Exploring the removal of centralized authories from SSL

Douglas Anderson[a], Eric Boyd[b], James Kelly[c]

[a] *dander01@uoguelph.ca*
[b] *boyde@uoguelph.ca*
[c] *kellyj@uoguelph.ca*

Abstract

So abstracts are pretty cool and stuff. Good ones have information about the project. This one does not.

Keywords: Security, SSL, Central Authorities

1. Introduction

In the modern world the Internet holds a very important role in commerce and social aspects of life. Both of these pursuits require the ability for two or more parties to communicate securely. To facilitate this secure communication, the Internet has resorted to using the SSL (Secure Socket Layer) and it successor TLS (Transport Security Layer) to protect the data being exchanged. These protocols utilize public-private key pairs to facilitate RSA encryption. While this protocol has been extremely successful it must rely on a central authority to confirm the identity of the owner of public keys. This central authority is a single point of failure in this authentication system, and has in the past been compromised, allowing successful impersonation of several popular, high profile websites.

In 2011 the central authority Comodo was hacked and the hacker made off with a SSL certificates for various sites including Gmail, Yahoo Mail,

Hotmail. [1] This would allow the hacker to preform man in the middle attacks on the sites and read the emails of users of these services. The attack was easily executed because of Comodo's extremely weak password that was easily broken with a word list. This illustrates the vulnerability in the SSL protocol that central authorities create.

2. Background

3. Method

For our project we attempted to build upon the Perspective Project by allowing servers to send messages to notaries requesting that the notary make note of the change of SSL certificate. This fixes the problem in the perspectives project that can occur when a server changes it's SSL certificate and a user queries the notary for that server's SSL certificate. Because the notary has not yet updated it's record of the SSL certificate and reports to the user that there is a mismatch which may lead the user to abort their attempt to create an SSL connection.

4. Results

5. Conclusion

6. Further Work

7. References

[1] Peter Bright. Independent iranian hacker claims responsibility for comodo hack, 2011.

[2] David G. Andersen Dan Wendlandt and Adrian Perrig. Perspectives: Improving ssh-style host authentication with multi-path probing. *Usenix ATC*, 2008.