IronFox: Securing the Web

Stephen McMurtry & William Johnson | Khadija Stewart (Advisor) | DePauw University

State of the Internet

Web browsers allow us to access the resources of the Internet, but they are inherently trusting and expose users to unnecessary risk.

The Price of Insecurity

- $100B lost yearly to cyber crime
- 10M identities stolen every year
- Only 30% of the Internet's top 100 sites encrypt their connections
- Secure connection schemes are not always secure (Heartbleed, Shellshock)

Overview

Our project consisted of performing a security audit of today's most popular web browsers and creating a secure web browsing option for the less technical users. The first part of our project consisted of studying and analyzing the security features of today's top browsers. We then identified and studied the most common cyber vulnerabilities. We determined that the studied browsers are still vulnerable to these attacks and decided to use Mozilla Firefox's open source code to assemble and package a more secure browser. We researched and identified security features and extensions that combat the most common vulnerabilities and expanded the functionality of Mozilla Firefox with these add-ons, creating the IronFox browser.

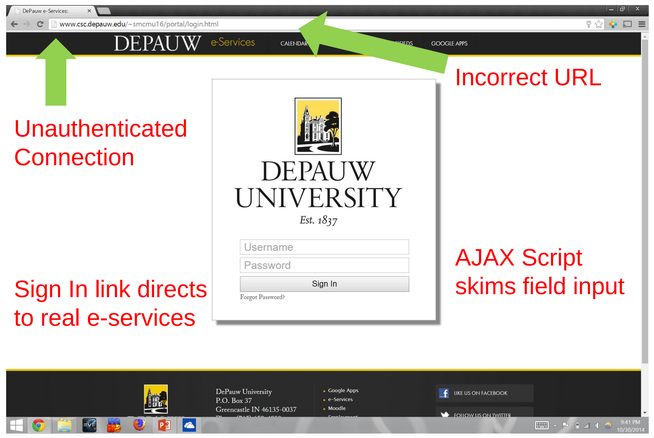
Common Network Vulnerabilities

- Cross-Site Scripting
  - Clickjacking
  - Cookie Hijacking
- SQL Injection
  - Buffer Overflow
- Man-in-the-Middle
- Phishing & Pharming
- Distributed Denial of Service (DDoS)

E-Services Phishing Attack

Our first order of business was to conduct a browser-based attack in the wild. We set up a counterfeit e-services login page that used an AJAX script to surreptitiously record the username and password that were input into the text fields. That information was stored in a file for collection and later analysis. The only indication that the page was malicious comes from a careful reading of the URL. An astute user would have noted that the connection to Stephen's personal e-services page was not secure. Most users, however, would click right on through and be directed to e-services as if nothing had happened.

The Attack Site



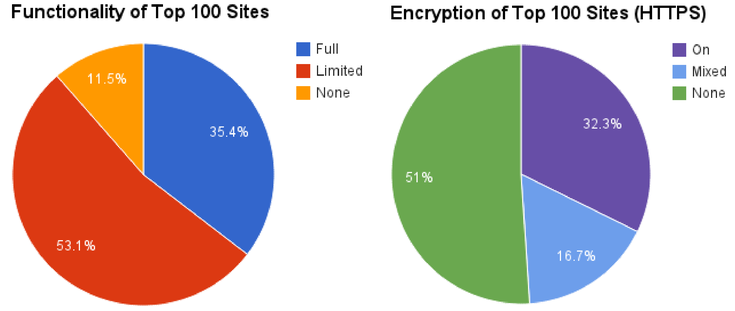
Creating IronFox

In order to combat the most common web vulnerabilities, we packaged a version of Firefox that includes a number of security-focused extensions.

- HTTPS Everywhere/HTTPS Finder - Use a dynamic whitelist to force secure connections on websites that support it.
- LastPass - Stores passwords in an encrypted cloud instead of in plaintext on local machine.
- AdBlock Plus - Prevents malicious ads.
- NoScript - Blocks scripts and requires a whitelist to let them run.

We took this modified distribution of Firefox for a spin on the top hundred websites to test its functionality. Most sites were usable, but lacked some dynamic content. Only a minority of sites were completely inoperable.

Browsing in the Wild



Results of usability tests on the top 100 sites

Conclusion

Although popular web browsers offer rudimentary security measures, these measures are often opt-in, requiring users to police their own browsing behavior. While this may prove sufficient for a knowledgeable user, it leaves novice technical users at risk. Our browser, IronFox, activates a number of secure settings by default, making it more difficult for the novice user to accidentally reveal sensitive information to malicious entities.

Further Research

Stephen McMurtry and Tao Qian are continuing development of IronFox by developing a free and open source (FOSS) Firefox extension that will mimic the functionality of NoScript and implement a recommendation engine that will aid users in whitelisting purportedly trustworthy scripts. Usability testing and deployment will follow in the near future.

Acknowledgements

We would like to thank the National Science Foundations (NSF) and the Science Research Fellows (SRF) for funding our research. We would like to thank the DePauw Computer Science Department for hosting the Research Experience for undergraduates (REU). We would like to thank our advisor Khadija Stewart for guiding our research. And we would like to thank the Mozilla Foundation for their continuing development of an open source browser.

This work was supported by NSF grant number CNS-1156893