The Development of a graduate course on identity management for the Department of Networking, Security, and Systems Administration

Marsha Mitchell

Follow this and additional works at: https://scholarworks.rit.edu/theses

Recommended Citation

This Thesis is brought to you for free and open access by RIT Scholar Works. It has been accepted for inclusion in Theses by an authorized administrator of RIT Scholar Works. For more information, please contact ritscholarworks@rit.edu.
The Development of a Graduate Course on Identity Management for the Department of Networking, Security, and Systems Administration

By

Marsha Mitchell

Thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Networking and Systems Administration

July 2008

Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences
Rochester Institute of Technology

B. Thomas Golisano College of Computing and Information Sciences

Master of Science in Networking and Systems Administration

Thesis Approval Form

Student Name: Marsha Mitchell

Thesis Title: The Development of a Graduate Course on Identity Management for the Department of Networking and Systems Administration

Thesis Committee

<table>
<thead>
<tr>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charlie Border</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chair</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Luther Troell</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nirmala Shenoy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committee Member</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Development of a Graduate Course on Identity Management for the Department of Networking, Security, and Systems Administration

I, Marsha Mitchell, hereby grant permission to the Wallace Library of the Rochester Institute of Technology to reproduce my thesis in whole or in part. Any reproduction must not be for commercial use or profit.

Date: ___________    Signature of Author: ___________________________
Abstract

Digital identities are being utilized more than ever as a means to authenticate computer users in order to control access to systems, web services, and networks. To maintain these digital identities, administrators turn to Identity Management solutions to offer protection for users, business partners, and networks. This paper proposes an analysis of Identity Management to be accomplished in the form of a graduate level course of study for a ten-week period for the Networking, Security, and Systems Administration department at Rochester Institute of Technology. This course will be designed for this department because of its emphasis on securing, protecting, and managing the identities of users within and across networks. Much of the security-related courses offered by the department focus primarily on security within enterprises. Therefore, Identity Management, a topic that is becoming more popular within enterprises each day, would compliment these courses. Students that enroll in this course will be more equipped to satisfy the needs of modern enterprises when they graduate because they will have a better understanding of how to address security issues that involve managing user identities across networks, systems, and enterprises. This course will focus on several aspects of Identity Management and its use in enterprises today. Covered during the course will be the frameworks of Identity Management, for instance, Liberty Identity Federation Framework and OASIS SAML 2.0; the Identity Management models; and some of the major Identity Management solutions that are in use today such as Liberty Alliance, Microsoft Passport, and Shibboleth. This course will also provide the opportunity to gain hands on experience by facilitating exemplar technologies used in laboratory investigations.
# Table of Contents

1. **INTRODUCTION** ......................................................................................................................... 1

2. **STATEMENT OF PURPOSE** ......................................................................................................... 2

3. **REVIEW OF CURRENT RESEARCH** ............................................................................................. 2
   3.1 **WEB SERVICES** .......................................................................................................................... 2
   3.2 **IDENTITY MANAGEMENT SOLUTIONS** ..................................................................................... 3
      3.2.1 Microsoft .NET Passport ........................................................................................................... 4
      3.2.2 Liberty Alliance .......................................................................................................................... 5
      3.2.3 Shibboleth ................................................................................................................................... 6
   3.3 **SAML 2.0** ................................................................................................................................. 7
   3.4 **IDENTITY MANAGEMENT AND SECURITY** .............................................................................. 8
      3.4.1 IM and Identity Theft ................................................................................................................ 8
      3.4.2 Protecting Identity Attributes ................................................................................................... 9
      3.4.3 Privacy Preferences of the User ............................................................................................... 10
   3.5 **DESIGNING THE COURSE** ....................................................................................................... 11
      3.5.1 Active Learning ........................................................................................................................ 11
      3.5.2 Course Format and Design ........................................................................................................ 12
      3.5.3 Lab Structure ............................................................................................................................ 12

4. **THESIS DELIVERABLES** ............................................................................................................. 13

5. **COURSE FORMAT** ...................................................................................................................... 14

6. **COURSE OUTLINE** ..................................................................................................................... 14

