Secure Environment for Internet Browsing

Alexandru-Tudor GAVRILESCU
IT&C Security Master Program
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies
ROMANIA
tudor.gavrilescu@gmail.com

Abstract. The Internet is used by a large proportion of the population, but unfortunately their education regarding the usage of the instruments available is poor, resulting in potential informational frauds, especially in the financial field.

In this article I have approached a few simple problems, yet very important and frequently occurred, regarding the secure environment for Internet browsing, proposing solutions for each of them. The security methods are: anti-phishing; the prevention of SQL injection, through the verification of the data given as input in the Address Bar and in the password fields and blocking the access in case of a potential threat; a virtual keyboard for preventing the recording of the keys pressed (key loggers); the backup of the credentials in a local file and the encryption of it to prevent unauthorized access, the decryption of the data is made using a unique encryption key, owned by the user.

Key-Words: phishing, virtual keyboard, web browser, cryptography, SQL injection, key logger, cookies.

1. Introduction

A web browser is a software application, which allows the user to access the information available on the World Wide Web (www). An information resource is identified by a Uniform Resource Identifier (URL), and it can be a web page, an image, a video clip or any other type of content. The web browsers can also be used to access the information available on the private servers.

I have chosen the subject of the secure environment for Internet browsing because in these days, a lot of users do not pay attention to the potential risks to which they expose themselves when they give personal data to certain sites. I consider this problem to be of great importance, because the Romanian users are often victims of online frauds, fact which generates an increased reticence regarding the usage of the Internet, which represents an obstacle in the way of the IT market’s evolution.

In this article I have proposed 4 solutions for 4 problems: phishing, SQL injection, key loggers and encryption. The solutions are: anti-phishing method; strictly verification of the data given by the users; a virtual keyboard to prevent the key loggers; and the backup and encryption of the data.

This article is structured in 5 chapters: the first is the introduction, in which I presented the concept of a web browser; the scope and goals of the article; the justification of the chosen subject. The second chapter comprises the theoretical part which creates a background for the application; the types of informatics attacks, briefly explained; and methods of security against them. In the third chapter I presented the application, from the point of view of the user, explaining its interface and the functions used. The fourth chapter is about the technical documentation of the application, presented in the form of a manual. The last chapter presents the personal conclusions regarding the subject.

2. Online security

The informatics attacks can be classified under 3 levels: the opportunistic attacks, intermediary attacks and sophisticated attacks. Each of them has different characteristics and different potential threat level. The types of attacks chosen to be discussed in the paper are: the key loggers, phishing, SQL injection and cookies tracking. Also, two methods of
security are presented in this paper: data encryption and anti-phishing.

2.1 Attack Levels
Opportunistic attack: is the most frequent type of attack and is often associated with the occasional attackers. It has the following characteristics: the attacker has a very general objective and it uses a large range of targets. One of the immediate impacts can be the Denial of Service (DoS). A method of protection against this type of attacks is the proper configuration of the firewall software, controlling and monitoring the access, in order to get awareness of new vulnerabilities of the system.

Intermediary attack: it has a specific organized goal. The attacker executes the same types of actions as the one who launches an opportunistic attack, but it hides its tracks. This kind of attack has the following characteristics: it initially compromise the security of one of the trusted external systems; the attacker have patience and is highly skilled; there is a high probability of success, in comparison with the opportunistic type of attack.

Sophisticated attack: it has a specific organized goal and it can greatly affect the essential services. This type of attack can compromise the internal personnel. This attacks have a very high rate of success. It has the following characteristics: the attacker has enough time to gather information about the system's architecture and about the personnel; the attacker has a clearly defined goal and it can modify or create his own tools.

2.2 Attack Types

Key Loggers
A key logger monitors the activity of the keyboard, recording the signals sent by each key and the sequence. The key logger’s software can be divided into 5 categories:

- Hypervisor-based: it runs similar to a virtual machine.
- Kernel-based: complex method, from the point of view of writing and protecting from.
- API-based: the key loggers are attached to the keyboard’s software and then the operating system notifies the attacker when a key is pressed.
- Key logger journal: which allows to intercept the input data of the users which is sent to the server for processing; the journal is processed before it is encrypted through the HTTPS.
- Packets analysis: it represents the act of interception of the TCP packets, by capturing the network traffic associated to the unencrypted passwords.

