GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Unauthorized Access – Threats, Risk, and Control

By Dicky Hau

GSEC Practical Assignment, Version 1.4b, Option 1
July 11, 2003

ABSTRACT

Computer technology has transformed the way people learn, work, and play. Computers have become an integral part of our everyday existence. They are used to store and to send personal letters, bank transactions, and highly sensitive military documents. In today's competitive world, every business is "forced" to improve its efficiency and productivity in order to stay ahead of the competition or simply to stay in business. Computer networking technologies - intranet, extranet, internet - have advanced to the point where information can be stored, transmitted, and available to people accessing and conducting their business anytime and from anywhere. Internet-based technologies integrate corporate applications, knowledge management applications, decision support systems, internet search and repository, and external third party systems such as suppliers, customers (e-commerce), and business partners (e-business). With all the capabilities offered by computer, networking, and internet technologies an organization gains many benefits, including rapid access to information, more functionality for users, improved customer services, reduced costs, and increased visibility in the internet world. These benefits also push companies into implementing internet-based technology without considering the security threats that this entails.

A company's proprietary information about products, processes, customers, and suppliers is a critical business asset to its daily operations and survival. The most common threat in a networked system is unauthorized access to information and computer resources (information technology system). This may cause the loss of confidentiality, integrity, and availability of the information technology assets. To ensure business continuity and minimize potential damage, companies need to establish a computer-based access control (so-called logical access control) to protect their proprietary information from intentional or accidental disclosure, modification, erasure, or copying, as well as their IT resources from misuse. This control provides an organization with the ability to restrict, monitor, and protect the confidentiality, integrity, and availability of these resources.

ACCESS THREATS AND RISKS

Internal Threats

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Internal threats are from individuals that have legitimate access such as employees, students, and contractors. Insiders can be extremely difficult to detect or to protect against because they have legitimate access to the system, know what to look for, and most likely know how to circumvent intrusion detection systems. They can misuse the company's IT resources to:

- perform port scans on outside systems and initiate attacks from inside the company.
- access, process, and distribute pornography materials.
- access unauthorized information (salary, secret trade).
- spread SPAM, SCAM, and/or malicious code.
- implement unauthorized changes to data or programs or steal data files for personal gain.
- visit illegal download sites.
- install illegal software into their computer (copyright infringement).

Passwords are an important line of defense against unauthorized access to an IT system. When employees share their password or leave their computer unprotected; it provides opportunities for unauthorized users.

External Threats

Outside intruders can be hackers/crackers, saboteurs and thieves. If the network is compromised, intruders can attack or misuse the system.

One common technique used by intruders to gain unauthorized access to the system is password theft. The intruder obtains the password of an authorized users' account by:

- finding a sticky note with the password written on it; often stuck on the monitor or hidden under a keyboard,
- going through garbage to find discarded documentation that may contain passwords (dumpster diving),
- running a password-cracking application to figure out passwords that are stored in plain text from users accounts. This application can figure out a weak password in a matter of seconds. The program works with the same speed or even faster than the spelling check feature worked in a word processor. Types of attack are:
  - dictionary attack: compare passwords against dictionary files until the match is found,
  - hybrid attack: use a dictionary attack with a check for extra characters attached to either end of the word,
  - brute force attack: compare every possible combination and permutation of characters available until the match is found. It is used for passwords that are very complex and difficult to guess.

Other access techniques include:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Sniffing/wiretapping/eavesdropping on network traffic: place a device or program to intercept or monitor packets sent over the network. As a result, sensitive information such as passwords and trade secrets can be captured.
- Exploiting security weaknesses: use vulnerability assessment tools to probe network systems, then exploiting identified vulnerabilities to gain access to or to break-in to the system.
- Internet Protocol (IP) spoofing: a system is configured to impersonate another system's IP address in an attempt to gain access to the targeted system.
- Social engineering: intruders trick legitimate users into disclosing information they want. The information can be confidential or sensitive information. They prey on qualities of human nature such as a desire to be helpful, a tendency to trust people, or fear of getting in trouble.