7. **COURSE SCHEDULE** .................................................................................................................. 15

8. **LECTURE MATERIAL** .................................................................................................................. 15

9. **MIDTERM EXAM FORMAT** ......................................................................................................... 16

10. **LAB 1 DEMONSTRATING AUTHENTICATION THROUGH SINGLE SIGN-ON IN AN INTRA-DOMAIN** ......................................................................................................................... 19

11. **LAB 2 DEMONSTRATING AUTHENTICATION AND AUTHORIZATION IN AN INTER-DOMAIN ENVIRONMENT** ....................................................................................................................... 21

12. **WRITTEN ASSIGNMENT & PRESENTATION** ............................................................................. 23

13. **CONCLUSION** ............................................................................................................................. 24

14. **APPENDICES** ............................................................................................................................. 26
   14.1 **COURSE OUTLINE** ................................................................................................................... 26
   14.2 **LECTURE PRESENTATIONS** ..................................................................................................... 30
      14.2.1 Introduction to Identity Management ...................................................................................... 30
      14.2.2 Technologies and Standards in Identity Management ............................................................. 59
      14.2.3 Identity Management Solutions & Consortiums ..................................................................... 98
   14.3 **LAB DIAGRAMS** ...................................................................................................................... 125

15. **REFERENCES** ............................................................................................................................. 127
1. INTRODUCTION

The Internet has become a popular resource for enterprises that strive to become more efficient in day-to-day processes by offering web services to facilitate and maintain information. These web services also serve the purpose of attracting and preserving client and partner relationships by the convenience it provides. Some organizations form collaborations, which then require users to have access to resources that would otherwise have been restricted. A username and password is one way for an enterprise to authenticate users and grant access to restricted resources on their networks. If, however, the collaboration includes users with different access levels, or if the organization has multiple web applications, the use of a username and password as a way to identify users and the resources they are authorized to access can become tedious to manage. For the user, having to remember numerous username and passwords can be overbearing, and in turn, may cause the same credentials to be used repeatedly, therefore increasing security risks. One way that organizations are overcoming this issue is by forming Circle of Trusts (CoTs) and utilizing Identity Management (IM). Circle of Trusts describe a network between Service Providers (SP), and, in most cases, Identity Providers (IDP). Service Providers are the organizations offering web services, such as intranets and extranets. Identity Providers are authenticators that have the task of identifying users to SPs before access is granted. Federated Identity Management allows SPs to “securely recognize and leverage user identities owned by trusted organizations within or across CoTs, and identity federation allows enterprises to share confidential user identities with trusted ones, without requiring users to re-enter their name and password when they access their network resources.” [1]

As with most universities that take part in research collaborations, sharing resources across networks is very common, but can also be burdensome to administrators and users when identity management solutions are not present. At Rochester Institute of Technology, research
collaborations take place on a regular basis, especially in the department of Networking, Security, and Systems Administration (NSSA). In this department, graduate students have the opportunity to take courses that will enhance their professional career and allow them to be invaluable assets to their clients, customers, and employers. These courses specialize in security and computer system related technologies that offer a competitive advantage to enterprises that utilize them. It is therefore justified that adding a course that focuses on Identity Management would be beneficial to the department because it offers graduate students the skills and knowledge necessary to help enterprises protect and manage their networks and resources in a digital world full of vulnerabilities.

2. STATEMENT OF PURPOSE
Digital identities are being utilized more than ever as a means to authenticate computer users in order to control access to systems, web services, and networks. To maintain these digital identities, administrators turn to Identity Management solutions to offer protection for users, business partners, and networks. Currently, the Networking, Security, and Systems Administration Department at Rochester Institute of Technology does not offer a course for Identity Management. This paper proposes such a course.

