Global Information Assurance Certification Paper

Information Security and Incident Response for a Computing System: An Overview

By
Ben Lee
July 20, 2004
GSEC – Version 1.4b Option 1

Abstract

Information security is a requirement for all sizes of computer systems. This paper will show an overview of some methods involved in setting up a security system. There are many parts to information security for a system including preventative measures, incident handling and post attack response. Information security during the earlier days of networked systems seemed more of a hassle than an essential process. System administrators constantly struggled between security and usability. Users never like to give up usability for security and their managers, usually non-computer savvy themselves, usually side with their users. Information Technology departments can no longer afford to ignore information security threats. Slowly, with the common place of the Internet in every day life, users are becoming more and more aware of threats and the damage they can do to systems. The balance must be maintained between usability and security, but as systems grow and get more complex, so does securing them.

1. Threats

There are four main security threats to a system: interception, modification, fabrication and interruption. [1]

Interception – This is the most common security threat. Interception is when data has been accessed by an outside source illegally. This can be unauthorized access to a database, coping of files, stealing network packets or even accessing someone's email on their unlocked computer.

Modification – Modification is when data has been changed from it original content. A common modification attack is when a hacker changes the header in an IP packet. Modification can also be done on the hardware side of the computing system. An example of this would be modifying a computer's IP and MAC address to intercept data from its original source.

Fabrication – Fabrication of data would be sending false information to the computing system. A hacker could send false financial information to a company finance department. Another example would be when a

[1] Pfleeger, Richard. Security In Computing. Upper Saddle River, NJ. Prentice-Hall, Inc. 1997. pg. 4

hacker commits identity theft and uses their identity to gain access to credit cards, financial information, medical records, etc.

Interruption – Interruption is when data is lost, stolen or blocked from your computing system. The most notorious computer system interruption is the famous denial of service attack. The best example of this is the SYN flood attack. In a SYN flood, a hacker establishes a connection to your computing system and sends a SYN packet to the system. Your system then sends back a SYN-ACK packet and awaits the return of the ACK packet from the hacker system. This never happens and leaves a half-open connection. This is consuming kernel data structures and, since it's a finite data structure, creates an overflow.[2]

By identifying these threats, you can better protect your data's confidentiality, integrity and availability across your computer system. Threats will always be around and will get more complex as computing systems get more complex. It is the job of the information security officer or department to be able to adapt and handle these threats.

2. Securing the Computing System: Assessments and Policies

How do I secure my system? This is a valid and often asked question in the business world. The more complex the system, the more complex the protection. Also, how do we define "secure"? What level? Is it secure from a casual hacker? Is it secure from a hacker group? Is it secure from cyberterrorism? Each level of security gets more and more expensive. There are many facets to securing an entire computing system. From trusting a system to user education, many security features can be put in place from expensive measures to those of negligible cost.

Threat and Risk Assessment

Before an effective information security mechanism can be designed and implemented, threat modeling and risk assessment must be completed. Threat assessment determines the types of threats to the computing system. Threat assessment is necessary to determine which threats you can protect against and which threats is cost prohibitive to protect against. In a threat assessment, it's best to determine all threats possible and then determine which threats are important to your system. If you're a small business you don't need to worry about information warfare where a government department would. Also, a government department wouldn't have to worry about industrial espionage as a threat as a company would. Risk assessment determines damage each risk could cause in terms of money and amount of incidents per year. This is

[2] CERT. "Denial of Service Attacks" June 4, 2001. URL: http://www.cert.org/tech_tips/denial_of_service.html. (July 10, 2004)

calculated by determining the annual loss expectancy (ALE). [3] ALE is calculated by the cost per incident times the number of incidents per year. If a firewall cost $30,000 to buy, install and configure to protect against a threat that's ALE is $100,000, the firewall is a real bargain. On the other hand, if your main threat is just someone snooping around on the network or stealing a little CPU time and the ALE is about $5,000, having a $30,000 firewall is cost prohibitive. There are almost an infinite number of threats to a computing system so every threat cannot be determined in a threat assessment. New threats appear every day.

> *"Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing."*[4]

Since computing systems change over time, risk and threats assessments must be reevaluated over time to make sure they are still valid and to identify new threats.

