Secure Information Sharing Utilizing Kerberos Authentication

Joseph A LaConte (jlaconte@uccs.edu)
December 11, 2008

Thesis Proposal
Computer Science Masters Degree Program
University of Colorado at Colorado Springs

Committee Members and Signatures:

Approved by	Date
Advisor: Dr. Edward Chow	
Committee member: Dr. Terry Boult	
Committee member: Dr. Xiabo Zhou	

Area of Research

Information security addresses the confidentiality, integrity, and availability of data [1]. Secure Information Sharing (SIS) focuses on guaranteeing the proper permission for accessing data. Specifically, privilege levels for every individual should be managed and enforced corresponding to requested services and data.

This thesis will expand upon previous research in SIS by exploring the Kerberos protocol. Kerberos is a network protocol initially developed by MIT that uses secret-key cryptography to provide authentication between client/server applications [2]. A version of this protocol is used in the Windows Domain environment to authenticate users and provide some services. Our campus utilizes username/passwords for authentication; however, the Windows Architecture "implements extensions to the Kerberos protocol that permit initial authentication using public key certificates rather than conventional shared secret keys," allowing multiple means of authentication [7]. In other words, Windows authentication is not limited to username/passwords, but can be extended to other methods such as smartcards.

The ENforCE HRBAccess system is the chosen environment for the initial SIS solution. Enforce has been implemented under a Windows Service Oriented Architecure (WSOA) [3]. Although the test system will primarily be windows based, the Kerberos protocol is not limited to this platform.

ENforCE uses http sessions to determine if a policy is active [4]. Authentication is achieved using the same http session and a public key infrastructure (PKI) [5]. More specifically, a policy cannot be granted until a user has accessed an http application that authenticates against the user's certificates. In addition, the policy is maintained by continuing the http session. If the browser is closed, the policy will be terminated.

Research Questions

What are the benefits of using an existing authentication protocol such as Kerberos?

The current authentication scheme can be improved both for users and administrators. The thesis will explore this topic further.

Can Kerberos be leveraged for use in the ENforCE solution?

The thesis will explore the use of Kerberos in the ENforCE solution. What role can Kerberos fulfill in this system? How much of the SIS authentication and enforcement responsibilities can this protocol accomplish? Do the results apply to only to this SIS solution? These types of questions will need to be addressed.

What complications arise from this change?

The thesis will discuss the results of this modification.

Discussion

This thesis will explore the use of the Kerberos protocol within the ENforCE HRBAccess solution.

Interfacing with Kerberos, the SIS strategy should be capable of identifying a user. The thesis will explore the possibility of replacing the current use of a public key infrastructure (PKI) and attribute certificates (AC). A related goal is to reduce the maintenance and setup of an SIS solution. The thesis will evaluate the two solutions based on this goal and attempt to identify related assumptions.

One of the major hurdles this thesis will face is the extension of Kerberos, tying this user authentication back into our SIS strategy. The chosen authentication platform will primarily be Windows based since this is the current implementation of ENforCE.

Scope of Thesis

This study will centralize on the use of Kerberos authentication within a SIS strategy. The ENforCE test case will be updated to use this form of authentication. The process of extending and interfacing Kerberos will be documented.

The thesis will attempt to explore and expand on the following:

- An interface between the ENforCE solution and Kerberos authentication.
- The possibility of eliminating the current requirement for a public key infrastructure (PKI) and attribute certificates (AC).

A comparison of the two solutions will be discussed along with a determination of the benefits and complication of this method, concluding the value of this method and if it truly simplifies the solution.

Benefits of Study

The primary benefit of study will be to determine if Kerberos authentication simplifies the existing SIS solution. The current solution requires specific knowledge of the SIS configuration such as the location (url) of the IIS server and the simple fact that the user must establish and maintain a session with this server to be granted access to a resource. A goal of the Kerberos solution is to make the SIS enforcement more transparent to end-users.

If an additional PKI can be prevented, the solution will become more transparent to the end user (by the lack of a required key issuance and management). In addition, this would reduce the maintenance and setup requirements of our solution.

Through the comparison of the two solutions, additional enhancements for future work may be identified. For example, can the SIS strategy be extended to offer a single sign-on (SSO) solution for network-wide applications in addition to the current level of access enforcement (network level versus application level)?

Milestones and Deliverables

Preliminary Schedule	**Milestone**	**Deliverable**
Jan 9, 2009	Additional research about interfacing with and extending the Kerberos protocol.	Part of thesis
Jan 23, 2009	Design of updated ENforCE system.	Documentation
Feb 20, 2009	Implementation of new design.	Demonstration
Feb 27, 2009	Use cases to demonstrate integration of Kerberos.	Demonstration and Virtual Environment
Mar 20, 2009	Analysis of results and concepts.	Part of thesis
Mar 27, 2009	Thesis draft.	Thesis Draft
Apr 10, 2009	Thesis finalized.	Thesis
Apr 17, 2009	Defense	Presentation

References

[1] The Security Practitioner. What is 'Information Security'. 2008 http://security.practitioner.com/introduction/infosec_2.htm

[2] Kerberos: The Network Authentication Protocol. 2008. http://web.mit.edu/kerberos/

[3] Khaleel, Osama and Chow, C. Edward. 2007. ENgine FOR Controlling Emergent Hierarchical Role-Based Access (ENforCE HRBAccess), p 38.

[4] Khaleel, Osama et al, p 48.

[5] Khaleel, Osama et al, pp 9, 28, 39, 52-58.

[6] Godavari, Ganesh and Chow, C. Edward. 2005. Secure Information Sharing Using Attribute Certificates and Role Based Access Control.

[7] Windows 2000 Kerberos Authentication. 2008. http://technet.microsoft.com/en-us/library/bb742431.aspx

[8] Panko, Raymond R. Corporate Computer and Network Security. Prentice Hall. 2004.

[9] Jamsa, Kris. Hacker Proof The Ultimate Guide to Network Security. OnWord Press. 2002.

[10] Smith, Roderick W. Linux in a Windows World. O' Reilly Media, Inc. 2005.

[11] Linn, J. 2000. RFC 2743. Generic Security Service Application Program Interface Version 2, Update 1. http://www.ietf.org/rfc/rfc2743.txt?number=2743

[12] Scherier, W. J. and Boult, T.E. 2008. Ph.D. Dissertation Proposal. Improving the Privacy, Security, and Performance of Biometric Systems. http://cs.uccs.edu/~gsc/pub/phd/wscheire/doc/proposal.pdf