PhishZoo: An Automated Web Phishing Detection Approach Based on Profiling and Fuzzy Matching

Sadia Afroz    Advisor: Rachel Greenstadt, Department of Computer Science, Drexel University

The Phishing Problem
Phishing is a web-based attack that uses social engineering techniques to exploit Internet users and acquire sensitive data. Most phishing attacks work by creating a fake version of the real site's web interface to gain the user's trust.

Motivations
- Over 90% users depend on a website's appearance as an indication of its authenticity.
- Users ignore web browsers indications
- The majority of users provide sensitive credentials to a small set of sites (fewer than 20)

Goals
- Use visual elements of a site to detect potential phishing attacks.
- Prevent targeted attacks on sites important to a user

Profile matching
Profile matching with SSDEEP:
Compute hash values of each elements using SSDEEP
Match hash values against the hash values of profiles

Profile matching with SIFT and HtmlParser:
Parse visible text from site's html
Find edit distance with profile html
Calculate match score = edit distance length of real text + length of phishing text

Results summary
- PhishZoo works best on phishing attacks those look similar to real sites.
- When we add phishing profiles results have high accuracy and low false positives
- Results comparable to best of breed black listing approaches with the added benefits of detecting new and targeted attacks

Performance analysis
- On a typical end-user machine (32 bit, 2 GHz processor running Windows Vista with 4 GB Ram) profile matching with SSDEEP is shown. Most users will have 20-30 profiles so matching time will be approximately two seconds. More matching could be done in an offline system that just looks at links in a mail spool.
- Profile matching with SIFT and HTMLParser takes 10 seconds

Conclusion and Future work
- Approach works well against current phishing attacks.
- Phishers may use screenshots of the real site instead of html code. SIFT can be used but we need to improve speed and precision.
- Work on methods to safely detect phishing sites that infect visitors.

Goals
- Over 90% users depend on a website's appearance as an indication of its authenticity.
- Users ignore web browsers indications
- The majority of users provide sensitive credentials to a small set of sites (fewer than 20)

Approach works well against current phishing attacks.
- Phishers may use screenshots of the real site instead of html code. SIFT can be used but we need to improve speed and precision.
- Work on methods to safely detect phishing sites that infect visitors.