Cantina Antiphishing

[1]Angel N.V,[2]Aneesha K.V,[3]Swathy M.S, , [4]Ms.Reesha P.U
[1]Computer Science,
[1] St.Joseph's college,Thrissur,India

Abstract-The paper proposes a anti-phishing techniques strive to prevent phishing attacks by providing better authentication of the server. However, phishing actually exploits authentication failures on both the client and the server side. Initially, a phishing attack exploits the user's inability to properly authenticate a server before transmitting sensitive data. The anti-phishing system using the following techniques the administrator can found the site is a phishing site or not. First, heuristic checks if a page's URL contains an "at" (@) or a dash (-) in the domain name. Second, This heuristic applies the URL check above to all the links on the page and finally Heuristic checks if a page's domain name is an IP address. This heuristic is also used in PILFER. A complete anti-phishing solution must address both of these failures: clients should have strong guarantees that they are communicating with the intended recipient, and servers should have similarly strong guarantees that the client requesting service has a legitimate claim to the accounts it attempts to access. Reduce reliance on users.

***Index Terms*—**Cantina Anti-phishing, phishing attacks, Anti-Phishing System.

I. INTRODUCTION

In phishing, an automated form of social engineering, criminals use the Internet to fraudulently extract sensitive information from businesses and individuals, often by impersonating legitimate web sites. The potential for high rewards (e.g., through access to bank accounts and credit card numbers), the ease of sending forged email messages impersonating legitimate authorities ,and the difficulty law enforcement has in pursuing the criminals has resulted in a surge of phishing attacks [1]. Citizens and cost businesses billions of dollars in 2004 alone. Phishing also leads to additional business losses due to consumer fear. Anecdotal evidence suggests that an increasing number of people shy away from Internet commerce due to the threat of identity fraud, despite the tendency of US companies to assume the risk for fraud. Thus, the research community and corporations need to make a concentrated effort to combat the increasingly severe economic consequences of phishing. We present three main contributions in this paper. First, we propose several design principles needed to counter phishing attacks: 1) sidestep the arms race, 2) provide mutual authentication.

II.EXISTING SYSTEM

Phishing attacks succeed by exploiting a user's inability to distinguish legitimate sites from spoofed sites. Most prior research focuses on assisting the user in making this distinction; however, users must make the right security decision every time. Unfortunately, humans are ill-suited for performing the security checks necessary for secure site identification, and a single mistake may result in a total compromise of the user's online account. Fundamentally, users should be authenticated using information that they cannot readily reveal to malicious parties. Placing less reliance on the user during the authentication process will enhance security and eliminate many forms of fraud [2]. We propose using a trusted device to perform mutual authentication that eliminates reliance on perfect user behavior, thwarts Man-in-the-Middle attacks after setup, and protects a user's account even in the presence of key loggers and most forms of spyware.

III.PROPOSED SYSTEM

We advocate the following set of design principles for anti-phishing tools. Many anti-phishing approaches face the same problem as anti-spam solutions: incremental solutions only provoke an ongoing arms race between researchers and adversaries. This typically gives the advantage to the attackers, since researchers are permanently stuck on the defensive. As soon as researchers introduce an improvement, attackers analyses it and develop a new twist on their current attacks that allows them to evade the new defenses. Instead, we need to research fundamental approaches for preventing phishing [3]. Most anti-phishing techniques strive to prevent phishing attacks by providing better authentication of the server. However, phishing actually exploits authentication failures on both the client and the server side. Initially, a phishing attack exploits the users inability to properly authenticate a server before transmitting sensitive data.

However, a second authentication failure occurs when the server allows the phisher to use the captured data to login as the victim. A complete anti-phishing solution must address both of these failures: clients should have strong guarantees that they are communicating with the intended recipient, and servers should have similarly strong guarantees that the client requesting service has a legitimate claim to the accounts it attempts to access. Reduce reliance on users [4]. The majority of current phishing countermeasures rely on users to assist in the detection of phishing sites and make decisions as to whether to continue are in many ways unsuited to authenticating others or themselves to others. As a result, we must move towards protocols that reduce human involvement or introduce additional information that cannot readily be revealed. These mechanisms add security without relying on perfectly correct user behavior, thus bringing security to a larger audience.