The solution to this problem is a virtual keyboard, which has the same functions of a physical keyboard and I can be successfully used in simple actions like writing of small texts (user names and passwords). Another solution is an anti-key logger, a software designed to detect the key loggers and which include the ability to delete or disable the key loggers hidden in the PC.

Phishing
It represents a new type of attack, which targets both personal computers and corporations, and which uses the “fishing” of information as main method of action. The “fishers” use spam emails to direct the victims to websites specially designed by the hackers, which seem secure at the first sight. The “fishers” have developed their methods and techniques, using malicious codes hidden in all types of files or web applications, which install ghost applications which are immediately activated when the emails are opened.

The phishing is a method of identity stealing, that is why it often target database centers. From the moment the attacker managed to obtain identification information of a local user, it can access the information of the database and all the network's resources. This method is popular among the bank frauds and it is especially used for illegal transfers of funds through different banking systems.

The simplest method of fighting this kind of attack is to educate the users in this regard. On the long term, however, the companies must reach an agreement on
how the emails authentication process should take place, unanimously accepted.js

**SQL Injection**
This type of attack is often used to compromise the applications used to manipulate large quantities of data. This thing is realized by inserting SQL statements, with the goal to insert a specially design SQL query. This attack exploits the security vulnerabilities of the software.
A method of protection is using the escape characters, which have special meaning in SQL. This way, a black list is created which contain all the characters which need to be converted. Another method of protection is restricting the user’s access strictly to the part of the database it needs.

**Cookies Tracking**
A HTTP cookie is a special text, often codified, sent from a server to a web browser and back, every time the user access that server. The cookies are used for the authentication and monitoring of the user’s behavior. A good example is the implementation of the cookies in the “shopping basket”. The servers use the cookies with the goal to differentiate the users and to be able to react to their needs, during a session. Another application is the customization of the viewing of the web pages, taking into account the user’s preferences.

### 2.3 Security Methods

**Data Encryption**
The computers send data messages to the Internet in the form of packages. One of the biggest risk is the transmission interceptions. For the protection, all the transmissions must be encrypted. The data encryption represents the rearrangement of the data in a random way, which can be later rearranged using the encryption key.
There are several types of encryption systems, but we will only analyze the Data Encryption Standard (DES). Today it is considered the least secured method in many situations, but it is the simplest to implement. The algorithm has different forms, like Simple DES, Triple DES, the least being the most powerful. DES encrypts and decrypts the data in blocks of 64 bytes, using a key with a length of 64 bytes. 56 out of the total 64 bytes are used for the algorithm, the rest are used as parity bytes. DES is composed of 16 identical processing steps, named rounds, which produce the codified text. The security of the algorithm increases exponentially with the number of rounds.

**Anti-phishing**
The causes for phishing vulnerability can be summarized into the following categories:
- Weak Authentication Schemes
- Browser vulnerabilities
- Security Flaws
- Non secure desktop tools
- Lack of user awareness
- Ease of impersonating a trusted source

However, most phishing emails are sent asking the user to click on a hyperlink. After extensive analysis of hundreds of phishing emails and the methodologies used in phishing, phishing hyperlinks were categorized into the following general categories:
- The actual link and the visual link in the email are different i.e., the hyperlink in the email does not point to the same location as the apparent hyperlink displayed to the users.
- The DNS name in the hyperlink is substituted by the quad-tuple IP address.
- DNS names used are manipulated to look similar to the genuine DNS name the phishers are trying to forge.
- The hyperlink is encoded so that it becomes very difficult to read for example, unusually long hyperlinks.
- When visiting the phishing hyperlink, it usually asks the user for various personal details like username, password, account number, SSN, etc.
In general, the anti-phishing techniques can be classified into the following 4 categories:

- **Content Filtering**: In this methodology content/email are filtered as it enters in the victim’s mailbox using machine learning methods, such as Bayesian Additive Regression Trees (BART) or Support Vector Machines (SVM).
- **Black Listing**: Blacklist is collection of known phishing Web sites/addresses published by trusted entities like Google’s and Microsoft’s black list. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.
- **Symptom-Based Prevention**: Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.
- **Domain Binding**: It is a client’s browser based techniques where sensitive information (name, password) is bind to a particular domains. It warns the user when he visits a domain to which user credential is not bind.

