Single Sign-On Architectures

InfraSec 2002, LNCS 2437, pp. 40-58, 2002.

By: Jan De Clercq

Security Consultant

HP Security Office

jan.declercq@hp.com

Presented by: Zheng Liu

Summary

- This paper describes six Single Sign-On architectures that can be applied to several situations.

Situation	Applied Architecture
Single Authentication Authority, Single Set of Credentials	Simple SSO
Multiple Authentication Authorities, Single Set of Credentials	Token-Based
	Public Key Infrastructure-Based
Multiple Authentication Authorities, Many Different Credentials	Credential Synchronization
	Secure Client-Side Credential Caching
	Secure Server-Side Credential Caching

Summary (cont’s)

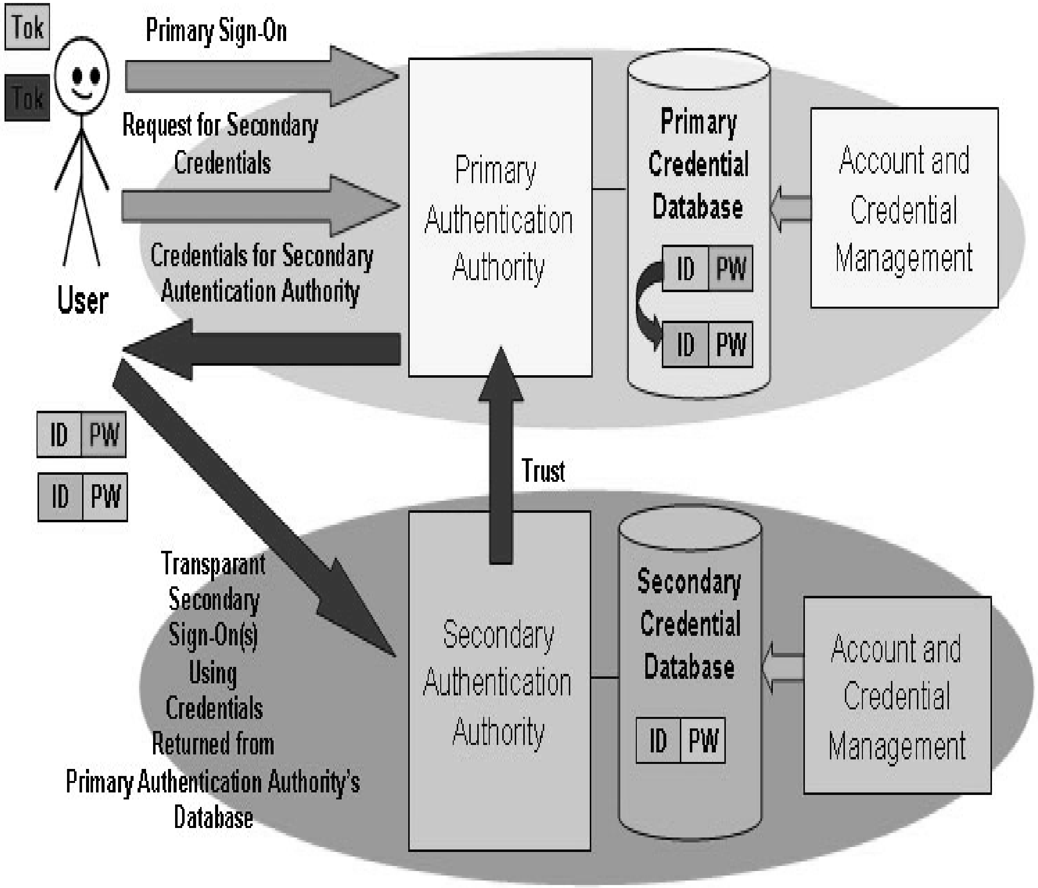
- The paper also introduces the way to extend scope of Single Sign-On system to cover different organizations.

Appreciative Comments

- The author has given a picture of each architecture, and a table to list some software that implemented that architecture. This gives people an intuitive idea of each architecture.

