Browser Enhancements Against Phishing Attacks

Rohin Dabas
rdabas@andrew.cmu.edu

Adrian Perrig
adrian@ece.cmu.edu

Gaurav Sinha
gsinha@andrew.cmu.edu

Dawn Song
dawnsong@cmu.edu

Chieh-Hao Yang
chiehhao@andrew.cmu.edu

Ting-Fang Yen
tyen@andrew.cmu.edu

Carnegie Mellon University
Pittsburgh, PA 15213

ABSTRACT

Web phishing is a form of social engineering attack that forges legitimate websites. In this paper, we present several mechanisms for detecting such attacks by incorporating several checks into the Mozilla Firefox browser, including URL-Certificate match and Hash Visualization, as well as examining the browser URL encoding for IDN URLs. Our experiments show that these mechanisms successfully detect several common attacks, such as websites forged using Javascript and misleading URLs, and the recent IDN phishing attack.

Keywords

phishing attack, hash visualization, webpage validation

1. INTRODUCTION

Web phishing attacks forge legitimate websites to trick users into disclosing information or to accept untrusted data. These attacks can be very hard to detect, since the forged page can look indistinguishable from a real one [6]. One kind of phishing attack even takes advantage of IDN (International Domain Name) URLs [3], which allow non-English characters to be used in domain names, to cause the displayed URL to be different from its actual form [1].

In this paper, we present a web phishing detection tool that implements web validation checks for SSL secured connections and that also detects possible IDN phishing attacks.

The web validation checks performs a URL-Certificate match, which examines the URL value and the name on the server certificate to see if they refer to the same webserver. The fingerprint on the certificate is then used to generate unique structured images, called Hash Visualization [4], that help users identify trusted websites.

The tool also detects IDN phishing attacks by intercepting browser encoded URLs and using UTF8-to-ACE transformation to detect those that use IDN. The user is warned against a possible attack on IDN URL discovery, as shown in Figure 1.

Our mechanism successfully detects web phishing attacks that forge the appearance of legitimate websites and those that use URL rewriting.

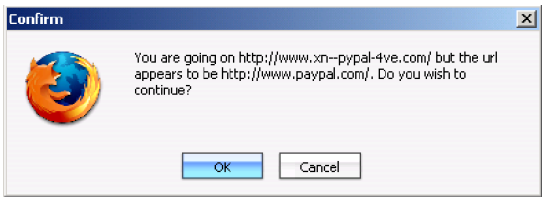

Figure 1: Warning Window

2. DESIGN AND IMPLEMENTATION

We chose to build our tool on the Mozilla Firefox browser, because it is open source and has good documentation.

2.1 Web Validation

Each time a SSL secured page is loaded, our tool examines the value in the URL bar to see if it contains the server name on the certificate as a substring. If it does, a smiley face icon is displayed above the menubar, along with a text string specifying the certificate information. Otherwise the text string says "Website not secured".

Our tool also generates a Hash Visualization from the fingerprint values on the server certificate. The basic idea is to use the fingerprints to construct a random expression that describes a function, mapping each image pixel to a color value. The resulting random image is unique for each certificate fingerprint, even one bit of difference would create completely different outputs. More information on Hash Visualization can be found at [4].

Displaying such hash visualization images on the browser helps the user identify trusted webservers and detect phishing attacks that use forged certificates, since humans are good at recognizing images.

2.2 IDN Phishing Detection

For IDN phishing attack detection, we enable the IDN support in Mozilla Firefox, disable punycode display of URLs, and overlay Firefox's navigation handling functions with our custom implementations.