3. Review of Current Research

3.1 Web Services
In modern enterprises, it is very common to be able to access resources over the Internet whether you are an employee carrying out daily tasks, a business partner closing on a deal, or a consumer making a purchase. Whatever the case may be, these activities are carried out using Web-based services, which offer convenience to both consumers and enterprises by providing a low cost way
of conducting business. Web-based services, also called Web services (WS), can include almost “any organization on the Web today, for example, Internet portals, retailers, transportation providers, financial institutions, entertainment companies, not-for-profit organizations, government agencies, etc.” [7] The architecture of Web services includes four key components. The first is the consumer, which is the user of the web service. The second is Universal Description Discovery and Integration (UDDI), which “defines operations of a service registry and is a data structure for registering and storing business information and technical specifications.” [4] The third component, Web Services Description Language (WSDL), is the universal language of WS that allows computers receiving and sending data to be interoperable. The last component, Simple Object Access Protocol (SOAP), “is an XML/HTTP-based message transfer protocol for WS.” [4] As more and more users take advantage of the benefits of WS by creating digital identities that are unique to each WS, the increase in administration costs for the enterprise and the high security risks for the user forces the need for Identity Management Systems.

3.2 Identity Management Solutions

Initiatives that include protocols and standards for Identity Management have attracted much attention by researchers based on notions concerning the privacy of the user or the security of the network. Some of those initiatives proposed have been included in further research towards the development of Identity Management solutions. A few of the major solutions for Identity Management are Microsoft .NET Passport, Liberty Alliance, and Shibboleth. Much work has been done involving these three projects, as they each vie to be the better solution for enterprises today.
3.2.1 Microsoft .NET Passport

Microsoft .NET Passport solution allows enterprises the ability to outsource part of its administration that includes authentication services, which, in turn, reduces costs. .NET Passport benefits the end users by offering the convenience of registering with or signing into one passport-enabled site, and automatically being authenticated when they visit other passport-enabled websites, also called participating sites. The way this Microsoft solution works for enterprises and users is similar to the way the passport document works for countries and travelers. Each traveler is issued a passport, which conveniently holds the traveler’s personal information in one document. Each country that the user traverses must trust the passport documentation system, and allow or deny that traveler entrance into the country based on the personal information in his or her passport. The same is true for enterprises that use the Microsoft .NET Passport solution. These enterprises have passport-enabled web services that take advantage of the single sign in service. A user creates a passport profile with one of the participating sites by simply registering with that site. He or she can choose which information is saved in the profile. When this user visits another passport-enabled site for the first time, his passport profile will allow him to bypass the registration process and automatically sign him in. [10]

The Microsoft .NET Passport solution entails three processes. The Registration Process encompasses the user’s credentials and profile information. In this process, the user can explicitly define what information gets stored in his or her profile. Credentials are the user’s email address, password, security questions and answers, and security keys. Profile information is the user’s personal data such as his or her name, birth date, country, gender occupation, address, and so forth. The credentials are never shared with participating sites; however, the personal information can be shared at the user’s request. The Authentication Process entails
signing in and out of .NET Passport, email address and password controls, operational communication, SSL channels, using security keys, cookies, and the use of profile information. The Profile Management Process allows the user to change their settings and profile information by signing directly into memberservices.passport.com. [10]

3.2.2 Liberty Alliance

Liberty Alliance is another well-known Identity management solution that offers benefits to both users and businesses. It is a consortium of 150 companies. The entire project is based on four key objectives:

- “Enable consumers to protect the privacy and security of their network identity information”
- “Enable businesses to maintain and manage their customer relationships without third-party participation” [7]
- “Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers” [7]
- “Create a network identity infrastructure that supports all current and emerging network access devices” [7]

The way this solution works is through businesses affiliates that offer web-based services that combine to form a circle of trust (CoT). The participants of CoTs are called service providers (SPs). Identity providers (IDP) are SPs that “brokers trust to other participating members or SPs in the CoT.” IDPs control the Identity Management tasks such as authentication. [1] One of the differences between Microsoft .NET Passport and Liberty Alliance is that .NET Passport is based on the centralized identity management (IM) model while Liberty Alliance is based on the distributed IM model. [4] What that means is that the IDP in the centralized model is the sole authenticator while the IDP in the distributed model is dispersed amongst members and SPs. This
means that each member must trust each other. Therefore, when a user wants to authenticate to several web services in the CoT, he or she only has to sign on once with a member of the CoT. Other members that the user accesses pass authentication messages between SPs and IDPs; therefore, eliminating the need for the user to sign on again. [7]