Security Policies

Security policies help define security standards to be followed throughout the organization. Good security policies help define basic rules, guidelines, and definitions to help combat security inconsistencies through different departments or organizations. Instituting security ad hoc leaves the entire computing system vulnerable to attack. Information security is like a chain in where it's only as good as its weakest link. With a uniform security policy, the chain links are of equal strength. The best policies are broad enough to be applied to a myriad of different computing systems, yet maintain its strength and easiness to follow. In the case a large company with many departments, it might be necessary for each department to have its on security policy. This is common practice especially in financial and defense companies. Even within that situation, a larger company policy needs to be in place for a foundation for the departments to build on. The first part of a security policy is the scope. This consists of a general overview of the policy and usually discusses the organizations resources, hardware, software and personnel. Also within the scope, the responsibilities are stated for the organizations securing the computing system. The next part of the policy is the roles and responsibilities section. This section defines who and how the security department or officer will handle the 3 major information security requirements: Integrity, confidentiality and accessibility. With integrity, the information needs to be secure from modification, interruption, theft and/or damage. Confidentiality would be to make sure the data is not accessed by unauthorized users or hackers. Lastly, accessibility is to make sure the data is only accessible by authorized users and those users can only access that data in a secure manner.

---

[3] Schneier, Bruce. Secrets and Lies. New York, NY, John Wiley and Sons, Inc. 2000. pg. 301

[4] United State General Accounting Office. "Information Security Risk Assessment". August 1999. URL: http://www.gao.gov/special.pubs/ai99139.pdf. (July 11, 2004)

Once these roles are defined, the policy addresses who will be responsible for implementing the security feature to ensure the computing system is secure as defined by the policy. Mostly, this would be system administrators, network engineers and software engineers. In most cases, the policy explicitly defines what measures are to be taken to secure each segment of the computing system. It is the responsibility of the information security officer or department to make sure the policy is followed throughout the organization, department or company they oversee. If these policies are not enforced throughout the computing system as a whole, it leaves a gap in the defense that can be exploited and severely reduces strength of the security system as a whole. This brings us to the last section of the security policy; the enforcement. Since any section of the computing system that does not conform to the minimums of the security policy can leave the entire computing system open to attack, enforcement must be in place to ensure that all parties described in the policy follow it. These enforcements discuss penalties and disciplinary actions that would be needed. These penalties and disciplinary actions can have a broad range depending on the failure or what losses happened during a security breach. In the case such as a hacker gained access could be handled by a warning by the administrator's manager. On the other hand, if a contamination of a unclassified system by a user putting classified data on a system or loss of data, a much sever repercussion is necessary to ensure something of that magnitude does not occur in the future. Major infractions such as the example above, may even be serious enough for law enforcement to be notified.[5] The policy should also have a section to define user education. One of the best ways to get access to a system is to trick a user into giving up their user id and password. Users need to be educated on the role they play in information security and how serious of a matter it can be. They need to be made aware of how their actions can adversely affect the security of the system. Even something as simple as installing a screen saver can undermine the security of the system. A few years ago, a hacker embedded a virus in a screen saver called Captain Jon. Users thought they were just installing a comic screen saver, but in reality, they were infecting their own computer with a virus.

3. Methods of Defense

Once the security policy is developed, it must be implemented by the responsible parties. The security policy can be seen as the minimum amount of security the company, organization or department would like to have on its computing system. In the defense industry, having unclassified and classified systems within the same organization or department is commonplace. The classified system usually requires a much stronger security policy than an unclassified system to maintain the government's approval of use of classified material on the computing system. Implementing a broad security policy that would cover both computing system equally can be done, but is not wise. Security officers must

[5] University of Florida Office of Information Technology. "IT Security Policy". July 15, 2003. URL: http://www.it.ufl.edu/policies/security. (July 11, 2004)

maintain a balance between security and usability. Classified systems are usually small which in turn has a smaller user base. Due to the nature of work these users do, they understand the need for such strong information security. It's a better idea to develop another security policy that covers, at minimum, the requirements set forth by the government of the nation the organization is working for or with. All security policies, no matter how evolved, have mostly the same security measures.

