Single Sign-On Architectures

J. De Clercq, “Single Sign-On Architectures.” In G. Davida et al. (eds.): *InfraSec 2002*, LNCS 2437, pp. 40-58, 2002.

Presented by Luo Zheng Yuan

Summary

- This paper focus on introducing a variety of different Single Sign-On architectures (SSO) available when designing SSO solutions for organizations with different sizes and needs.
- This paper also give brief introductions to some SSO-enabled applications used in real business.

Appreciative comment(1)

- Besides introducing the technical details of SSO architectures, the author gave some interesting backgrounds to help us know “the whole story”.

- What is SSO?

  “The Open Group defines SSO as the mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords.”

- Why SSO?
  - “A study conducted by the Network Applications Consortium (http://www.netapps.org) in large enterprises showed that users spend an average of up to **44 hours per year** to perform logon tasks to access a set of 4 applications.”
  - The same study measured the content of the calls to companies’ helpdesk: **70 per cent of the calls** were password reset requests.

Appreciative comments (1) (continue)

- Why not SSO?
  - “An often heard argument against SSO is that SSO credentials are the “key to the kingdom”. If one can obtain the SSO credentials he gets access to all resources secured by them.”

Appreciative comment(2)

- For each architecture presented in the paper, at least one concrete application of the architecture is given.
- Improve reliability of the paper.
- Encourage readers to read more.

  - Token-based SSO systems
    - "**Microsoft** has implemented Kerberos as the default authentication protocol of **Windows 2000**."
    - "**CyberSafe** sells plug-ins that can be used to enable an operating system platform to generate, understand and validate Kerberos credentials."

Appreciative comment(2) (continue)

- Secure Sever-Side Credential Caching
  - "Examples of secure server-side credential caching SSO systems are **IBM's Tivoli Secureway Global Sign-On**, **Computer Associates eTrust** and **Vasco's SnareWorks Secure SSO**"

Table 6. Secure Server-side Credential Caching SSO (non-exhaustive list)

Secure Server-side Credential Caching SSO	
IBM Tivoli Secureway Global Sign-On	http://www.ibm.com
Computer Associates eTrust	http://www.ca.com
Vasco SnareWorks Secure SSO	http://www.vasco.com

Critical comment

- Credential synchronization is classified as SSO architecture dealing with multiple credentials.
- But this is a little bit confused when I read the paper first time, is credential synchronization SSO?

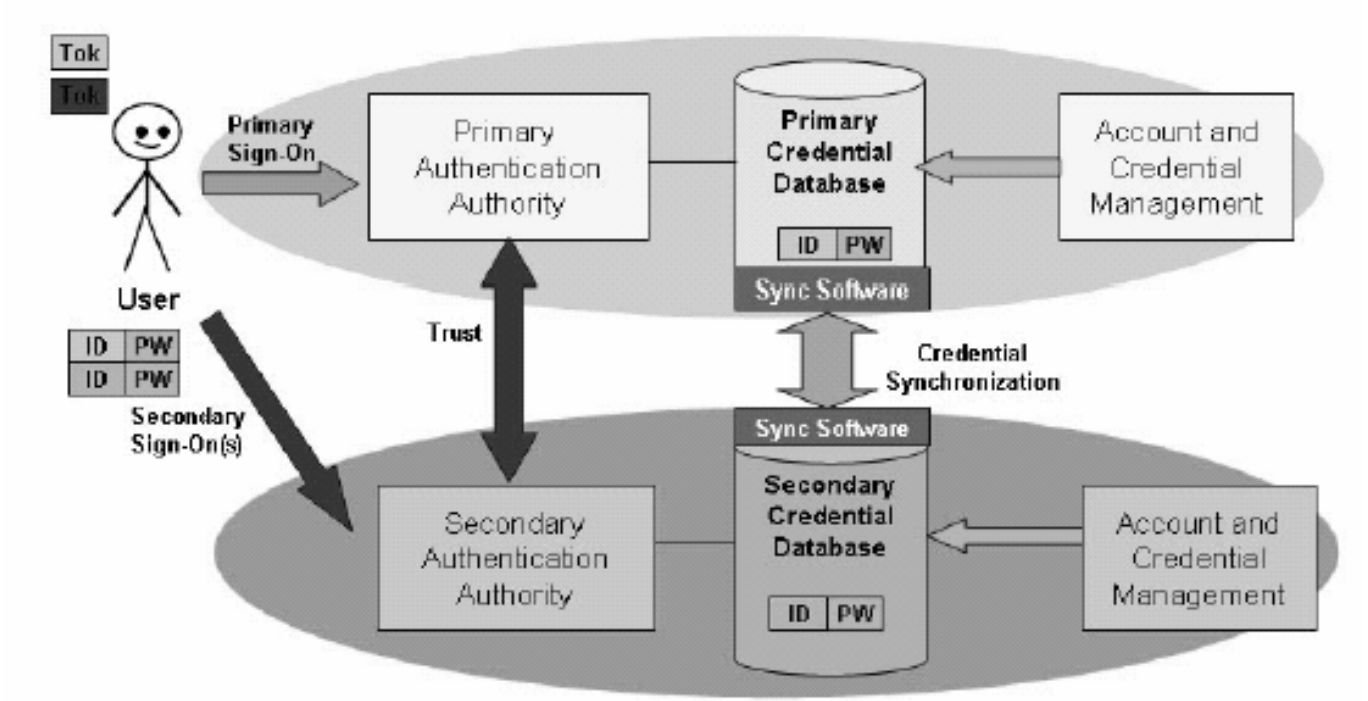

Fig. 6. Password Synchronization-based SSO

Question:

- Would you like Single Sign-on system to be used in university?
  - My answer is yes, because it will help me save lots of time.
  - But since SSO is very powerful, it is also very dangerous, losing your primary credentials could mean that all your secrets are exposed.
  - The complexity of setting up SSO system must be considered by business users.