Once the intruders gain access to the internal network, they can approach, trespass within, communicate with, store data in or retrieve data from, interfere with, or otherwise intercept and change the system. They can:

- Obstruct computer services by placing malicious programs to overload computer resources. This could result in filling up hard drive storage space, sending messages to reset a host's subnet mask, using up all of the computer resources to accept network connections. Common techniques include SYN attack, and teardrop attack.
- Use the system as a stepping-stone to invade other systems (distributed denial of services, DDoS), or relay of viruses, worms, or SPAM.
- Install malicious programs (such as viruses) to destroy or modify files.
- Insert an undetectable program (such as Trojan horse) into an authorized application used to transfer money (theft of money) or send trade secrets/credit card numbers to remote servers (theft of information).
- Place a backdoor that enables attackers to come back to the system at a later date, bypassing the usual security authentication and authorization steps.

Risks

Risks from these threats include:

1. Unauthorized disclosure of information: disclosure of confidential, sensitive or embarrassing information can result in loss of credibility, reputation, market share, and competitive edge.
2. Disruption of computer services: be unable to access resources when they are needed can cause a loss of productivity. Disruption of services during critical processing time may be disastrous.
3. Loss of productivity: misuse of IT resources such as network bandwidth may cause slow response times, delaying legitimate computer activities that, in time-critical applications such as stock trading, can be very costly.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4. Financial loss: the losses can be directly from the theft of money or indirectly from the recovery of security incidents such as corruption of information or disruption of services.
5. Legal implications: security or privacy breaches can expose a company to lawsuits from investors, customers, or the public.
6. Blackmail: intruders can extort money from the company by threatening to exploit the security breach.

Most of the security threats and risks to an organization are the result of inadequate and improper access control. Poor access control can expose the organization to unauthorized access of data and programs, fraud, or the shutdown of computer services. External threats become more important as the company's network extends to suppliers, customers and partners. Even authorized users can be a risk if not controlled properly.

LOGICAL ACCESS CONTROLS

Logical access control is one of the safeguards used to prevent unauthorized access to an organization's sensitive or critical information and to minimize the impact to an organization from security breaches. Not only can it control who or what is to have access to a specific system resource, but also the type of permitted access. This control can be incorporated into software such as operating systems, data base management systems, applications or implemented into external devices such as routers.

Effective logical access control starts with defining system-specific security policies that clearly and concisely state what protection mechanisms are to be enforced in order to achieve security requirements for a system. Thus the security policies are formalized by security models and implemented by security mechanisms providing access controls that minimize both internal and external threats.

Security Policy

> "The security policy is a statement of intent with regard to control over access to, dissemination of, and modification of information. The security policy must be precisely defined and implemented for each system that is used to process sensitive information. The security policy must accurately reflect the laws, regulations, and general policies from which it is derived." (Jordan, p. 6).

The policy states a set of rules that regulate who (a subject) can access a specific resource (an object) in an IT system and what the subject can do (type of access) based on the security label of the subject and object. The control can be

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

implemented internally to a computer system (operating system, application programs) or in external devices (routers).

Many people think of a user as a subject and a file as an object. A subject (a user, program, or process) is an "active" entity that requests access to an object. An object is a "passive" entity to be accessed and can be a file, a storage device, database, network, or printer. The roles of the subject and object depend on the situation. For example, a process requests access to a database (act as an object) to accomplish a task, then the database (now acting as a subject) is requested by a program to accomplish another task.

Types of access include the ability to read, write, delete, execute, append, and copy.

A security label is used to determine if the access is authorized based on the defined rules in the policy. Every subject and object has a security label associated with its sensitivity level. A label for a subject is called a clearance while the label for an object is called a classification. Examples of security labels used in the military and their order are: top secret > secret > confidential > restricted > unclassified. In a private organization, it might be proprietary > sensitive > confidential > public.

Security Models

Security policies describe rules about who is allowed to do what. A security model is used to formalize the policy. The model shows how the system will address the security requirements and determine the consequence of building the system. The model should be precise and easy to understand. There are three types of security model:

1. Access Control Model: supports confidentiality, accountability, and integrity policies.
2. Information Flow Model: supports confidentiality policy.
3. Integrity Model: supports integrity policy.