Passwords

Passwords are a very important part in any security policy. A good password can stop attackers from gaining access to the computing system. If a hacker can crack one users password and gains access to their workstation, the whole computing system can be compromised. Good passwords are more important than users think. In today's computing world, users have passwords for just about major computing item they have to access. This is both good and bad. Good because each part of the system they access has password protections in place. The bad part is that most users hate trying to remember all those passwords. Most users do one of two things. They will either write down their passwords on their desk or just use the same password for all systems. Either method is a hacker's delight, especially the same password method. If a hacker cracks that one password, they have access and rights to everything that user had access and rights to on the system. This is a good test that tiger teams try in order to gain access to a system. Tiger teams are a group of "good" hackers, usually from within your company's information security department that can test the security of the computing system. A good password is one that cannot be cracked or guess by any attempts by a hacker. Dictionary password crackers are commonplace tools for the hacker today. A good dictionary password cracker can crack passwords with words in a dictionary in less than a minute. Another method is brute force attacks. In this attack, a hacker attempt, as many times as it takes, to login into the system with the user's id and tries a myriad of passwords that are usually put in a large list the hacker has to try to guess the correct passwords. This method has really been dropped by hackers because so many systems, especially UNIX systems, have account lockouts in place where the users account is locked out after 3 unsuccessful login attempts. Good passwords are probably the cheapest security feature for a computing system. All that is required are password restrictions and user compliance. Password restrictions can be set up on the computing systems servers. Depending on the operating system, passwords restrictions can be setup by third party software or by the operating system itself. In UNIX, there are files that can be edited to institute password restrictions globally. In most UNIX derivatives, these files are in the /etc/default or /etc/security folders. Below are some of the settings that can be defined. For this example, these are the setting for AIX[6]:

[6] IBM. "User file". April 26, 2004. URL: http://publib16.boulder.ibm.com/pseries/en_US/files/aixfiles/user.htm. July 18, 2004.

maxage - Defines the maximum age (in weeks) of a password. The password must be changed by this time. The value is a decimal integer string. The default is a value of 0, indicating no maximum age.

maxexpired - Defines the maximum time (in weeks) beyond the maxage value that a user can change an expired password. After this defined time, only an administrative user can change the password. The value is a decimal integer string. The default is -1, indicating no restriction is set. If the maxexpired attribute is 0, the password expires when the maxage value is met. If the maxage attribute is 0, the maxexpired attribute is ignored.

maxrepeats - Defines the maximum number of times a character can be repeated in a new password. Since a value of 0 is meaningless, the default value of 8 indicates that there is no maximum number. The value is a decimal integer string.

minage - Defines the minimum age (in weeks) a password must be before it can be changed. The value is a decimal integer string. The default is a value of 0, indicating no minimum age.

minalpha - Defines the minimum number of alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number.

mindiff - Defines the minimum number of characters required in a new password that were not in the old password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number.

minlen - Defines the minimum length of a password. The value is a decimal integer string. The default is a value of 0, indicating no minimum length. The maximum value allowed is 8. This attribute is determined by the minalpha attribute value added to the minother attribute value. If the sum of these values is greater than the minlen attribute value, the minimum length is set to the result.

minother - Defines the minimum number of non-alphabetic characters that must be in a new password. The value is a decimal integer string. The default is a value of 0, indicating no minimum number.

pwdchecks - Defines the password restriction methods enforced on new passwords. The value is a list of comma-separated method names and is evaluated from left to right. A method name is either an absolute path name or a path name relative to /usr/lib of an executable load module.

pwdwarntime - Defines the number of days before the system issues a warning that a password change is required. The value is a decimal integer string. A zero or negative value indicates that no message is issued. The value must be less than the difference of the maxage and minage attributes. Values greater than this difference are ignored, and a message is issued when the minage value is reached.

These files are maintain and only accessible by the system administrator. With these files properly set up, password administration is automated. Determining what makes a good password, is necessary for properly setting up password restrictions, but how do you determine what makes up a good password? A good password will use a combination of letters, numbers and symbols. Using letters and numbers, that can be 36 different combinations. If you require or use capitals, the combination is up to 58. With symbols, that raises it even further to 92.[7] Using all of these together creates over a trillion different possible passwords. This could take decades to crack. Password length is also of great importance. As the minimum length is increased, the combinations rise exponentially.

