (9 April 2003).

Schneier, Bruce. Applied Cryptography, Second Edition. Canada, John Wiley & Sons Inc., 1996.

Silicon Spin. Prod. Dave Roos. TechTV. San Francisco. 10 Jul. 2002.

Garfinkel, Simson and Eugene Spafford. Practical Unix and Internet Security, 2nd Edition.