1. <u>Access Control Model</u>

An Access Control Model defines rules that dictate how subjects access objects. It provides confidentiality, integrity and also provides accountability. There are three main types: discretionary, mandatory, and role-based (also called non-discretionary).

Discretionary Access Control (DAC) enables a subject, at its discretion, to specify what type of access can occur to the object it owns. The most common approach to implementing this model is through access control lists (ACL). The access can be dictated by the identification of subject and object (identity-based), by user (user-directed) with certain restrictions, or

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

hybrid (combination of the both). This model is commonly used in commercial and industrial environments because of its flexibility to change access types over a short period.

Mandatory Access Control (MAC) determines access based on the security label, not the identity, of the subject (clearance) and object (classification). It is a rule-based access control. The administrator (not owner) sets rules to control who can access which objects and make changes to the security level of a resource. The users cannot modify these rules. As this model is much more structured and strict on rules, it works well in an environment with rigid information access restrictions – like the military, or a hospital.

Role-Based Access Control (RBAC), also called Non-Discretionary Access Control, is centrally administered through authorized decisions based on an individual's role within an organization (e.g. physician, nurses, patient care unit manager, admitting clerk, etc. in a hospital model). Access types are grouped by role name and the use of resources is restricted by the subject's assigned role. The administrator grants and/or revokes system privileges based on a subject's role. This model works well for organizations with a large turnover of personnel.

2. Information Flow Model

This model addresses both the information flow direction and security levels to ensure the confidentiality of information. It forbids the flow of higher security level information down to a lower security level. The Bell and La Padula (BLP) model is an example of this model. The BLP uses security levels to determine appropriate access rights based on the defined rules as follows:

- For read permission: subjects at a higher level can read to the objects with a level that is either equal to or lower (no read-up).
- For write permission: subjects at a lower level can "write-up" to objects with a level that is either equal to or higher (no write down).

Only the administrator can make changes to a resource's security label. This model preserves confidentiality, but not integrity.

3. Integrity Model

This model is used to preserve the data integrity but not secrecy. Examples of this model are the Biba Model and the Clark-Wilson.

The Biba Model is a modification of the BLP Model, with an emphasis on data integrity. Its access rules are:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- For read permission: subjects can read objects only if the integrity level of the subject is either higher than or equal to the integrity of the object (no read-down).
- For write permission: subjects can write objects if the integrity level of the subject is either equal to or lower than the integrity of the object (no write-up).

The Clark-Wilson model is used to address security requirements in commercial applications (deals with input, alteration, and tracking of data). This model uses two mechanisms to enforce the integrity for both internal and external consistency. These mechanisms are:

- Well-formed transactions: data accessed only by specific programs, no direct access.
- Separation of duties: users must collaborate to manipulate data, requiring more than one person to violate security policies.

Not all information requires the same type of protection. Each of the above models is associated with one or more of the properties of information security policy. An organization needs to identify the security requirements for its IT resources and then determine the most appropriate model to meet its needs.

Logical Access Control Mechanisms

These mechanisms are used to implement and enforce security policies and are intended to counter internal and external threats. Some of the mechanisms are passwords, access control lists (ACLs), encryption, and secure gateways/firewalls.

Passwords are an integral part of overall security and the first line of defense against unauthorized access to IT systems. They are often targeted because more than half of typical users have a weak password. Therefore, a company needs to establish a strong password policy that states how it is to be implemented, administered, and enforced. The policy defines the rules of expiration frequency, character length, password composition, invalid login attempts, and password history, etc. To ensure compliance with the policy, the company can periodically:

- run a scan program against password files for weak passwords and advise users to select a stronger password.
- examine workspaces for passwords attached to keyboards or monitors.

Network users are also required to be:

- trained on how to protect and select a stronger password.
- aware of “social engineering”.

Access Control Lists (ACL’s) are a register of subjects that are permitted specific types of access to objects. Typical access types are read, write, execute, append, modify, create, and delete. Microsoft Windows NT/2000, Unix-based

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

systems are among the operating systems that use ACL's to determine the denial or permission of access to objects.