Another good password restriction is making the user change their password after so many days or months. You want users to change their password frequently to reduce the risk of passwords being compromised. The industry standard is usually 90 days. This is a good median because any more increase the risk of a compromise and any less create other security risks like users writing down passwords. Restricting the amount of characters that can be repeated in the new password is also a good measure. It enforces the user to make a more unique password from the one they were using. Two more restriction to enforce good passwords are password history and password minimum age. These two work hand in hand. The password history forces the user to make unique password each time. With this enabled, users cannot reuse their passwords over and over again. The password minimum age makes the user keep their change password for a specific period of time. This is good to ensure the user does not recycle back to their old password. One item that is constantly overlooked is system accounts. These accounts are installed by either the operating system or by software installed on the computing system. Some of these accounts do not have login privileges, but those that do are usually installed with a default password. With all the other task system administrators are required to do, this is an often overlooked vulnerability. These accounts must have their passwords change, and if possible, adhere to the password restrictions themselves. Most of the time, this cannot be done without interfering with the roles these accounts do in the operating system or software. In that case, close monitoring of these accounts are required.

[7] SearchSecurity.com. "Testing password strength give policy some bite." October 23, 2002. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html. July 18, 2004

Auditing

Having a good audit trail is a good way check the security health of your system. A good audit trail can give a security officer a wealth of knowledge. Some operating systems, like HP-UX, have auditing tools built into the operating system. In HP-UX, auditing can only be enabled on a trusted system. Trusting the system enables the auditing functions, shadows the password file and creates the trusted computing base. Once the system is trusted, auditing can be enabled on the system. Auditing can be enabled per event or per system call. These events and calls are ones that are not self-auditing like passwd and login. Each event and call can be setup to audit success and/or failures depending on the requirements of the security policy. Once auditing is enabled, each success and/or failure is then logged by they system. In the case of a HP-UX system, only ROOT can view these files by running the AUDISP command. With this command, the administrator can select what items in the audit log they would like to see. The command has many flags to give the administrator flexibility in auditing. AUDISP's syntax starts with success or failure, start time, end time and audit file. An example of this is below:

Audisp –f –t 07040000 –s 07042359 audfile1

Setting up auditing correctly is a major step. Otherwise, the administrator is flooded with excess information that can be completely overwhelming. Some good guidelines for proper auditing are below from Hewlett-Packard[8]:

- Check the audit logs at least once per day. Keep the online auditing file for at least 24 hours. Keep all auditing records stored offline for at least 30 days.
- Review the audit log for unusual activities such as late night logins, login failures, failed access to files, or failed attempts to perform security-relevant tasks such as changing file permissions or ACLs.
- Archive the audit file everyday to prevent it from overflowing (and potential loss of auditing data).
- Revise the events that are audited periodically.
- Change the audited users periodically.
- Do not follow any pattern or schedule for event or user selection.
- Specify site guidelines. Involve users and management in determining these guidelines.
- Ensure the physical security of systems and disks containing the audit logs, backups of these logs, and printouts of these logs.

[8] Hewlett-Packard. "Administrating you HP-UX Trusted System". August 1996. URL: http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90121/B2355-90121_top.html&con=/hpux/onlinedocs/B2355-90121/00/00/37-con.html&toc=/hpux/onlinedocs/B2355-90121/00/00/37-toc.html&searchterms=ID|audit&queryid=20040708-012405. July 20, 2004

- Provide a backup power source (UPS) for the disks containing the audit log so the data are not lost in the event of power failure.
- Provide disk mirroring and other high availability support for the audit log disks.

Intrusion Detection System

Intrusion detection systems are usually software programs that detect unauthorized attempts to gain access to the network. These are put between both the server and the firewall or outside the firewall. Depending on where these are setup, they can detect anything from port scanning to buffer overflow attacks. Intrusion detection systems can detect either anomalous or pattern intrusions. Anomalous intrusions tracks changes in the system from the normal patterns like a network traffic spike, high CPU utilization or network traffic from an unknown IP. This method is good for because it covers a broad range of areas to monitor. Pattern detection is where IDS looks for patterns of a well know intrusion attacks. There are many software vendors that make pattern intrusion detection systems.[9] Intrusion detection systems are great for handling the hacker threat before the hacker can get in the computing system and do damage.