Example of pictures and tables

- Picture and table used for Secure Server-Side Credential Caching:


Tok
Tok
User
Primary Sign-On
Request for Secondary Credentials
Credentials for Secondary Autentication Authority
Primary Authentication Authority
Primary Credential Database
ID PW
ID PW
Account and Credential Management
ID PW
ID PW
Trust
Transparant Secondary Sign-On(s) Using Credentials Returned from Primary Authentication Authority's Database
Secondary Authentication Authority
Secondary Credential Database
ID PW
Account and Credential Management

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

Appreciative Comments (cont’s)

- Explanations of technical terminology, and some words that may cause confusion

Example:

• **Authentication servers** are the physical machines performing the authentication functions.

A big challenge in today’s authentication infrastructures is to extend the SSO scope to cover many “different” authentication authorities. “Different” in this context means: implemented on different platforms and governed by different organizations.

Critical Comments

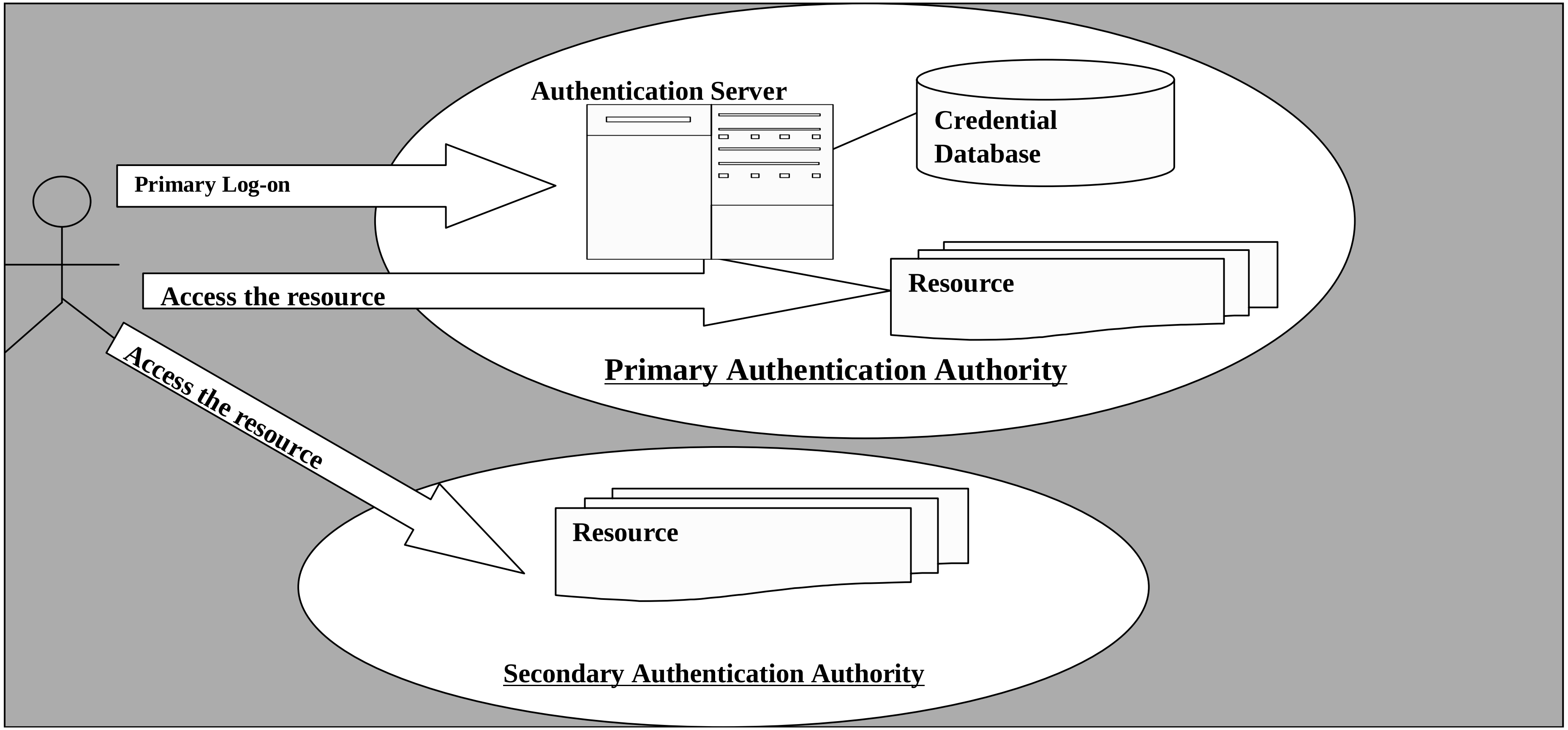
- Author omitted some important negative effect. It may affect the validity of his conclusion on security advantage of SSO.