Avoid dependence on the browsers interface. The majority of current anti-phishing approaches propose modifications to the browser interface. Unfortunately, the browser interface is inherently insecure and can be easily circumvented by embedded JavaScript applications that mimic the “ trusted” browser elements.

IV.SYSTEM ARCHITECTURE

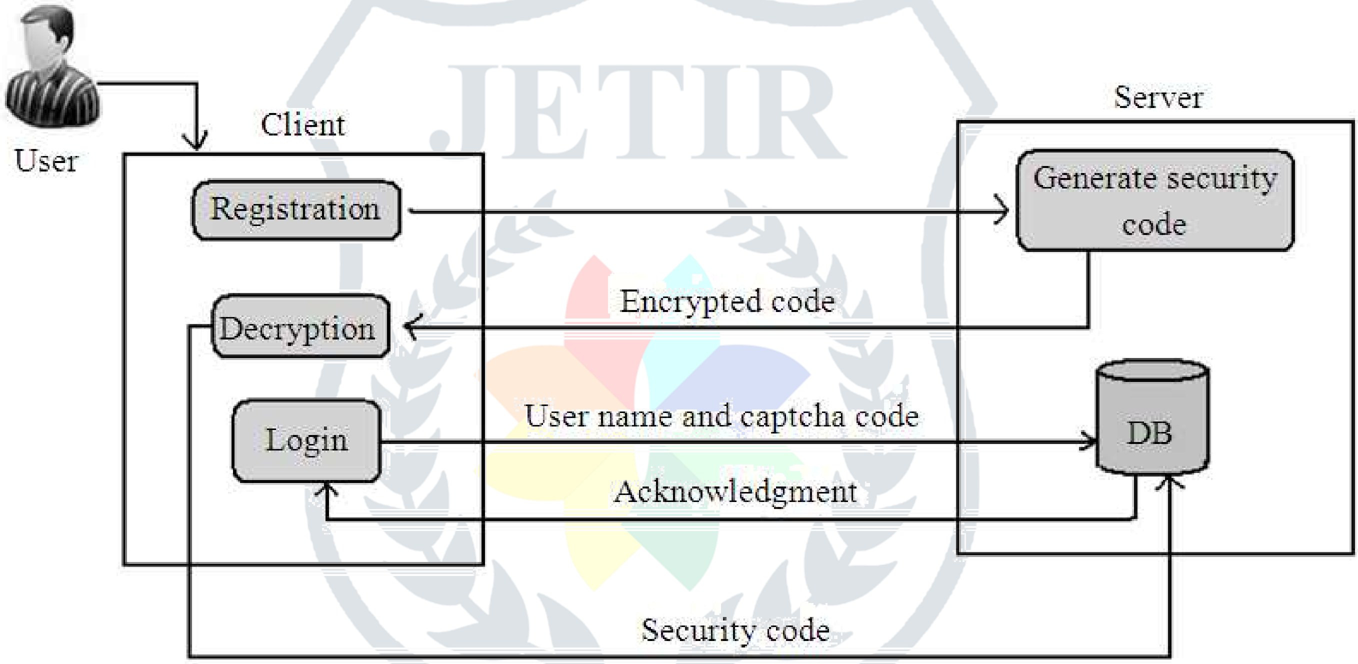
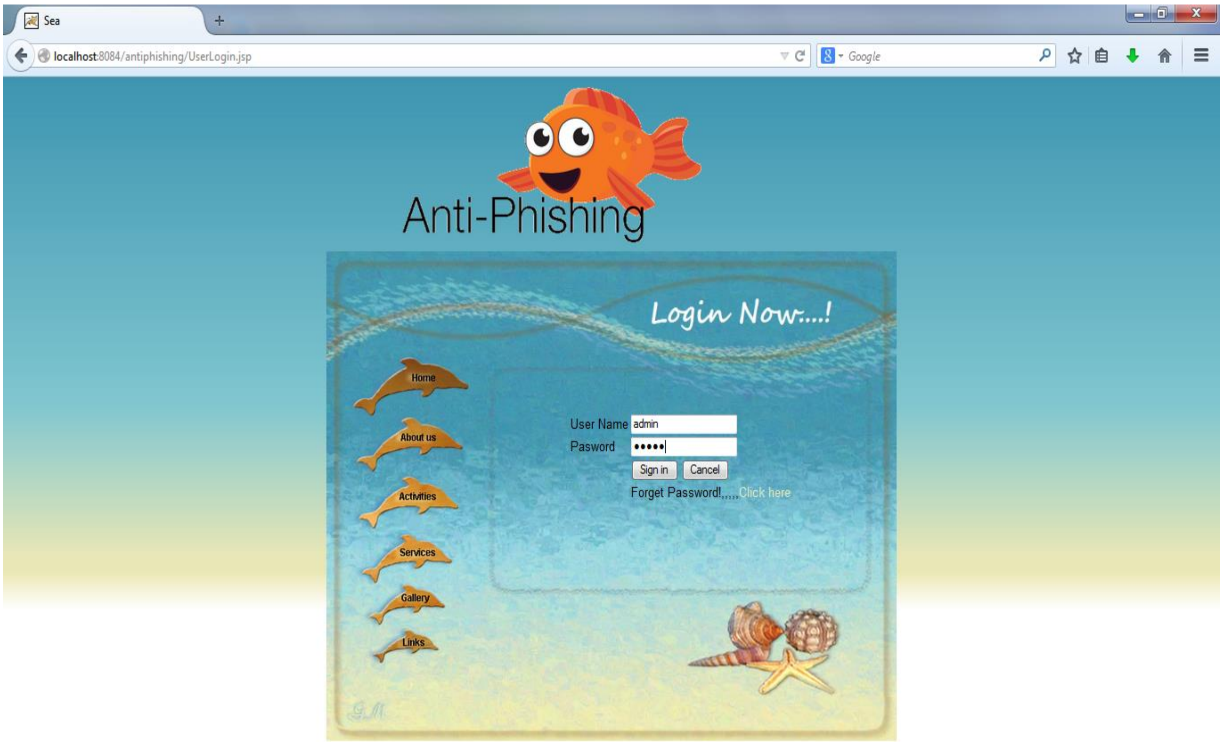


