HUMAN FIREWALL – CASE STUDY FACULTY OF ECONOMICS
BABEŞ-BOLYAI UNIVERSITY, CLUJ-NAPOCA, ROMANIA

PHD. STUDENT SERGIU JECAN
Business Information Systems Dpt.
Faculty of Economic Sciences, “Babes Bolyai” University Cluj Napoca
Str. Teodor Mihali, Nr. 58-60 400591, Cluj Napoca
ROMANIA

Abstract: It is known the fact that the safety of a system is determinated of the most little secure part of it. Many network administrators consider that if they have a good firewall they and their network are secure. But this is really true? The most vulnerable piece from a chain can break down the whole system. And in our case, end user is the most vulnerable piece. So, Human Firewall – must be the first target for any security policy that is implemented.

Key-Words: authentication, authorization, password

1. Introduction
Until the advent of the World Wide Web and the concomitant development of global computer networks, most networks could provide access to their resources with few concerns about the status of those who sought the information, or concerns that the information was restricted to certain classes of users. Developments in computer technologies have irrevocably altered networks operations, and it is now the exceptional network that has not in some way responded to the challenges of authenticating and authorizing its users, particularly those users needing to access the network systems and networked information resources from remote locations. Furthermore, networked information resources increasingly require authentication controls and need to specify different levels of authorization.

2. Authentication & Authorization
Authentication is the process of verifying that someone or something are who they say they are before they are granted access to protected resources.[1] Such resources may include software applications, computing facilities, printed data, check printers, or physical access to facilities and materials. Most discussion of authentication concentrates on online authentication, but offline methods of authentication have been around for quite a while. Such offline methods of authentication include checking for valid forms of identification like a driver's license or passport, or having security personnel check and recognize an employee's face before admitting them into a building.[2] Online authentication tools include user IDs and passwords, smart cards, security tokens, and biometrics.

Authentication can be based upon what someone has (a smart card, token, or ID card), what he or she knows (a password or PIN), what he or she is (a biometric like a fingerprint or voiceprint), or any combination of these. Normally, the more authentication factors in use, the more secure the authentication.
A distinction can be made between authentication and authorization; the former deals with validating that users are who they say they are, while the latter deals with validating which specific resources the user has permission to access.
Authorization is the process of giving someone permission to do or have something, including privileges of use, such as access to read and/or write files and directories, amount of allocated storage space, access to licensed electronic resources.
There are two type of authentication:
- between two computers
- between a human and a computer
Over the times, it has imagine several methods that confirm the identify of the user's to the system.
The authentication based on passwords is the easiest method and it is supposed to (transmit) clearly the access password. This way of authentication appeared as a necessity of the terminals without self power of calculation.
Approximately in the same period, some of the systems passed to the authentication based on the address, a method which was much disputed because of its advantages.
Once with the system's evolutions and increasing the power of calculation, it passed to cryptographically authentication.
Configure computers for user authentication - is one of the first steps you can make to a secure network.
An organization's security policy for networked systems should specify that only authorized users may access the computers. To enforce this, you need to configure the computer to authenticate users, who must prove that they are authorized for such access. Configuring the computer for authentication usually involves configuring parts of the operating system, firmware, and applications such as the software that implements a network service. A password policy should address:

- **length**: a minimum length for passwords. It is common to specify a minimum length of eight characters.
- **complexity**: the mix of characters required. It is common to require passwords to contain both uppercase and lowercase letters and at least one nonalphabetic character.
- **aging**: how long a password may remain unchanged. It is common to require users to change their passwords periodically (every 30-120 days). The policy should permit users to do so only through approved authentication mechanisms.
- **reuse**: whether a password may be reused. Some users try to defeat a password aging requirement by changing the password to one they have used before.
- **authority**: who is allowed to change passwords

It is relatively easy for an unauthorized user to try to gain access to a computer by using automated software tools that attempt all passwords. If the operating system provides the capability, you should configure it to deny login after some failed attempts. Typically, the account is "locked out" for a period of time (such as 15 minutes) or until a user with appropriate authority reactivates it. It is very important to unlock account after a specified period of time, because meanwhile owner of account may come back and if his account is lock he is in impossibility to work.