Availability of authentication service

- Author: there are less chances that users forget or loss their password. This makes SSO increase the availability of the authentication service.

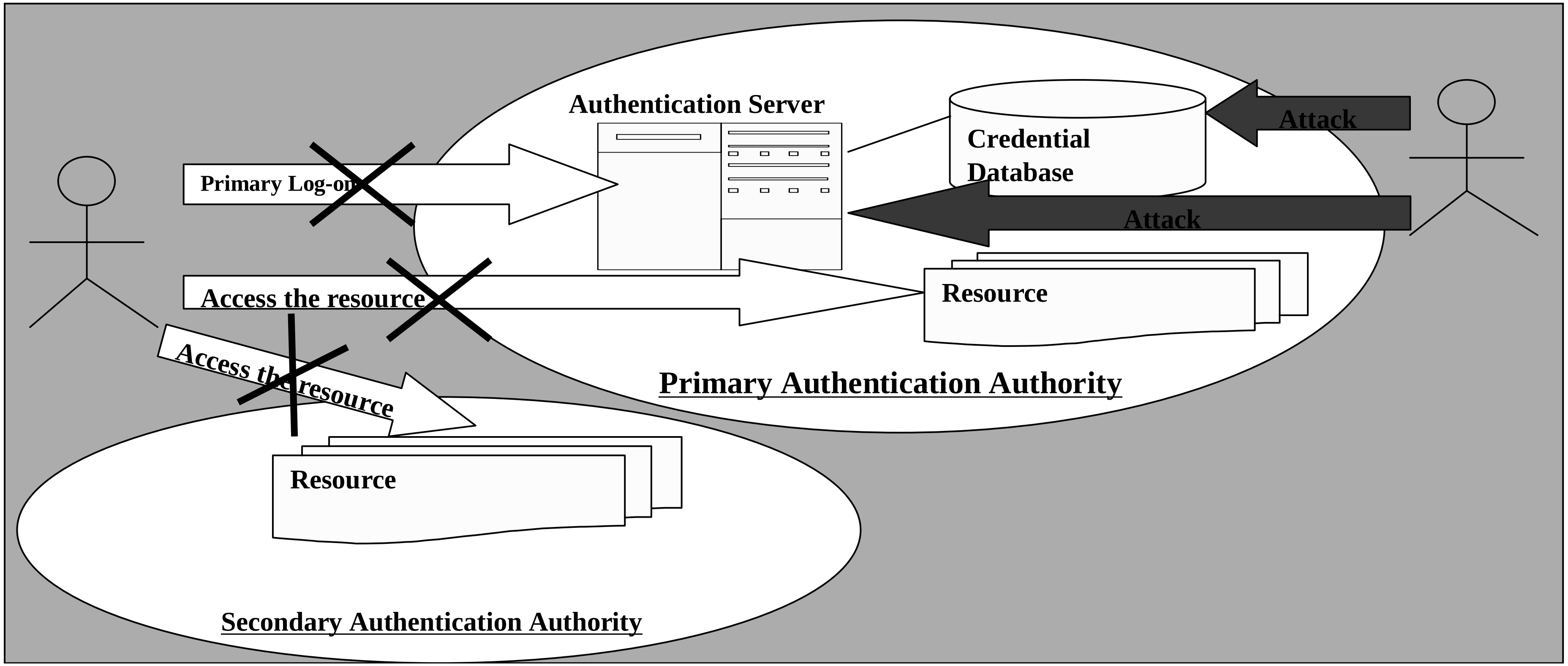
Availability of authentication service (cont’s)

- Primary authentication authority becomes the bottle neck.



