W3C Workshop on Declarative Models of Web Applications,
Dublin, Ireland
5-6 June, 2007

Trusted Mobile Browsers

Anil Saldhana
Red Hat Inc
Anil.Saldhana@redhat.com

Introduction

Even with the rapid proliferation of usage of mobile devices, it is undeniable that mobile web browsing has not gained major traction. The reasons may be plenty. A recent news report [1] confirms that the mobile browsing has not caught up with technical advances in mobile telephony. According to the report, software used for mobile browsing is limited in nature and not suitable for usage at par with regular web browsing. I am sure that with increasing reliance on the internet and necessities on the move will increase an adoption rate in mobile browsing.

Trusted Mobile Browsers

To increase the adoption of mobile browsing, there is a need to both simplify the browser as well as making the user do less. The users can deal with bandwidth issues because that is something under their control. The greater the costs, the better the bandwidth. The mobile browser complexity is not in the user’s control. He is at the mercy of technology and vendors. This is where standards play an important role in simplifying the complexity of web browsing by moving all intelligence into the browsers, the network and the back-end server applications that the browser is interacting with. The user will have to do very little.

Assuming that the browser has become ultra intelligent, there is still the concerns for privacy and security in the minds of the user. The browsing exercise should dispel all fears of security for the user. This is possible when the browsers are built with security by default.

There are 3 areas where the user will be concerned about security and privacy. One is the browser itself, the other is the channel where data flows from the browser to the server and the last is the server application. Since the server application is not specific to mobile browsing alone, we can ignore it in this paper. The browser can be solidified such that security is enforced.

The critical concern that remains is the channel. Given the costs and computing capabilities of mobile devices, I feel that Public Key Cryptography using X509 certificates for the mobile browser is overkill. There is a need to identify alternatives to mutual authentication using certificates. One such alternative is the Secure Remote Password [2][3].

The views expressed in this Position Paper are of the author alone and do not necessarily reflect the views of the author’s employer or any other party.

Secure Remote Password

The Secure Remote Password [SRP] is a mechanism where in the key agreement between the client and server is mathematical based and derived out of a simple password entered at the client. Essentially, it drives out the man-in-the-middle concerns.

The SRP capabilities can be inbuilt into the mobile browsers. For secure sites where the user intends to do business, if PKI is a concern, then the user can enter a password to the site and the browser can perform SRP computations to agree on a secret key with the server and ensure a secure channel.

Conclusion

The need for simplified and intelligent mobile browsers is important for the success of the mobile e-commerce industry. In this paper, I have also highlighted the need for trusted browsing that is inbuilt in the browser with SRP technology.

Reference

[1] *'Mobile Browsers Still Closed for Business'*, Matt Hines, (http://www.eweek.com/article2/0,1895,1920439,00.asp)
[2] Secure Remote Password (http://en.wikipedia.org/wiki/Secure_remote_password_protocol)
[3] Secure Remote Password (http://srp.stanford.edu/)

About the Author

Anil Saldhana is the Project Lead for JBoss Security and Identity Management, JBoss Division, Red Hat Inc. He represents JBoss/Red Hat at the JCP, W3C and Oasis standards organizations. He is also an active member of the Apache Program Management Committee for Web Services at the Apache Software Foundation. He speaks frequently at conferences on topics related to security and software.

The views expressed in this Position Paper are of the author alone and do not necessarily reflect the views of the author's employer or any other party.