Encryption transforms data from plain-text into cipher-text (unreadable text). It is one of the defenses against network sniffing and abuse of privilege attacks because only the appropriate secret key can decrypt the information. It is used to provide confidentiality and integrity protection. It is especially useful when strong physical access controls cannot be provided, such as for laptops, mobile storage devices, Personal Digital Assistants (PDA), or wireless communication. Any sensitive information transmitted over public networks should be encrypted in order to prevent intentional and accidental unauthorized disclosure. To prevent abuse of privilege attacks by insiders, encryption may be used on extremely sensitive information while it is transmitted or stored inside the company's network.

Secure gateway/firewall is a system, or group of systems, that enforces an access control policy. It is used to prevent unwanted and unauthorized communication into or out of a network. A firewall can examine all traffic entering or leaving the private network and can block that which does not meet the rules defined in the policy. Companies use firewalls to protect unauthorized access from external network communications via telephone or internet. They can also be used to control insiders' access to illegal websites or unauthorized services such as electronic 'chat', instant messaging, or streaming audio/video. Most companies block these types of services because an intruder can use them as tools for a system attack.

CONCLUSION

Companies are increasingly dependent on computer/network technology for improving the efficiency and productivity of their business in order to survive and thrive in today's competitive world. It is a business need and sometimes is a legal requirement to protect their proprietary information against the threats of unauthorized disclosure, modification, and destruction, computer fraud, and service disruption. Companies may suffer financial and productivity losses, as well as loss of reputation due to extensive internal and/or external security threats. A properly implemented logical access control provides for the safeguarding of assets against threats, ensures business continuity, minimizes potential damages, and maximizes return on investment.

Strong logical access control includes sound security policies, clearly defined security models, well-designed system architecture, proper implementation of security mechanisms such as passwords, encryption, access control lists, and firewalls. Access to information should be governed by the need-to-know principle. Only with the properly designed and implemented logical access control will companies be able to realize the benefits and potential of computer

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

technology. This will give their business the edge over their competitors to avoid being the next victim of security threats.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

REFERENCES:

Aspinall, David. "Security Models." Computer Security Lecture 9." 6 February 2003..
URL: http://www.dcs.ed.ac.uk/home/compsec/lecs/secmods.pdf

Cmpe 471. "Computer Crime: Techniques and Countermeasures."
URL: www.cmpe.boun.edu.tr/courses/cmpe471/fall2001/download/cmpe471-compcrime.ppt

Belanger, Dr. France. "Chapter 2 – Access Control and Site Security." ACIS5584 E-Commerce Security.
URL: http://www.cob.vt.edu/accounting/faculty/belanger/sec/5584_week2.pdf

Emin Gun Sirer. "Security Models."
URL: www.cs.cornell.edu/courses/cs414/2002SP/lectures/35-secmodels.pdf

Hlinovsky, Jan. "Access Control and Security Models." T-110.402.
URL: www.tml.hut.fi/Opinnot/T-110.402/2002/Luennot/titu20021023.pdf

Jordan, Carole S. "A Guide to Understanding Discretionary Access Control in Trusted Systems." NCSC-TG-003 Version-1. 30 September 1987.
URL: http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-003.pdf.

Krause, Kicki and Tipton, Harold F. "Handbook of Information Security Management."
URL: http://www.cccure.org/Documents/HISM/ewtoc.html

"Logical Access Controls – Session 9." IT Audit Training for INTOSAI. October 1997.
URL: http://www.nao.gov.uk/intosai/edp/sessio9.pdf

Olovsson, Tomas. "A Structured Approach to Computer Security." Technical Report No. 122, 1992. Department of Computer Engineering, Chalmers University of Technology, S-412 96 Gotherburg, Sweden.
URL: http://www.ce.chalmers.se/staff/ulfl/pubs/tr122to.pdf

Rothke, Ben. "Access Control Systems and Methodology." New York Metro eSecurity Solutions Group 732/516-4242 EY/COMM 6027684.
URL: http://www.cccure.org/Documents/Ben_Rothke/Access%20Control.ppt

