International Journal on
Advanced Science
Engineering
Information Technology

Vol. 2 (2012) No. 5
ISSN: 2088-5334

Ancillary Resistor leads to Sparse Glitches: an Extra Approach to Avert Hacker using Syndicate Browser Design

Devaki Pendlimarri [#], Paul Bharath Bhushan Petlu [*]

[#] *Dept. of Computer Science & Engineering, Sri Venkatesa Perumal College of Engg. & Tech., Puttur - 517583, India*
E-mail:pdevaki02@gmail.com

[*] *Dept. of Information Technology, Sri Venkatesa Perumal College of Engg. & Tech., Puttur - 517583, India*
E-mail: trishipaul@rediffmail.com

Abstract— **After the invention of internet most of the people all over the world have become a fan of it because of its vast exploitation for information exchange, e-mail, e-commerce etc. for their easy leading of life. On the other side, may be equally or less/more, many people are also using it for the purpose of hacking the information which is being communicated. Because, the data/information that is being communicated through the internet is via an unsecured networks. This gives breaches to the hacker who is known as the man-in-the-middle to hack the data/information. In this paper, we describe some novel methodologies to prevent the hacker in hacking the data/information. The web browser design is being carried out in our R&D lab and we have found that the novel methodology has given solution to prevent the man-in-the-middle from several attacks.**

Keywords— **Hacking; attacks; network security; information security; man-in-the-middle; web browsers; phishing attack.**

I. Introduction

In the electronic communication system the data/information security is an important and highly burning issue. In the early computing days as there were a few computer systems and a small number of users who work within the same network. However, with the advent of internet and its vast exploitation for e-banking, e-commerce etc. the use of computers has been increased and the information is being communicated across the unsecured networks. This gives chance for the security breaches [4],[5].

The major glitch of the internet is that the unsecured network. As they are unsecured and we do not have control on it, the information that is being communicated through this network is not guaranteed. The hacker/attacker being a man-in-the-middle, the information can be retrieved and do harm to the system or individual, which is being considered as a major glitch to the system as well as the individual.

The hacker can attack the data/information at any layer. At each layer we have set of protocols to prevent the hacker from several attacks. However, still the hacker is finding the ways to attack. Through the web browsers we are accessing the web pages of the services offered by several organizations/corporations. The web browsers are designed so as to provide convenience and comfort to the user. Though there are controlling mechanisms like firewalls etc. these browser do not have control over the information it receives. By following certain measures we can give some control to the browser on the information which leads to the fewer glitches.

Here, we suggest some novel set of methodologies to prevent the hacker or attacker being a man-in-the-middle between two systems in the unsecured network tries to hack the information and do harm to the system or an individual.

II. Background

There were many applications developed and being served through the internet, which had made the leading life of the people so easy. Some of them are:

- E-Banking: Internet banking (e-banking or online banking) means any user with a personal computer and a browser can get connected to his bank –s website to perform any of the virtual banking functions. In internet banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu. Any service can be selected and further interaction is dictated by the nature of service.
- E-Commerce: Electronic commerce or EC is commonly known as e-comm, e-commerce. In

practice, this term and a newer term, e-business, are often used interchangeably. For online retail selling, the term e-tailing is sometimes used. The EC is the buying and selling of goods and services over electronic systems such as the internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread internet usage. The use of commerce is conducted in this way, spurring and drawing on innovations in electronic funds transfer, supply chain management, internet banking, online transaction processing, electronic data interchange, inventory management systems and automated data collection systems.

- E-mails: Electronic mail, commonly known as e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time, instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

The other side of the internet is its glitches. As the information exchange through the internet is via an unsecured network, the hacker/attacker being a man-in-the-middle, can easily hack the information that is being communication and do harm to the data. Every organization/corporation providing their services through the internet requires security for their information. But, some applications require high security because any glitch will lead to a big loss/damage such as e-banking. Some of the glitches from the man-in-the-middle are [6]:

A. Phishing Attacks

The phishing attack is that the hacker sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. The hacker creates a fake web site that looks exactly same like a popular site such as SBI bank or PayPal etc. When the user attempts to log on with their account information, the hacker records the username and password and then he tries that information on the real site.

B. Hijack Attack

The hacker takes over a session between you and the other individual and disconnects the other individual from the communication. You will still believe that you are talking to the original party and may send private information to the hacker by accident.

C. Spoof Attack

The hacker modifies the source address of the packets that is being transmitted through the network. Hence, it appears to be coming from someone else instead of the source name. This may be an attempt to bypass your firewall rules and allowing entering into the system.

D. Buffer Overflow Attack

The attacker sends more data to an application than is expected causing a buffer overflow. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

E. Replay Attacks

The hacker will capture the user credentials in the network traffic. He then resends the captured data in the network with the hopes of getting the same response as the original user. In case of passwords, replay attacks are the attempts to gain the access to the information without having to know the valid credentials. For example, if an attacker can sniff packets that contain encrypted authentication credentials, the attacker may be able to re-send the encrypted credentials—without ever decrypting them—and be authenticated by the recipient if the authentication protocol is vulnerable to replay attacks.