Figure 1. System Architecture

The system architecture is shown in figure 1. This modules deals with the registration of local users and management of users. The management includes Delete , View and Edit details of local users. The Administrator have the privilege of Delete and View Users. The registration and Edit details are the privileges of local users.

The system Authentication is achieved through the login process. Only the registered user can login into the system. So that the outsiders can't access the system. While signing into the system the users should provide a username and password which is already chosen during the registration. If the user name and password is not exist, the user can't login. It means that the user is not registered. Administrator username and password are already saved in database. After logging in the users(Administrator, User) can change their password. While the user is trying to access a site(browsing a site), first the request will be accepted by the administrator. After getting the URL, the administrator will check whether the site is a phishing site or not. If he found that the site is a hacker site, he will alert the user by giving option for continue / discontinue from the page.

V.IMPLEMENTATION

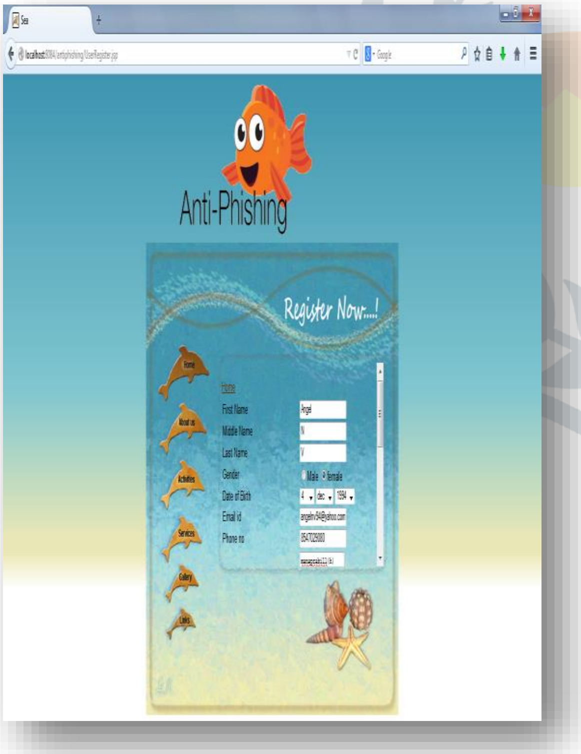


User Name admin

Pasword •••••

Forget Password!,,,,,Click here

Figure 2.Admin Login



First Name Angel

Middle Name N

Last Name V

Gender ○ Male ● female

Date of Birth 4 dec 1994

Email id angelnv94@yahoo.com

Phone no 8547029080

Figure 3.User Register

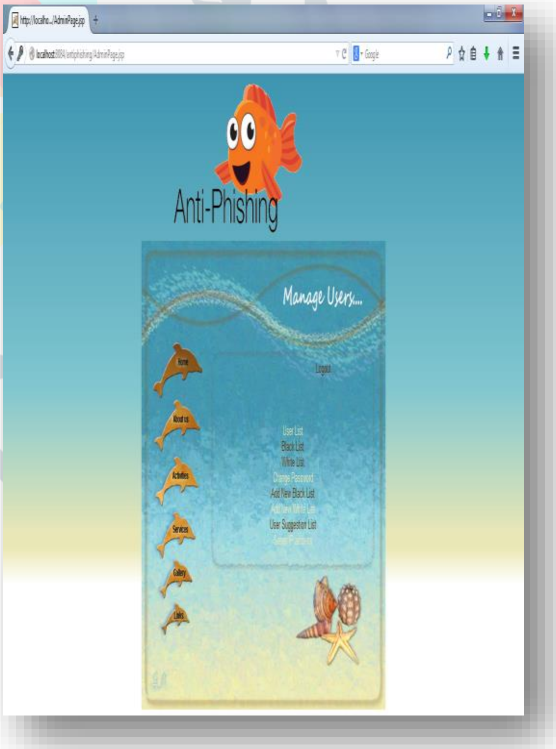
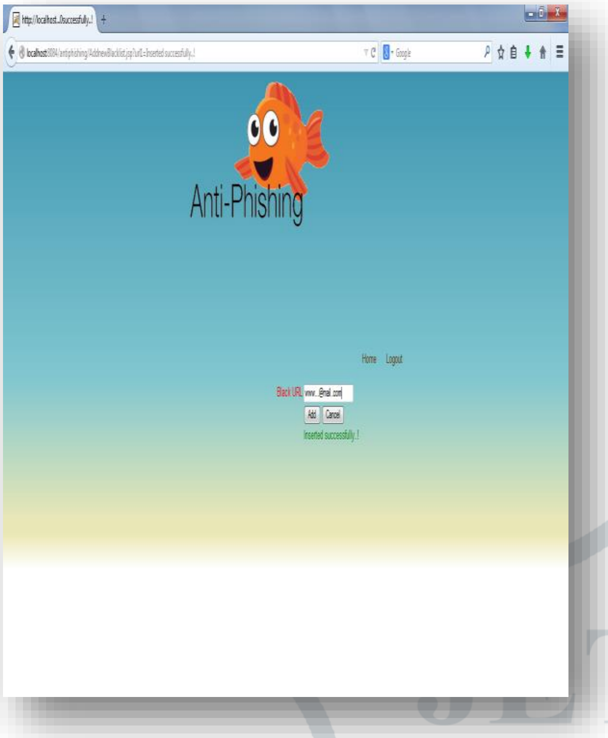


