

Project Proposal: Anti-Phishing Plug-in

by Dmitry Denisenko for ECE 1776

September 24, 2006

Introduction

Phishing is the act of trying to fraudulently acquire sensitive information by masquerading as a trustworthy person or business in an electronic communication [1]. Recently, a particular type of phishing became very popular: websites that fool users into thinking they are a popular website, such as a bank or an online retailer, to obtain user's passwords. This project will involve the development of Firefox browser plug-in that will identify a phishing website when one is visited.

Current Anti-Phishing Methods

The number one anti-phishing method is education. Large banks and retailers have been continually educating their users not to trust any emails or phone calls that request personal information such as user names and passwords. To augment that, many have developed a two-factor authentication mechanism (e.g. ING Direct's "We know It's You / You Know It's Us" method [2]). These mechanisms allow the user to establish the identity of the website before giving it any confidential information.

In addition, there has been some technological advancement by software vendors. Microsoft's Internet Explorer 7 browser comes with anti-phishing plug-in. The plug-in taps into a continually-updated database of phishing websites and warns the user if the browser is directed to one of them. [3]

The Google Toolbar, available for Internet Explorer and Firefox, comes with a "Safe Browsing" feature. Part of the Safe Browsing warns the user if a phishing site is visited. It also accepts feedback from users containing suspected phishing site. The phishing detector works by "combining advanced algorithms with reports [...] from a number of sources" [4]. Unfortunately, a more detailed description of the algorithms or the sources could not be found.

Scope and Limitations

For this project, we will limit our scope to writing a Firefox plug-in that will detect if the currently visited site is likely to be a phishing site. We will use Google as a reputation system, checking if the current site is the most reputable site to visit given the site's content. This will be done by querying Google with some selected phrases from the site and checking if the current site comes up as one of the top hits.

We believe that this is the first publicly available purely algorithmic approach to phishing site detection. Of course, others will be available from other groups in the course by the time the project is complete.

A large part of the project will be spent perfecting how to query Google to establish a site's reputation. Considering that even Google uses reports "from a number of sources" to detect phishing, a purely algorithmic approach will most likely not give perfect results. Nevertheless, we will try to measure effectiveness of the algorithmic approach (by itself, and compared to other phishing detectors) and understand its limitations. The limitations will most likely come from two sources: limitations of our queries to Google, and limitations of Google's ranking system itself.

Not all kinds of phishing can be detected by the proposed plug-in. DNS server spoofing and cross-site scripting are two examples [1]. Time-permitting, these and other security attacks might be handled as part of the project.

References

1. *Phishing*, Wikipedia, <http://en.wikipedia.org/wiki/Phishing>
2. *New Secure Login*, ING Direct, <https://secure.ingdirect.ca/INGDirect.html?command=displayLearnMoreStepOne>
3. *Anti-Phishing Home*, Microsoft, <http://www.microsoft.com/mscorp/safety/technologies/antiphishing/default.msp>
4. Google Toolbar Help, Google, <http://www.google.com/support/toolbar/bin/static.py?page=features.html&v=2.0f>