Firefox uses UTF-8 [2] rather than simple ASCII character

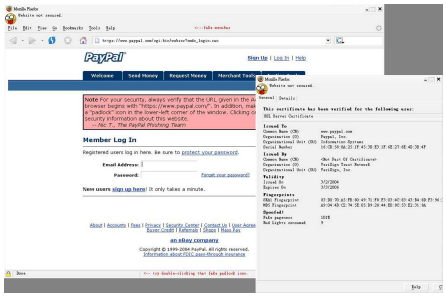

Figure 2: A spoofed webpage as detected by our tool

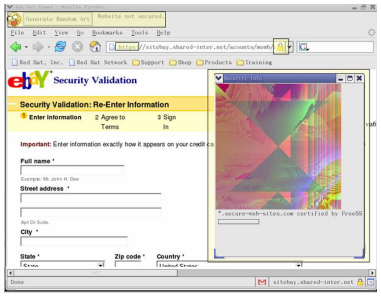

Figure 3: A webpage with fake certificate as detected by our tool

set to display and format URLs. Our tool intercepts the UTF8 encoded URL and determines whether it is an IDN URL by using UTF-to-ACE transformation. ACE (ASCII Compatible Encoding) is a way for the Domain Name System to accept non-ASCII characters or non-Latin scripts by encoding an ASCII representation of a UTF8 word. For example, the French word "dsaronn" would be translated into "xn–dsaronn-xxaoh" in its ACE form. The Domain name to be registered would then be "xn–dsaronn-xxaoh.tm". And the Japanese word for "name" would be "xn–r8j7cuc".

On intercepting an IDN URL, an alert window is displayed which shows both the IDN URL as well as its punycode representation. The user then can decide whether or not to continue browsing the suspicious webpage.

3. EVALUATION

We tested our tool on several web phishing attacks, including the one described in [7]. We were able to successfully detect IDN phishing attacks [1] [5] and other attacks using forged webpages and fake SSL certificates.

Figure 2 shows the detection of a webpage spoofed using screen shots and Javascript. Figure 3 is the detection of a spoofed webpage with a fake certificate. Figure 4 is the image of the real Ebay website with the legitimate certificate. Note the page validation information above the browser menubar that is different for validated webservers.

The security of these checks is based on the fact that the checks are performed and displayed by the client-side browser. The graphical icons in our tool are placed above the menubar, which cannot be disabled like other icons in the toolbar or menubar, and the Hash Visualization images cannot be

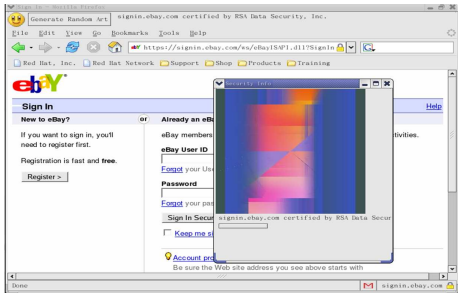

Figure 4: The real Ebay website

forged without breaking the hash preimage-resistance property.

4. CONCLUSION

This paper addresses the problem of common web phishing attacks by implementing browser enhancement mechanisms in Mozilla Firefox. We succefully detect spoofed webservers with forged certificates or URL rewriting attacks such as the IDN phishing attack.

Most of these attacks were made possible by inherent browser design properties and do not have a trivial solution. Our tool at least provides explicit information about the webpage to the end user, and also assures them that possible phishing attacks could be detected.

5. REFERENCES

[1] T. S. Group. The state of homograph attacks. http://www.shmoo.com/idn/homograph.txt.

[2] D. Inc. http://www.ddbcinc.com/askDDBC/topic.asp/TOPICID=1328.

[3] NIC.sh. http://nic.sh/idnfaq.html.

[4] A. Perrig and D. Song. Hash visualization: a new technique to improve real-world security. 1999. International Workshops on Cryptogrpahic Techniques and E-Commerce, CrypTEC.

[5] S. Systems. http://secunia.com/.

[6] E. Z. Ye, Y. Yuan, and S. Smith. Web spoofing revisited: SSL and beyond. Technical report tr2002417, February 2002.

[7] Z. E. Ye and S. Smith. Trusted paths for browsers. Technical Report TR2002-430, Dartmouth College, Computer Science, Hanover, NH, May 2002.