Web Authentication Today and For Tomorrow

Position paper for the
W3C Workshop on Transparency and Usability of Web Authentication
New York City, March 2006

Shivaram H. Mysore

Microsoft Corporation
One Microsoft Way, Building 27/2099
Redmond, WA 98052
USA

smysore@microsoft.com
http://blogs.msdn.com/shivaram/

Introduction

This paper attempts to illustrate some common problems associated with Web Authentication today and then provide some directions to form a basis for a dialogue on how we can attempt to address this problem.

Web Authentication: Today

Today, the following are some usage scenarios by which users authenticate to get access to protected content:

1. Web Browser based – Username-Password, One Time Password, and Knowledge based (your favorite color, your pet name, high school, etc) are the most common authentication mechanisms
2. Virtual Private Network (VPN) – Username-Password, Certificates (IPSec, TLS/SSL), One Time Password and Radius server based authentication are most common authentication mechanisms
3. Web Services – Username-Password and Certificates are the most common authentication mechanisms

There are two major classes of issues that we deal with: Technological and User perspectives.

Username-Password requires the least amount of infrastructure and is also easy to implement. Over a period of time, the usage has permeated extensively and many network infrastructure components have optimizations to accommodate this kind of authentication. One such example is the use of authentication credential caching by caching servers at the edge so that protected content can be provided to authenticated users without requesting the same from backend servers. Passwords are also common amongst generic user population which necessitates management tools like, password provisioning, recovery, and de-provisioning. These management tools use additional Knowledge based authentication mechanisms. A majority of the user population require access to protected content from un-trusted and un-managed networks and machines. One time passwords are commonly used when accessing protected content from un-managed machines as there are few requirements for additional software.

Certificate based authentication is preferred for accessing protected content from un-trusted networks. But, provisioning and carrying Certificate based credentials have been a problem so far thus limiting its usage and effectiveness. Even on a user machine, there are numerous key stores and hence key management is a huge problem for the end user and even for application usability and compatibility. For example, on a Windows machine, there is the Windows key store, a browser (Firefox, Opera, etc) has its own key store, Java virtual machine has its own, and if there are any server applications (Web and

Application servers), they require additional key stores. All of these are problems and frustration for the user to manage keys in addition to user education by Application vendors on how to provision the keys with their proprietary wizards.

Phishing and Pharming are the latest set of threats for users trying to safeguard their credentials and identity.

Usage tracking and advertisements have become the business models for most Internet companies. It has to be noted that not all the companies have the same standards in terms of guarding the data that is accumulated. This has been demonstrated with the loss of credit card and other personal information of many users by some of the Internet companies.

Privacy has become another major issue as the companies try to collect more information than needed from the user in the hope of creating a new revenue stream.

Suggested Directions for the next generation of Web Authentication

1. Consider what principles might govern use of personally identifiable information collected for usage tracking
2. Deprecate username/password authentication due to its demonstrated weaknesses and replace with digital credentials and secure tokens (ex. Smart Cards, InfoCard, etc). When selecting a digital credential, the life cycle management of the same should also be well thought through.
3. Use of Reputation Service (IE7) and Secure DNS like mechanisms to make more networks and web destinations secure and trustworthy. If there is a way that a user can trust that the network that he is connecting to is safe, the servers can provide better service to the user.
4. Use of Smart Card based technology for credentials at least for enterprise customers. This should also help consolidate the key stores on the operating system and can also help in roaming of credentials securely.
5. Use of federated model for Authentication.
6. Security should be built-in – not an optional component. If service providers start forcing users to use strong authentication (ex. mutual TLS/SSL authentication), the usage rate will increase.
7. Certification of Service Providers to make sure that data gathered is stored securely and used appropriately.
8. Use of device authentication mechanisms to securely collect strong digital credentials (Ex. finger print from a finger print reader, entering a PIN into a Smart Card reader to unlock the card, etc.). This is very important as the Web Authentication means that authentication is possibly happening at OSI's Application Layer (Layer 7), but, the credentials could be natively collected from the system. Transferring the credentials securely from the native layers in the operating platform to the remote server over Layer 7 is a challenge. The need for so many of the parts on the client side (ex. browser, reader, digital credential token, PIN to unlock the token, additional software required, say, drivers, etc) pose huge usability problems.
9. User Education. It is not enough for service providers to say – "you can check your statements online", but, provide meaningful ways (what should users look for on a screen, how to logon, etc) in demonstrating how this can be done.