Vigano, Luca. "Access Control II: Security Models."
URL: www.informatik.uni-freiburg.de/~softech/teaching/ws02/itsec/material/slides-accesscontrol2-171202.pdf

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: August 23rd, 2020

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Virginia Beach 2020 - Live Online	Virginia Beach, VA	Aug 30, 2020 - Sep 04, 2020	CyberCon
SANS Virginia Beach 2020	Virginia Beach, VA	Aug 30, 2020 - Sep 04, 2020	Live Event
SANS London September 2020 - Live Online	London, United Kingdom	Sep 07, 2020 - Sep 12, 2020	CyberCon
SANS Baltimore Fall 2020	Baltimore, MD	Sep 08, 2020 - Sep 13, 2020	CyberCon
SANS Munich September 2020	Munich, Germany	Sep 14, 2020 - Sep 19, 2020	Live Event
SANS Munich September 2020 - Live Online	Munich, Germany	Sep 14, 2020 - Sep 19, 2020	CyberCon
SANS Network Security 2020	Las Vegas, NV	Sep 20, 2020 - Sep 25, 2020	CyberCon
SANS Australia Spring 2020 - Live Online	, Australia	Sep 21, 2020 - Oct 03, 2020	CyberCon
SANS Australia Spring 2020	, Australia	Sep 21, 2020 - Oct 03, 2020	Live Event
SANS Northern VA - Reston Fall 2020	Reston, VA	Sep 28, 2020 - Oct 03, 2020	CyberCon
SANS Amsterdam October 2020	Amsterdam, Netherlands	Oct 05, 2020 - Oct 10, 2020	Live Event
SANS Amsterdam October 2020 - Live Online	Amsterdam, Netherlands	Oct 05, 2020 - Oct 10, 2020	CyberCon
SANS Cyber Defense Forum & Training	Virtual - US Central,	Oct 09, 2020 - Oct 17, 2020	CyberCon
SANS Orlando 2020	Orlando, FL	Oct 12, 2020 - Oct 17, 2020	CyberCon
SANS October Singapore 2020 - Live Online	Singapore, Singapore	Oct 12, 2020 - Oct 24, 2020	CyberCon
SANS October Singapore 2020	Singapore, Singapore	Oct 12, 2020 - Oct 24, 2020	Live Event
SANS Riyadh October 2020	Riyadh, Kingdom Of Saudi Arabia	Oct 17, 2020 - Oct 22, 2020	Live Event
SANS Riyadh October 2020 - Live Online	Riyadh, Kingdom Of Saudi Arabia	Oct 17, 2020 - Oct 22, 2020	CyberCon
SANS Dallas Fall 2020	Dallas, TX	Oct 19, 2020 - Oct 24, 2020	Live Event
SANS Dallas Fall 2020 - Live Online	Dallas, TX	Oct 19, 2020 - Oct 24, 2020	CyberCon
SANS San Francisco Fall 2020	San Francisco, CA	Oct 26, 2020 - Oct 31, 2020	CyberCon
Instructor-Led Training | Oct 26 ET	,	Oct 26, 2020 - Oct 31, 2020	CyberCon
SANS Sydney 2020	Sydney, Australia	Nov 02, 2020 - Nov 14, 2020	Live Event
SANS Rocky Mountain Fall 2020	Denver, CO	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS London November 2020 - Live Online	London, United Kingdom	Nov 02, 2020 - Nov 07, 2020	CyberCon
SANS Sydney 2020 - Live Online	Sydney, Australia	Nov 02, 2020 - Nov 14, 2020	CyberCon
SANS London November 2020	London, United Kingdom	Nov 02, 2020 - Nov 07, 2020	Live Event
South by Southeast Asia Nov 2020	, Singapore	Nov 02, 2020 - Nov 14, 2020	CyberCon
SANS Paris November 2020	Paris, France	Nov 02, 2020 - Nov 07, 2020	Live Event
SANS Rocky Mountain Fall 2020 - Live Online	Denver, CO	Nov 02, 2020 - Nov 07, 2020	CyberCon
SANS Paris November 2020 - Live Online	Paris, France	Nov 02, 2020 - Nov 07, 2020	CyberCon