To accomplishment what other said before, we want to suggest that **auditing** – reading log file, check last logon on the system, is one of the most important task of a network administrator. Auditing provide information on when authentication and authorization was granted or denied.

### 3. Strong user authentication

#### The importance of user authentication in network security

In a network environment, user authentication can enable a perimeter device (a firewall, proxy server, VPN server, remote access server, etc) to decide whether or not to approve a specific user's request to gain entry to the network.[4]

It is necessary to be able to identify and authenticate users with a high level of certainty, so that they may be held accountable should their actions threaten the security and productivity of the network. The more confidence network administrators have that a user is who they say they are, the more confidence they will have in allowing those users specific privileges.

#### The need for something more than standard passwords

Predictable, easily-crackable, and/or unchanging passwords are the single weakest point in the standard site-security model. The majority of security attacks are achieved through password access. User authentication that relies on standard passwords alone fails to provide adequate protection for network systems.

When users make up their own passwords, they tend to choose ones which are easy to remember and, as a result, easy to guess. When passwords are created from randomly-generated characters, users tend to write them down because they're difficult to remember. Even if users are careful about the passwords they use, they are victim to a much more informed hacker/cracker community. A variety of easily accessible password-attack techniques can be used to guess user passwords or even decipher them when certain known encryption methods are used.

Because of the vulnerability of standard passwords, it is imperative that standard password-based access to systems or networks be managed properly, with the utmost attention given to controlling the generation, distribution, retrieval and use of passwords. In large and diverse networks, this is often a very difficult goal to achieve.

There is an easier solution to this problem, and that is to use strong user authentication.

It is important to understand that effective security is not found in a single product or system, but rather in the compilation of a variety of security solutions and tools used throughout the network. A firewall1 may be somewhat effective, but it is not flawless in keeping out potential trouble-seekers and is therefore only part of the overall security picture. Multiple layers of defence are necessary and a highly effective additional layer of defence is strong user authentication.[5]

There are three types of information that a system can use to prove that users are who they say they are.

---

1. [5] "many people feel that Internet security and Internet firewalls are synonymous. Although we should know that no single mechanism or method will provide for the entire computer and network security. Computer networks may be vulnerable to many threats along many avenues of attack. Firewalls can help protect against some of these attacks, but certainly not all."
Although the presence of all three is most desirable (and most demanding), the presence of at least two out of the three allows for a reasonable level of confidence in someone’s identity. When two out of the three are present, it is generally referred to as ‘strong authentication.’ (In practice, a network can achieve various levels of ‘strength’ or ‘weakness’ and thus various levels of trust and reliability, all tailored to its own particular security needs.)[Jecan05b]

- The first type of information is "something you have". Typically, this means that the user has a particular physical device that they alone were given and authorized to use that allows them access.
- The second is "something you know". Typically, this means that the user knows a secret, such as a particular password that only they were supposed to have been given and that they alone know.
- The third is "something you are". This means that the user possesses some human attribute, some biometric feature that can be scanned and digitally documented, such as a fingerprint or retinal scan.

The third type of information, comparing a biometric feature, is the most costly and the most difficult to implement. Therefore, when security managers are seeking a simple, cost-effective ‘strong authentication’ solution, often they look to incorporate the first two pieces of information, ‘something you have’ and ‘something you know.’[6]

**Passwords**

Since many authentication mechanisms depend on passwords, it’s important to understand how password can be compromised. There are three ways of getting around a requirement for a fixed password:
- ✓ find a way to get the system to tell you the password;
- ✓ find a way to authenticate without knowing the password;
- ✓ guess what the password is.

**4. Social Engineering** is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that are against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes. It is generally agreed upon that “users are the weak link” in security and this principle is what makes social engineering possible.

