Security through diversity, an approach to browser security.

Andrew Kampjes

Supervisors: Tony McGregor, Peter Gutmann.

March 23, 2012

Abstract

Users of browsers are being fooled into giving away confidential data to malicious websites. Existing techniques are inadequate. I propose a system combining multiple heuristic techniques to help protect users of the internet.

Introduction

Phishing is a massive world wide problem on the internet. Phishing is when attackers build websites which look like a trusted site to gain a users credentials and private information. These websites cause between 2 billion and 3.2 billion of losses every year to users and the credit companies backing them [2] [5]. The current security proposition for users is to trust all sites that are SSL secure. Anything with a SSL certificate in their browsers trust chain is considered safe and trustworthy regardless of whether this is actually the case REF. This is demonstrated by the ease of which disreputable websites are able to get certificates[4]. Another factor is also the Certificate Authority's security which, when compromised allows arbitrary SSL certificates to be created. Users shouldnt have to rely only on a SSL cert to know if the site theyre visiting is where they really want to be. We need a new security value preposition, one that takes into account how risky a site is deemed to be. I plan to create security through diversity by using multiple heuristic techniques to alert users to possible phishing attempts.

Background

Existing phishing protection utilises blacklists almost exclusively with very hit and miss results. The idea of security through diversity is that there is to diversify defenses so there is no single point of failure. A combination of features should make the attacker's task much more challenging. There exist a number of security addons for browsers, addons for Firefox such as Certpatrol[1] and Perspectives[2] that add an extra measure of checks to SSL certificates. One example of existing work into a heuristic approach to detect phishing is CANTINA+[3], an extension of CANTINA[1].

Planned Approach

1. Read some more papers and create a list of phishing detection methods, either existing or original.

2. Create an environment for testing, consisting of a client, a proxy[3] and a malicious server.

3. Find a sample of phishing websites to test against, these will probably

[1] https://addons.mozilla.org/en-US/firefox/addon/certificate-patrol/
[2] https://addons.mozilla.org/en-US/firefox/addon/perspectives/
[3] probably squid, http://www.squid-cache.org/

need to be from archives of such sites and will be probably offline for testing.

4. Take existing phishing detection methods and original phishing detection methods and test effectiveness off each of them against sample websites.
5. Combine techniques using some weighting to decide the chance of a site being a phishing site.
6. Options for extensions involve useability studies or deployment in a real world environment.

Resources

I will require either physical or virtual machines on a network, with the malicious server being able to run Windows XP, Windows 7, Windows server, Linux.

Evaluation

Results will be compared to results in the recent CANTINA+ system[3], both overall and also compared to any original techniques that are created. Usability and accessibility of any software created should also be tested.

Conclusion

I will graduate with honours and also hopefully learn something along the way. If I'm good I'll give a talk at the kiwicon hackers conference this year[4].

References

[1] *Cantina: a content-based approach to detecting phishing web sites*, 2007.

[2] *Examining the impact of website take-down on phishing*, 2007.

[3] Guang Xiang Jason Hong Carolyn P. Rose Lorrie Cranor. Cantina+: A feature-rich machine learning framework for detecting phishing web sites. *TISSEC*, 12(2):28, 2011.

[4] Peter Gutmann. An embarrassingly simple solution to the problem of protecting browser users, 2011.

[5] T McCall. Gartner survey shows phishing attacks escalated in 2007; more than $3 billion lost to these attacks, 2007.

[4] https://kiwicon.org/