F. Active Attacks

The attacker tries to bypass or break into the secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DOS, or modification of data.

G. Passive Attacks

This type of attack monitors an unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

H. Password Attacks

The attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords. A brute-force attack is when the attacker tries every possible combination of characters. The hybrid attack uses the both techniques.

There are many other types of attacks through which the hacker/attacker is making harm to the system. Here, we suggest some novel set of methodologies to prevent the man-in-the-middle being a hacker or attacker to hack the information and do harm to the system or an individual.

III. Methodology

If we see the working model of the internet, we can clearly understand that the service provider do not have a control on their information which is being communicated through the unsecured networks. Any user can access any web page with its URL. While this page is travelling through the network, any hacker being a man-in-the-middle can access the information and view this page on his browser. This is because of the loop holes in HTTP/IPs. The service provider as well as the user, both are suffering with many attacks.

There are several organizations/corporations which are offering their services through the internet such as e-banking. They are taking high security measures at their end to the data/information. However, the users are suffering with many attacks. The Phishing attack is one of the major attacks through which the user is suffering today.

Here, we suggest a novel methodology to prevent the hacker/attacker from capturing the information through several types of attacks being a man-in-the-middle. The theme of the novel methodology is that "More control leads to the fewer problems". We suggest some additional control methods in the design of the browser to give solution to several attacks.

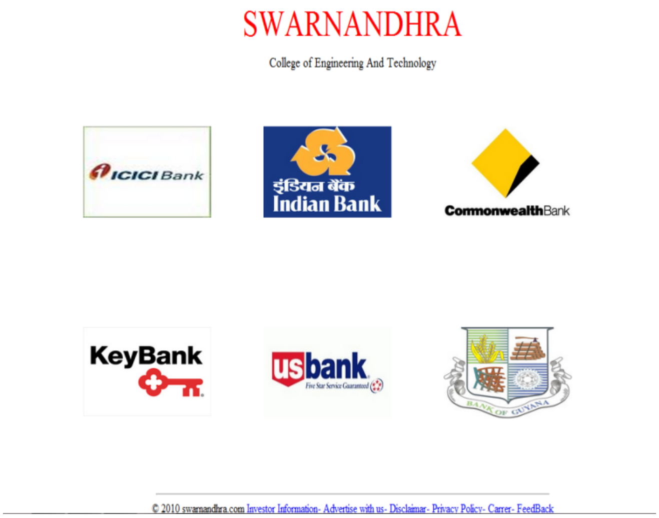
A. Syndicate Browser Design

E-banking is one of the internet service which requires the most and high security at the both ends i.e., the service provider and the user. There are many banks offering their services through e-banking. These services can be accessed with the respective web pages through their URLs provided the user must have an account. As the user was asked to enter the URL there is a chance to type the wrong URL, which leads to the chance of phishing attack. Why does the user need to type the URL? Why can't he select an option of service? There are many other ways of phishing attack.

We found that the hacker is able to attack the user through the phishing attack to know the user's information because of the following reasons:

- Typing wrong address of the site's URL
- Sending links of the fake web sites to the mail accounts
- Opening fake web sites along with the opening of new web page
- Etc.

These types of attacks can be prevented with the help of the novel methods presented here. We suggest the organizations/corporations which need high security to their data/information to form a syndicate to use a common browser designed with some set of protocols. These protocols will give abundant control to the browser to prevent the hacker. This new browser is designed without the address bar to type the URL. This browser will show the icons of the registered organizations / corporations on its home page. The sample browser home page is as shown in Fig 1. The generalized structure of the services of the browser is shown in Fig 2. A click on the icon will get connection with the corresponding organization / corporation services through the internet. The server also designed so as to respond to the requests received from this browser only with the help of additional information that is sent to the server along with the request.



SWARNANDHRA

College of Engineering And Technology

© 2010 swarnandhra.com Investor Information- Advertise with us- Disclaimar- Privacy Policy- Carrer- FeedBack

Fig. 1 A sample browser home page with some bank icons

The browser will have some browser variables. Whenever the user clicks a link to open in a new tab, this URL is stored in the web browser variable. When the reply is received, the received URL is compared with the browser variable for the match. If it matches with the browser variable then the page is displayed. Otherwise, the page will not be displayed. Another browser variable is used to prevent opening more than one new tab at a time. This leads to the prevention of the phishing attack. We can prevent the hacker by giving some control to the browser with the help of browser variables.