Figure 4.User Managing

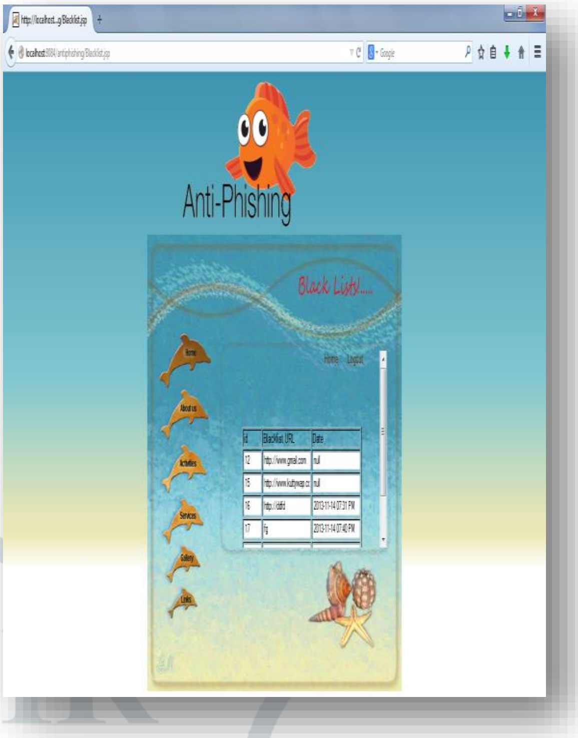


Black URL www...@mail..com

Add Cancel

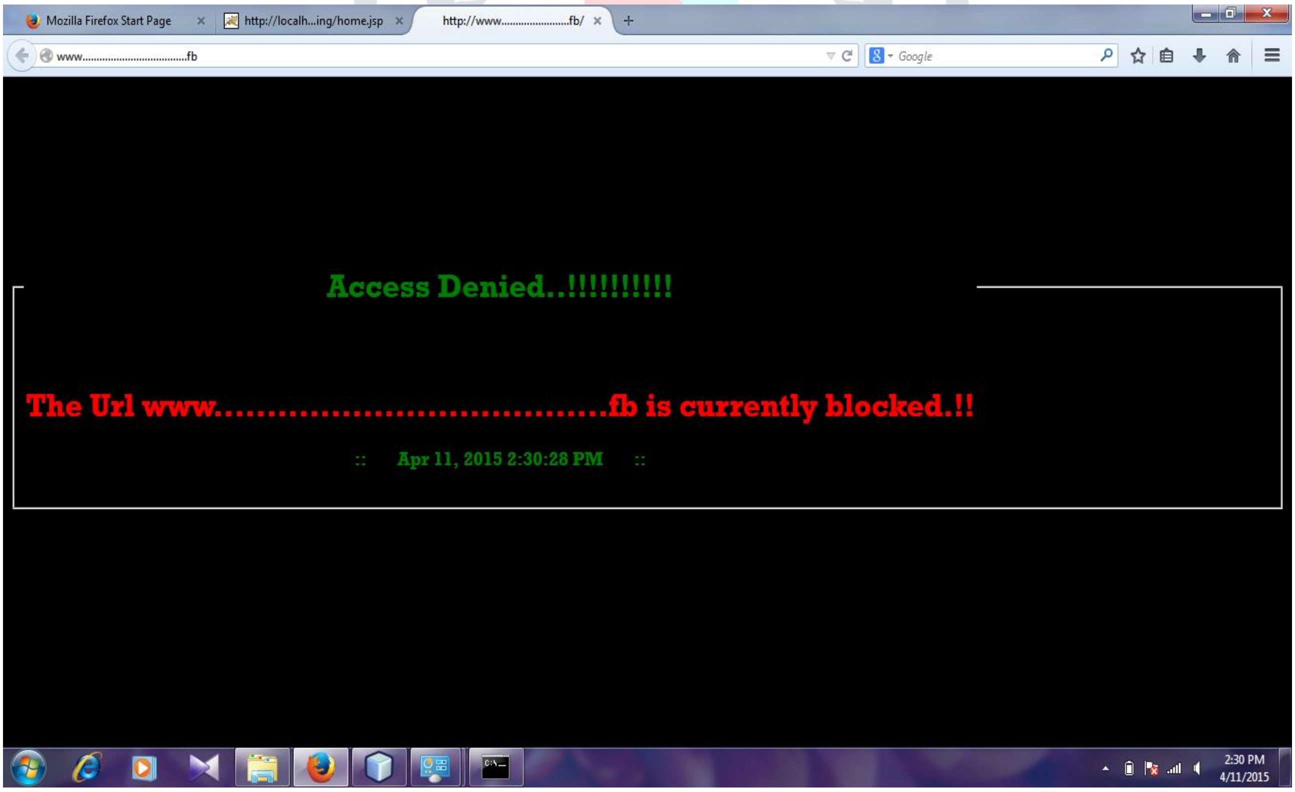
Inserted successfully..!