3. Solution

In this implementation, I tried to look into several attack and find a good solution to tell the user that it’s in danger and try to block the internet traffic in some cases. This solution contains 4 parts that work together and manage to save the user from several attacks, ones with a really big impact.

In the anti-phishing part I experimented with link related feature and also with the requests sent to a specified cloud:

1. **Unmatching URLs**: A binary value to show whether the visible URL is as the same as the hidden URL.

2. **Cloud**: A database with the blacklist that contains all known phishing sites until now.

The second part contains some SQL injection filtering applied on the textboxes and the address bar of the browser. Also on the textboxes where the user inserts his password it will activate the on-screen virtual keyboard. This will be manipulated in such a way that it will be very hard to interpret the mouse clicks and position. This way the key logger, an attack that records all the keys pressed, will be useless. It will show a certain number of clicks that cannot be put in such an order that the attacker will find out what the user tried to write.

In the last part I tried to implement a mechanism that will save all the credentials that the user uses into a file. This file will replace the browser cookies part. The file stored locally will be encrypted with a unique generated key. Only the user will have access to it. Besides this, the mechanism will know when and where to write the stored credentials. This way the user will type only once and after that it will be just a plain auto-complete.

This entire structure can be illustrated in Figure 1 and Figure 2.

![Figure 19. URL check flow](image-url)
4. Implementation

The prototype currently includes a C#.Net implementation of a web browser. Installation of the system is simple. The user will have to use this web browser for browsing the internet. In regard to the interface, it can be easily seen just by opening the application, that it contains the main elements found in a regular browser. The window contains 5 important buttons:

- **Previous**: a button used for navigating to the previously accessed web page
- **Forward**: a button used for navigating to the web page accessed after the current one
- **Stop**: a button used to stop the ongoing navigation
- **Refresh**: a button used to refresh the page that the navigator is currently accessing
- **Go**: a button used to start navigation to a certain page.

All other features have nothing in the interface except the warnings:

**SQL injection** – the browser will continuously check the entered URL and the text entered on all the textboxes on the site. (Figure 3) If it contains some SQL queries the internet traffic will be blocked telling the user what is happening.

**Figure 21. Browser address bar**

Anti-Phishing – The browser will check every link inserted in the address bar before the navigation. This is made with the help of a function that will send a request to a cloud from which it will get an answer if it’s ok or it’s considered a threat. If it’s considered a threat then the browser blocks any traffic and warns the user about what is happening. (Figure 4)

**Figure 22. Browser warning**

5. Conclusion

In this article it is described a browser that has a medium level of security. It takes into account the attacks that can be easily spotted and with a minimum informatics knowledge can be avoided. A lot of users do not pay the required attention to the small details around them and they do not realize at what risks they are exposed. This browser has implemented a prevention system against SQL attacks, system that not only helps the user but it will help everybody else if this browser
will be used at a larger scale. This way all the sites that are vulnerable to such attacks will be safe because all the attack would stop from the browser. One thing that it’s considered by others a low importance application is the virtual keyboard. In my software I manipulated the keyboard in such a way that it will always show up when the user tries to type a password, in a new form and in a new position on the screen. A lot of user doesn’t realize how easy the keys can be recorded by a key logger. One of the most important attack represents the phishing. In my application I tried to make the user avoid these types of attacks using web site scanning and checking the navigated URL. This application in the end completes the user in such a way that he will not miss the small details that could make him a lot of harm.

Acknowledgement

Parts of this research have been published in the Proceedings of the 7th International Conference on Security for Information Technology and Communications, SECITC 2013.

References