Liberty Alliance Federated Identity Management consists of three classes of specifications. The first is the Identity federation framework (ID-FF), which offers specs on identity federation, de-federation, and single sign-on based on Security Assertion Markup Language (SAML). The second specification is the Web-service framework (ID-WSF), which offers specifics for “creation, discovery, invocation of interoperable identity web-services and permission based attribute sharing.” The last specification is standard interoperable identity services (ID-SIS), which describes a standard for basic profile information. [11]

3.2.3 Shibboleth

Students the take this course will be using the Shibboleth package for implementation of single sign-on within and across networks. Shibboleth is an open source software package that is utilized by many types of organizations, such as universities, companies, and government agencies. It utilizes federated identity standards such as SAML, for single sign-on services, and encryption technology for security. The purpose of using this technology is to provide students with hands-on experience with the technology used in federated identity management environments and because it is “freely available, and is released under the Apache Software License.” [13]

“Shibboleth Single Sign-on and Federating Software was developed specifically to address the challenges of:
· Multiple passwords required for multiple applications
· Scaling the account management of multiple applications
· Security issues associated with accessing third-party services
· Privacy
· Interoperability within and across organizational boundaries
· Enabling institutions to choose their authentication technology
· Enabling services providers to control access to their resources” [13]

3.3 SAML 2.0

When identity information is being communicated between Service Providers (SP) and Identity Providers, Security Assertions Markup Language (SAML) is the protocol used in order to promote interoperability. SAML 2.0 uses an XML-based framework and offers benefits that include platform neutrality and loose coupling. The information that is exchanged using SAML is authentication, authorization, and attribute information. [9] The framework for SAML includes an Asserting Party (AP), which generates “assertions containing various statements about the subject of the assertion,” and a Relying Party (RP), which can “verify the validity of the assertion” and decide whether to provide services to the subject. [14] This protocol is a popular standard in Federated Identity Management because it is designed to be compatible with existing and emerging standards, it does not require frequent updates, and it provides a generic foundation for many different Identity Management solutions. For instance, the Identity Federation Framework of Liberty Alliance calls the AP of SAML the Identity Provider (IDP) and the RP of SAML the Service Provider. [14]
3.4 Identity Management and Security

This section shows how Identity Management and security are related through several articles from the ACM portal. In each article discussed below, the authors focus their attention on security from the user’s perspective. The first article surveys hacking tactics commonly used by attackers and explains how Federated Identity Management can lower the risks or even prevent these attacks. In the second article titled “Establishing and protecting digital identity in federation systems,” the authors propose a solution for protecting user’s personal attributes when they are shared amongst members of Circles of Trusts. The last article titled “Managing privacy preferences for federated identity management,” shows how managing user’s privacy preferences through a privacy policy can be simplified with a new protocol.

3.4.1 IM and Identity Theft

Much of the related work done on IM is targeted towards protecting the digital identity of users. In a paper titled “Federated Identity Management for Protecting Users from ID Theft,” the authors wanted to address the notion that online identity theft risks are increased with the use of FIM. They argue against the conception that once one SP is compromised, essentially, all other SPs that are in that federation are also compromised because of the single sign-on mechanism. The main purpose of the paper is to prove that although there are online identity theft risks associated with FIM, they are far outweighed by the benefits. The authors show that using the single sign-on mechanism guards against phishing attacks. A user should become skeptical if a site that poses as the original asks for a username and password where as the user normally would not need to enter that information. In addition, Strong Authentication is another mechanism used in Federated SSO that requires additional cryptographic methods of authentication beyond just the username and password. With Service Authentication, another SSO mechanism, it would be
impossible for a site to become a member of the federation because provider-to-provider authentication relies on digital certificates and signatures. This also takes the burden off the user to look for warning signs about the authenticity of a site. [8]