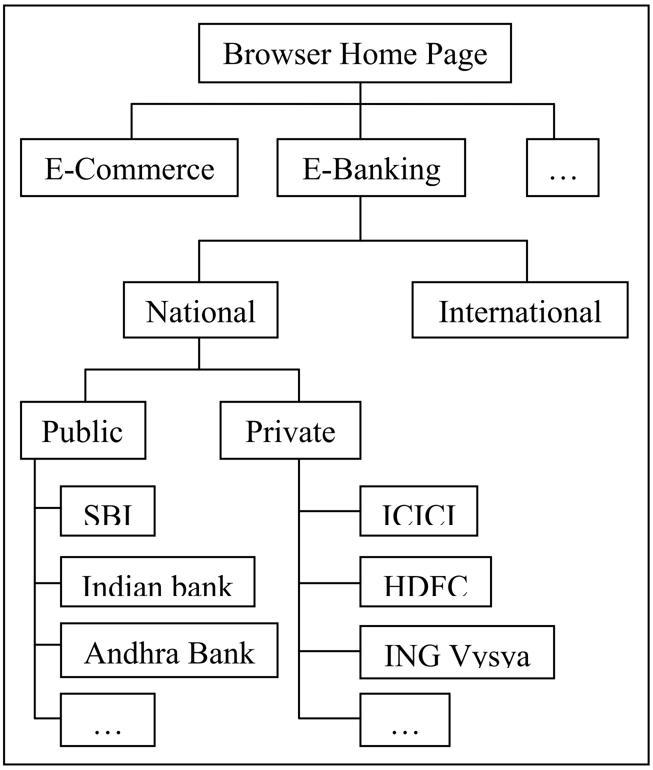


Fig. 2 A sample structure of the classification of the home page

B. *Support with the Hardware*

Whenever the user selects an option, the browser gets connection with the service. This service request will be sent to the browser through the unsecured network. As the network is unsecured, we can't control the information on the network. However, we can control the information on the pages at the server side as well as the user side in the application layer.

When the user selects a service on a page, this request is sent to the server with a hardware device id along with the IP address. This hardware device id should be read by the browser and attached to the packet sent to the server. The server processes the request and sends reply to the user from which it has received the request with the help of IP address. Along with this reply it also sends the hardware device id received from the user. The page is downloaded onto the browser so that the user is able to view. Before viewing page onto the browser the hardware device id is read by the browser once again and compared with the id received from the server along with the reply. If both the hardware device ids match then only it displays the page onto the browser. Otherwise, it displays an error message onto the browser. The hardware device id should be selected as unique of any two users such as RAM id etc. No two RAM ids are same. The browser is designed so as to read and attach the id along with the request sent. The user should be kept unknown from the details that "which hardware device id the browser will read".

Why do we need to use a hardware device id instead of IP address? The reason behind this is that any user can change their system's IP address same as the other user's IP address. But, the hardware device id can't be changed by a user.

C. *Support with the System Variables*

The above method also can be implemented with the system or browser variables. When the user submits the details, the browser will read a system variable created for this purpose. This variable is attached to the information sent to the server. The server will process the request and sends the system variable back along with the reply to the client. Now, once the browser receives the packets it first checks the system variable received with its system variable. If both system variables match then only the content will be displayed. Otherwise, the content will be erased or disappeared.

IV. Conclusion and Future Work

After the invention of internet most of the people all over the world have become a fan of it because of its vast exploitation for information exchange, e-mail, e-commerce etc. for their easy lead of life. The data/information that is being communicated through the internet is via unsecured networks. This gives security breaches to the hacker to attack the data/information in several ways. The novel methodologies presented here are able to prevent the man-in-the-middle at the application layer. These methodologies have given solution to several types of attacks. We are also moving forward to continue our research in finding the optimum methodologies to prevent the man-in-the-middle at the other layers by developing new set of protocols into HTTP, TCP/IP etc.

Acknowledgment

We thank the management and the principal for giving their support towards our research. We also thank the experts / researchers who have contributed their research towards the innovative ideas/algorithms in the area of preventing man-in-the-middle attacks.

We thank our colleagues and others who contributed towards the development of this paper.

References

[1] Journal of Computer Science and Security (IJCSS Karen Scarfone and Murugaiah Souppaya: *"Guide to Enterprise Password Management (Draft)"*, Recommendations of the National Institute of Standards and Technology, Special Publication 800-118, 2007, 38 pages.

[2] Abhay Kumar Raj, Rajiv Ranjan Tewari & Saurabh Kan Upadhyay: *"Different Types of Attacks on Integrated MANET- Internet Communication"*, International) Volume (4): Issue (3), 2010, pp 265-274.

[3] Network security types of attack passive attack active attack: http://www.computernetworkingnotes.com/ccna_certifications/types_of_attack.htm

[4] International Journal of Computer Science and Network Security (IJCSNS) Esmiralda Moradian and Anne Håkansson: *"Possible attacks on XML Web Services"*, VOL.6 No.1B, January 2006.

[5] http://www.hacking.in

[6] Devaki Pendlimarri, Paul Bharath Bhushan Petlu, N L Kumar Anantapalli, and Dr. M Muralidhara Rao; "Novel Methodologies: Preventing Man-in-the-middle", Proceedings of International Conference on Computing and Information Technology-2011 (IC2IT), North Bangkok, Bangkok, Thailand, pp 116-121.