A contemporary example of a social engineering attack is the use of e-mail attachments. After earlier malicious e-mails led software vendors to disable automatic execution of attachments, users now have to explicitly activate attachments for this to occur. Many users, however, will blindly click on any attachments they receive, thus allowing the attack to work.

Perhaps the simplest, but a still effective attack is tricking a user into thinking one is an administrator and requesting a password for various purposes. Users of Internet systems frequently receive messages that request password or credit card information in order to "set up their account" or "reactivate settings" or some other benign operation in what are called phishing attacks. Users of these systems must be warned early and frequently not to divulge sensitive information, passwords or otherwise, to people claiming to be administrators. In reality, administrators of computer systems rarely, if ever, need to know the user's password to perform administrative tasks. However, even this might not be necessary — in an Infosecurity survey, 90% of office workers gave away their password.

Social engineering also applies to the act of face-to-face manipulation to gain physical access to computer systems.

**5. Case study - Faculty of Economics - Babeş-Bolyai University, Cluj-Napoca, Romania**

Study case was perform on 96 teaching stuff from 150 total persons.

Online formulary allow some conclusion about theoretical problem discussed above.

First element that we have ask was IT and security knowledge. This can suggest an image of sampling pattern.

A particular situation constrain that both webmail and web server are on the same physical machine. Users can logon with same username and password; for web

---

2 Online Security

server they can use either secure ftp (sftp) or any other third party software that can communicate on port 22.

We can observe that if 86.5% check e-mail daily, and almost half of them (39.6%) never use their secure connection to server; even webmail use a secure connection – https – on this platform you can not make any audit operation;

On the other hand, webmail inspire less trust for 62.5% of them than other free mail like yahoo or gmail.

Concern password, we already mention that a relatively good password involved at least 8 characters; As we can see above, a lot of people use 6 – 12 characters on their password, and only 8% of them has more than 12 characters on password.

Even 67% use substring that are related with their person, most of them think that they have a relative good password, a reasonable password level.

We define a range from 1 to 10, 1 – week, 10 – strong, to quantify, what people think about their passwords.

A lot of them (14%) think that their passwords are very week.

There is another strange situation. More than 50% admit that they gave their password to other people. One of the most important rules in security is that nobody, even an administrator, cannot know or obtain your password; He only can erase or modify your password.

One of the big challenges is to not use the option “Remember password” form browsers like IExplore or Mozilla. They store your password locally, and is quite easily for an intruder to steal your hash (fingerprint). We already mention about online and offline password cracker. In case of online authentication, response time is relatively long, and you can lock account after several failed attempts to logon, offline password cracker are more convenient to use, because are more quickly, and it can test any combination.
And about audit, we already mention that is one of the most important element for a good security level. Only 66% verify their last login, and more than 80% never read their log files. Last login is the first signal that everything is ok or if you must make more research in auditing tools; if you know that you not login more than a week and you see that somebody use your account, you must go further and verify in log files who and what changes. This is a laborious work and a lot of time consumer.

6. Conclusion
It is known the fact that the safety of a system is determinated of the most little secure part of it. The systems of which we have spoken hereinbefore are no exception. An assailant will not choose for example to decode a secure communication with 1024 of bits when he can install a program which interceptive pressures of key if he has the occasion. The modification of protocols of authentication and casting keys to obtain a resistance to an attack has to be compatible with the park of software installed currently. A modification – no matter how many benefits it gets - will be hard to implement if it suppose major changes in software or tear the compatibility with the previous version.

Training users about security policies and ensuring that they are followed is the primary defense against any intruder and social engineering.

References:

Acknowledgements
The research included in the present article is circumscribed to TD-169 Grant “CONTRIBUTII LA CONCEPEREA, PROIECTAREA SI IMPLEMENTAREA UNUI SISTEM DESTINAT MANAGEMENTULUI UNUI INTRANET IN CADRUL IMM-URILOR.”.