3.4.2 Protecting Identity Attributes

Bhargav-Spantzel, Sqcicciarini, and Bertino’s [3] major concern was to provide a solution that would offer more security for users when their digital identity attributes are shared amongst several service providers (SP). They attempt to accomplish this by creating a single sign-on (SSO) ID used in the circle of trust (CoT) or federation. This ID will then be linked to other attributes, such as a social security number or credit card number, which they call Secured from Identity Theft (SIT) attributes, of the user without the need of the PKI cryptographic protocol normally used to protect these attributes when authenticating. Their main goal is to “preserve [the] privacy of the user identity without jeopardizing security.” [3] They do propose the use of other cryptographic tools such as zero knowledge proofs and distributed hash tables to hide the users attribute values in a protocol they call SIT attribute usage protocol. When the user wants to authenticate with a pre-registered SP that requires one of the SIT attributes, the user must provide at least one other SIT attribute and their SSO ID as proof of identity. IF any one of these is lacking, then the user will not be authenticated, and the SIT attribute will not be of use. The security model used to test this proposed protocol consisted of users and SPs using servers. The results showed that the protocol is robust in preventing user’s identity from being compromised by malicious attackers by proving four theorems. The first one proved that a mechanism called Duplicate Detection prevents an attacker from re-registering with a SP using a user’s SSO ID or a SIT attribute. The second theorem proved that the SIT attributes are never exposed either during registration with a SP or during authentication. The third theorem proved that the SIT attribute usage protocol offers protection from rogue users because of the required attribute values needed
for authentication. It also provides protection from rogue SPs because the true forms of the attributes are never exposed. The final theorem proves that the SIT attribute usage protocol offers confidentiality since the SPs are not able to learn the true form of the SIT attributes. [3]

3.4.3 Privacy Preferences of the User

Gail-Joon Ahn and John Lam also focused their attention on privacy issues with Federated Identity Management, specifically on the Liberty Alliance solution. Their approach was more on a practical level for businesses that could possibly be affected by these issues. In the Liberty Alliance Web Service Framework architecture, users are able to define their privacy preference or policy. In other words, users can determine what personal information is used to authenticate in Web services. However, the Web Service Framework architecture also contains Usage Directives that specify policies on the intended use of the personal data being requested. This framework, therefore, incorporates a multi-level policy based approach that requires the requesting party to ask for information and determine its usage. That determination must then be checked against the policy for intended usage. This information must also be checked against the privacy policy of the user’s preference profile. What the authors have proposed is a simpler version protocol to the multi-level policy approach currently in use. This protocol, called Preference Expression for Privacy (PREP) “is a language for storing the user’s privacy preference with Liberty enabled attribute providers.” [1] This approach proposes to eliminate the need to do multiple checks against several policies before information can be disseminated. In their research, the authors provide a proposed structure of the protocol and a mechanism to process user preferences. [1]
3.5 DESIGNING THE COURSE

In addition to the subject of Identity Management, this thesis also proposes to teach the subject to graduate level students by way of a graduate level course. The related work found below emphasizes some particular aspects of the process of designing a course that will be very useful when put into practice. The major area of this process is to decide how the topic will be taught and how the students will learn it best. It is important to do assessments and evaluations at each stage in the process so that there can be a means for constant improvement.

3.5.1 Active Learning

To design a course on Identity Management, one must take into consideration the students that will be learning about the subject. In traditional educational settings, the educator usually lectures to the students and gives reading and written assignments to compliment the lectures. It is then up to the student to understand what is being taught, usually by memorization. This method is effective while the student is enrolled in the course; however, if what was learned is not put into practice, it may be lost from the student’s memory. An addition to the traditional lecture approach to learning would be active learning.