Physical Security

Physical security can as simple or as elaborate as the organization or department would like depending on how much they want to spend. It can be as simple as a lock on the door to biometrics and smart cards. Most corporations only allow authorized individuals in the rooms that house the servers or networking equipment. Most use discretionary access to determine who has physical access to equipment. For instance, network administrators do not need access to the servers and system administrators do not need access to wiring collects. Security officers need access to all. This, of course, depends on the size of the organization. In smaller business, the security officer, system administrator and network engineer are the same person. At the very minimum, servers and network equipment should be behind locked doors with only the administrators and their managers have keys to those areas. The problem with using locks is that they require keys which can be easily lost, stolen or copied allowing unauthorized access. Another technology that is used instead of key locks are key pads. With key pads, no keys are required. The key pad uses a determined amount of digits to set its access code. When the access code is correctly input in the key pad, the door unlocks for a certain amount of time. This is to ensure that someone cannot unlock the door and have someone sneak in behind them. The codes can be given out to authorized personal and cannot be lost or copied. The drawback is that they can be easily intercepted by watching someone input the code to the key pad, over hearing the code be given to

[9] Graham, Robert. "FAQ: Network Intrusion Detection Systems" March 21, 2000. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html. July 20, 2004

someone or by lax administrators giving the code out. Still, this method is flawed also. Next, we have card readers and smart cards. Using these makes it much harder to gain access to secure areas. The card reader allows access when the employee swipes their card through the reader, the reader determines if that card carries the correct rights to gain access to that area. Smart cards act in much the same way. In a smart card, the card carries with a small computer chip that is complete self-contained in the card.[10] Smart cards can contain the full data of the user and any access they need. Smart cards are terribly difficult to hack. Hacking smart card, as of now, is very time consuming and expensive. The advantages of using cards is that these cards can give access to numerous areas, can be tracked easily and access can be easily revoked or given to users. The main problem with using cards, especially with large corporations is that it is an expensive technology.[11]

Biometrics is another technology that is gaining a good following. These are very difficult, if not almost impossible, to defeat. With biometrics, a user must present the security system with a physical characteristic to gain access to the area. Some of the physical characteristics that can be used are the eyes, face, fingerprint or voice. These are almost impossible to duplicate. Biometric systems use a scoring meter to determine if the biometric for the person matches users in their database. A threshold can be set for the score determine if the score is high enough to allow access. If the score is below the threshold, the user is not allowed access. The main draw back to biometric is the cost.[12] Biometric are extremely costly right now and are normal only used in areas where very high security is needed.

4. Incident Response

You've been hacked. Now what? This area of information security is often the most neglected. Companies loose millions of dollars to hackers yearly and will spend millions to prevent hackers from getting access, but they often do not train or inform their systems administrators on the proper procedures for incident handling. This area has grown rapidly in the information security industry into its own specialty called computer forensics. Computer forensics is the methodology of gathering, identifying and documenting data after an attack. Incident response is a complex task. It requires constant monitoring of the system with intrusion detection systems, log monitoring and a good relationship with other internal departments within the company. When incidents occur, it must be treated like a

[10] Chan, Charles. "An Overview of Smart Card Security". August 19, 1997. URL: http://home.hkstar.com/~alanchan/papers/smartCardSecurity/. July 20, 2004
[11] InformIT. "General Design Considerations for Secure Networks". June 18, 2004. URL: http://www.informit.com/articles/article.asp?p=174313. July 21, 2004
[12] Department of Defense. "Biometrics 101". March 2004. URL: http://www.biometricscatalog.org/biometrics/Biometrics_101_v5.pdf. July 23, 2004.