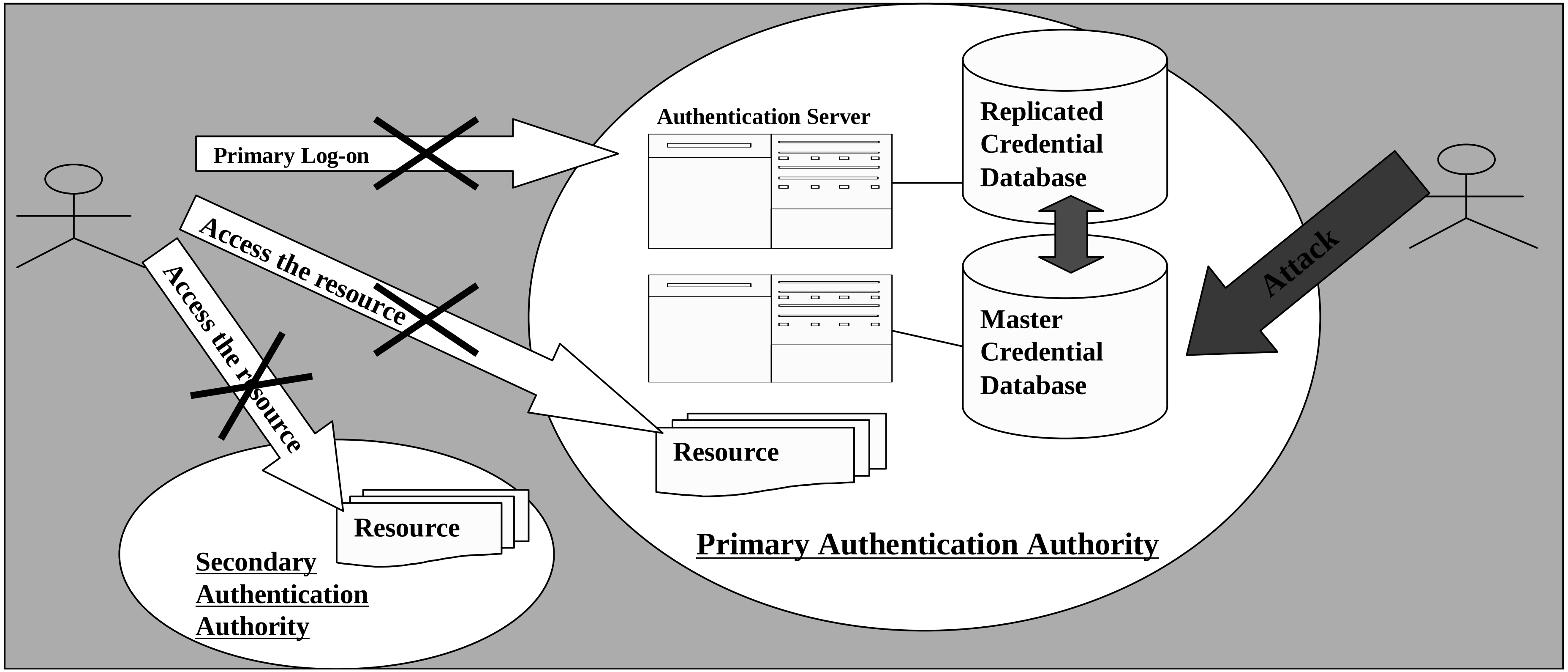
Availability of authentication service (cont’s)

- If the primary authentication authority is down, none of resources is accessible to users.
- Author pointed out that each authority can have several authentication servers and several credential database.



Availability of authentication service (cont's)

- Replication of credential database requires a single-master mode in order to avoid ambiguous user authentication.
- Modification to credentials on master database will affect those on replicated database.


Primary Log-on
Access the resource
Access the resource
Authentication Server
Replicated Credential Database
Master Credential Database
Attack
Resource
Resource
Primary Authentication Authority
Secondary Authentication Authority

Question

- Comparing the positive effect and the negative effect, will you recommend organizations to use SSO?

Thank you