A Vision for Browser-Assisted Web Authentication

Siddharth Bajaj & Slawek Ligier
Symantec User Authentication
Observations & Key Concepts

• Issues with Passwords
  – Too many passwords, users use same passwords, password policies don’t work.

• What works today: ATM Authentication
  – Combines possession factor (ATM card) with knowledge factor (4-digit PIN)
  – High Security without compromising security

• OpenID, etc. help but don’t completely address problem
  – You still need to authenticate to your OpenID/SSO provider.

• Separating Authentication (credentials) from Identity
  – Enables use of ‘anonymous’ device or ‘browser’ credentials
Separating Authentication (credentials) from Identity

- Enables use of ‘anonymous’ device credentials for auth.
- Credentials bound to user identity through a ‘registration’ workflow.
- Credentials
  - Based on user’s access device e.g. Browser-based
  - Token-based (OTP & USB tokens).
Browser Assisted Web Authentication

• ATM card analogy for the Internet
  – Browser based Device ID (Web-ID), similar to the ATM card is ‘something you have’
  – 4 digit PIN is ‘something you know’.

• Suggest using PKI ‘under-the-hood’ to implement Web-ID
  – High security, standard-based, widely deployed and proven technology
  – Create a focused ‘Profile’ of PKI for Web-ID use-case
    • Automate the lifecycle and usage based on policies
    • Consistent implementation across browsers
References

• Full paper:

• Authors
  – Siddharth Bajaj (siddharth_bajaj@symantec.com)
  – Slawek Ligier (slawek_ligier@symantec.com)