crime scene since, in most cases, it can be a true crime scene. Since computers have become common place in today's society, laws have been passed by many of the world's governments making many computer intrusions and hacking crimes. The chain of evidence must be preserve since it could be required to be presented in a court of law. You want ensure that, once the incident happens and has been identified, the data cannot be overwritten or corrupted. The best way to do this is to gather the information on a secure disk and write protect it. Once it is gathered, it can be examine a secure system with a known good configuration.[13] You want to make sure the whole collection of the evidence is well documented in case it has to be presented in court. This can show there was no tampering of the evidence while it was being gathered. There are several ways to find out who hacked your computing system. If the logs are intact, you can possibly get the suspect's IP. With that, you can do a TRACEROUTE to determine where the computer is located. The only problem with doing that is that you can alert the hacker that you are tracking them. The system administrator can also use NSLOOKUP to do a reverse DNS to find out information about the hackers system if they have registered their domain. If that comes back with some positive information, they administrator can then us WHOIS to get the hackers personal information since this is required when registering the domain name. All of this should be tracked and log to put with the chain of evidence. Through this whole process, management, security and human resources should be kept up to date during each step. Once any data loss is identified, law enforcement should be immediately notified especially in the cases of national security. Once they have been notified, they will take over the investigation. It is also a good idea to report incidents to other security organizations like CERT and SANS. The organizations can then notify others in the information security community this exploit so they can safeguard against them.

Summary

Information security is an ever evolving fielding. It has come a long way from the days of when information security was just thought of as a password to login into a system. With a clear, easy to follow security policy, a company can effective secure their computing systems from hackers. Users are becoming more and more educated on information security from either their workplace or dealing with threats at home from the internet. This puts a little less burden on the system administrators, but their role is the most important. Auditing them can help determine if a hacker has infiltrated the system and how they did it. Once they have identified the threat, proper procedures can be followed to gather data to help the proper authorities determine the correct course of action. User, management and system administrators must work together to ensure the security of the computing system.

[13] Kruse, Warren G and Heiser, Jay G.. Computer Forensics – Incident Response Essentials. New York, NY, Addison-Wesley, Inc. 2002. pg. 7

References

[1] Pfleeger, Richard. Security In Computing. Upper Saddle River, NJ. Prentice-Hall, Inc. 1997. pg. 4

[2] CERT. "Denial of Service Attacks" June 4, 2001. URL: http://www.cert.org/tech_tips/denial_of_service.html. (July 10, 2004)

[3] Schneier, Bruce. Secrets and Lies. New York, NY, John Wiley and Sons, Inc. 2000. pg. 301

[4] United State General Accounting Office. "Information Security Risk Assessment". August 1999. URL: http://www.gao.gov/special.pubs/ai99139.pdf. (July 11, 2004)

[5] University of Florida Office of Information Technology. "IT Security Policy". July 15, 2003. URL: http://www.it.ufl.edu/policies/security. (July 11, 2004)

[6] IBM. "User file". April 26, 2004. URL: http://publib16.boulder.ibm.com/pseries/en_US/files/aixfiles/user.htm. July 18, 2004.

[7] SearchSecurity.com. "Testing password strength give policy some bite." October 23, 2002. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html. July 18, 2004

[8] Hewlett-Packard. "Administrating you HP-UX Trusted System". August 1996. URL: http://docs.hp.com/cgi-bin/fsearch/framedisplay?top=/hpux/onlinedocs/B2355-90121/B2355-90121_top.html&con=/hpux/onlinedocs/B2355-90121/00/00/37-con.html&toc=/hpux/onlinedocs/B2355-90121/00/00/37-toc.html&searchterms=ID|audit&queryid=20040708-012405. July 20, 2004

[9] Graham, Robert. "FAQ: Network Intrusion Detection Systems" March 21, 2000. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html. July 20, 2004

[10] Chan, Charles. "An Overview of Smart Card Security". August 19, 1997. URL: http://home.hkstar.com/~alanchan/papers/smartCardSecurity/. July 20, 2004

[1] InformIT. "General Design Considerations for Secure Networks". June 18, 2004. URL: http://www.informit.com/articles/article.asp?p=174313. July 21, 2004

[11] Department of Defense. "Biometrics 101". March 2004. URL: http://www.biometricscatalog.org/biometrics/Biometrics_101_v5.pdf. July 23, 2004.

[12] Kruse, Warren G and Heiser, Jay G.. Computer Forensics – Incident Response Essentials. New York, NY, Addison-Wesley, Inc. 2002. pg. 7