Figure 5.User add Black URL



Id	BlackList URL	Date
12	http://www.gmail.com	null
15	http://www.kuttywap.cc	null
16	http://ddfd	2013-11-14 07:31 PM
17	fg	2013-11-14 07:40 PM

Figure 6.View The Black List



Mozilla Firefox Start Page
http://localh...ing/home.jsp
http://www......................fb/
www.......................................fb
Google
2:30 PM
4/11/2015

Access Denied..!!!!!!!!!!

The Url www......................................fb is currently blocked.!!

:: Apr 11, 2015 2:30:28 PM ::

Figure 7.Access Denied The Black List

Figure 2 shows the deals with the registration of local users and management of users. The management includes Delete , View and Edit details of local users. The Administrator have the privilege of Delete and View Users. The registration and Edit details are the privilege of local users like in the figure 3. The system Authentication is achieved through the login process. Only the registered user can login into the system. User can add the blacklist and view them like shown in the figure 5 & 6.Finally getting the URL, the administrator will check whether the site is a phishing site or not. If he found that the site is a hacker site, he will alert the user by giving option for discontinue from the page like shown in the figure 7.

V.CONCLUSION

We advocate the following set of design principles for anti-phishing tools. Many anti-phishing approaches face the same problem as anti-spam solutions: incremental solutions only provoke an ongoing arms race between researchers and adversaries. This typically gives the advantage to the attackers, since researchers are permanently stuck on the defensive. As soon as researchers introduce an improvement, attackers analyses it and develop a new twist on their current attacks that allows them to evade the new defenses. Instead, we need to research fundamental approaches for preventing phishing. . Most anti-phishing techniques strive to prevent phishing attacks by providing better authentication of the server. However, phishing actually exploits authentication failures on both the client and the server side. Initially, a phishing attack exploits the users inability to properly authenticate a server before transmitting sensitive data [5]. However, a second authentication failure occurs when the server allows the phisher to use the captured data to login as the victim. A complete anti-phishing solution must address both of these failures: clients should have strong guarantees that they are communicating with the intended recipient, and servers should have similarly strong guarantees that the client requesting service has a legitimate claim to the accounts it attempts to access. Reduce reliance on users. The majority of current phishing countermeasures rely on users to assist in the detection of phishing sites and make decisions as to whether to continue are in many ways unsuited to authenticating others or themselves to others. As a result, we must move towards protocols that reduce human involvement or introduce additional information that cannot readily be revealed. These mechanisms add security without relying on perfectly correct user behavior, thus bringing security to a larger audience. Avoid dependence on the browsers interface. The majority of current anti-phishing approaches propose modifications to the browser interface. Unfortunately, the browser interface is inherently insecure and can be easily circumvented by embedded JavaScript applications that mimic the " trusted" browser elements.

VI.FUTURE SCOPE

As a future work on phishing we can do more work on server side security. In the server side security policy we use dual level of authentication for user by which only authentic user can get the access of his account, and to educate the user about this policy will results in avoiding user to give his sensitive information to phished web site.

VII. ACKNOWLEDGMENT

First of all, I would like to thank God, the Almighty, for having made everything possible by giving me strength and courage to do this project. Without Him, I would not have had the wisdom or the physical ability to accomplish this project. I am grateful to Dr.Sr.Annie Kuriakos, Principal, St.Joseph's College, Irinjalakuda for giving me all the necessary facilities to carry out my project work successfully.I am also grateful to Dr.Sr.Lissy Anto P, Head of the Department, Department .of Computer Science and the Members of Project Review Committee for their valuable suggestions.I wish to express my deep gratitude to my guide Reesha P U, Lecturer, Department of Computer Science, for all the advice, encouragement and constant support she has given me throughout my project work. This work would not have been possible without her support and valuable suggestions.
I would also like to thank all my friends for their help and constructive criticism during my project work. A lot of people have directly or indirectly contributed to this project in a variety of ways.

REFERENCES

[1] http://www.phishtank.com

[2] Dr.Krishna , "Anti-phishing" International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 2 Issue 3 March 2013 Page No. 558-568

[3] http://www.antiphishing.org/report_phishing.html/

[4] Xinpeng Zhang, ," Cantina Anti-phishing" , IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012

[5] http://www.us_cert.govinavireport_phishing.html//.