SOFTWARE CONTROL SERVICES (PTY) LTD

475 King's Highway, Lynnwood
P.O.Box 36675, Menlo Park
Pretoria, South Africa
0102

(t) +27 12 348 7301
(f) +27 12 348 1129
(e) techsupport@softconserv.com
www.softconserv.com

Logical Security.

Version 0. 1

Prepared by: Michael Davis- Hannibal

Softcon Software Control Services (Pty) Ltd.

7 March 2017

Revision History

Name	Date	Reason For Changes	Version
MDH	22-Oct-10	Initial document	0.1

Contents

1. General

Logical Security consists of software safeguards for an organization's systems, including user identification and password access, authentication, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.

2. Elements of logical security

Elements of logical security include:

- User IDs, also known as logins, user names, logons or accounts, are unique personal identifiers for agents of a computer program or network that is accessible by more than one agent. These identifiers are based on short strings of alphanumeric characters, and are either assigned or chosen by the users.
- Authentication is the process used by a computer program, computer, or network to attempt to confirm the identity of a user. Blind credentials (anonymous users) have no identity, but are allowed to enter the system. The confirmation of identities is essential to the concept of access control, which gives access to the authorized and excludes the unauthorized.
- Biometrics authentication is the measuring of a user's physiological or behavioural features to attempt to confirm his/her identity. Physiological aspects that are used include fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements. Behavioural aspects that are used include signature recognition, gait recognition, speaker recognition and typing pattern recognition. When a user registers with the system which he/she will attempt to access later, one or more of his/her physiological characteristics are obtained and processed by a numerical algorithm. This number is then entered into a database, and the features of the user attempting to match the stored features must match up to a certain error rate.

a. Token Authentication

Token Authentication comprises security tokens which are small devices that authorized users of computer systems or networks carry to assist in identitfying that who is logging in to a computer or network system is actually authorized. They can also store cryptographic keys and biometric data. The most popular type of security token (RSA's SecurID) displays a number which changes every minute. Users are authenticated by entering a personal identification number and the number on the token. The token contains a time of day clock and a unique seed value, and the number displayed is a cryptographic hash of the seed value and the time of day. The computer which is being accessed also contains the same algorithm and is able to match the number by matching the user's seed and time of day. Clock error is taken into account, and values a few minutes off are sometimes accepted. Another similar type of token (CRYPTOCard) can produce a value each time a button is pressed. Other security tokens can connect directly to the computer through USB, Smart card or Bluetooth ports, or through special purpose interfaces. Cell phones and PDA's can also be used as security tokens with proper programming.

b. Password Authentication

Password Authentication uses secret data to control access to a particular resource. Usually, the user attempting to access the network, computer or computer program is queried on whether they know the password or not, and is granted or denied access accordingly. Passwords are either created by the user or assigned, similar to usernames. However, once assigned a password, the user usually is given the option to change the password to something of his/her choice. Depending on the restrictions of the system or network, the user may change his/her password to any alphanumeric sequence. Usually, limitations to password creation include length restrictions, a requirement of a number, uppercase letter or special character, or not being able to use the past four or five changed passwords associated with the username. In addition, the system may force a user to change his/her password after a given amount of time.

c. Two-Way Authentication

Two-Way Authentication involves both the user and system or network convincing each other that they know the shared password without transmitting this password over any communication channel. This is done by using the password as the encryption key to transmit a randomly generated piece of information, or “the challenge.” The other side must then return a similarly encrypted value which is some predetermined function of the originally offered information, his/her “response,” which proves that he/she was able to decrypt the challenge. Kerberos (a computer network authentication protocol) is a good example of this, as it sends an encrypted integer N, and the response must be the encrypted integer N + 1.

3. Common setup and access rights

Access Rights and Authority Levels are the rights or power granted to users to create, change, delete or view data and files within a system or network. These rights vary from user to user, and can range from anonymous login (Guest) privileges to Super user (root) privileges. Guest and Super user accounts are the two extremes, as individual access rights can be denied or granted to each user. Usually, only the system administrator (a.k.a. the Super user) has the ability to grant or deny these rights.

Guest accounts, or anonymous logins, are set up so that multiple users can log in to the account at the same time without a password. Users are sometimes asked to type a username. This account has very limited access, and is often only allowed to access special public files. Usually, anonymous accounts have read access rights only for security purposes.

The super user is an authority level assigned to system administrators on most computer operating systems. In UNIX and related operating systems, this level is also called root, and has all access rights in the system, including changing ownership of files. In pre-Windows XP and NT systems (such as DOS and Windows 9x), all users are effectively super users, and all users have all access rights. In Windows NT and related systems, (such as Windows 2000 and XP), a super user is known as the Administrator account. However, this Administrator account may or may not exist, depending on whether separation of privileges has been set up.

4. References

- en.wikipedia.org