This method of learning will be most beneficial to the students that enroll in this Identity Management course because of its nine methods of learning which have been proven to provide the most impact on a student’s learning experience during and after the time in which they are actually gaining knowledge. Those nine methods are cooperative learning, collaborative learning, experiential learning, exploratory learning, peer-assisted learning, problem-based learning, reflective learning, and writing-based learning. Incorporating these methods when laying out course goals will also assist with clearly defining the student outcomes for each goal.
Researchers are also discovering that active learning in higher education also promotes a “deeper understanding of the material, [a] higher-order [of] thinking skill, higher academic achievement, positive peer relationships, and higher self-esteem” which are all attributes that will be beneficial when a student goes out into the industry. [6]

3.5.2 Course Format and Design

In the same article, “A Learning Centered Approach to Designing Computer Science Courses,” the authors proposed a course design that will incorporate active learning and provide feedback to its effectiveness. The first portion of this design involves understanding situational factors such as the nature of the subject and the characteristics of the instructors and students. The second part involves determining the goals of the course. The third part requires a design of feedback and assessment procedures. This process occurs throughout the course from the onset where the instructor assesses herself to find out what exactly she is trying to convey, to where the students assess each other in group projects, to the end where course evaluations are completed. The next portion of the course design involves constructing teaching and learning activities in the form of a schedule. Once that is complete, instruction delivery and active learning can be determined. The final portion of the course design is to write the syllabus. [6] These steps will be used during this thesis to efficiently gather information on Identity Management and effectively project that information in the form of lectures, labs, and a project.

3.5.3 Lab Structure

To determine what labs will be included in the course design requires much thought and some sort of process. The authors Alan Fekete and Antony Greening devised a six-phase process for designing labs in the article “Designing Closed Laboratories for a Computer Science Course,”
which can be very useful for labs used in a course on Identity Management designed for a Networking and Security course. In the first phase, the designer must analyze the sequence and pacing laid out in the lecture materials. It is important to understand the level of knowledge the students possess going into the lab. The second phase involves dividing the technical material into several labs. The goal of this phase is to allot enough activity to keep the students attention without it becoming to overwhelming. The third phase is to determine useful learning experiences. In this phase, the designer can determine whether the work should be done in groups or individually. The fourth phase is to map experiences onto the lab framework. This phase determines the skills that will be developed from the lab activities and how they can relate to real world experiences. The fifth phase is to develop the lab specifications, and the sixth phase is to review the labs. [5]

There will be two labs for this course. The labs will be implemented in such a way that the second lab will be a continuation of the first. Students will apply the theoretical knowledge in which they gained from the first half of the course to the actual application of these labs in the second half. Further explanation and detail of the two labs are discussed in sections 10 and 11.

4. THESIS DELIVERABLES

• Course Outline
• Textbook Selection
• Three Lectures
• Midterm Exam Format
• Two Labs
• Final Project – Written Assignment & Presentation
5. COURSE FORMAT

This course will follow the ten-week quarter system at Rochester Institute of Technology, in which coursework will be divided into two halves. The first half will be theoretical while the second half will be hands-on. The first part of the course will consist of lecture material and reading assignments from the textbooks and other reading material. There will be open discussions covering the reading material each week during the class session. This half of the course will end with a midterm examination. The second half of the course will consist of lab assignments and discussion. Students will then use class time and outside of class time to work on the labs with their group members. There will also be a written assignment and presentation due towards the end of the quarter.

6. COURSE OUTLINE

See Appendix
# 7. COURSE SCHEDULE

**Tentative Course Schedule: the development of a graduate course in Identity Management for NSSA**

<table>
<thead>
<tr>
<th>Week</th>
<th>Class 1</th>
<th>Reading Assignment</th>
</tr>
</thead>
</table>
| 1    | Introduction to Identity Management | **Steel, Core Security Patterns** Chaps 7 (Identity Management Standards and Technologies)  
**Benantar, Access Control Systems** Chap 2 (Introduction to Identity-Management Models) |
| 2    | Technologies and Standards in Identity Management | **Steel, Core Security Patterns** Chaps 6 (Web Services Security – Standards and Technologies) and 7 (Identity Management Standards and Technologies) |
| 3    | Identity Management Solutions & Consortiums | **Steel Core Security Patterns** Chaps 7 (Identity Management Standards and Technologies)  
**Bucker, Identity Management Design Guide with IBM Tivoli Identity Manager** Part 1 (Architecture and Design)  
Online Resources and Handouts |
| 4    | Review for Exam | STUDY FOR MID-TERM EXAM |
| 5    | Mid-Term Exam | STUDY FOR MID-TERM EXAM |
| 6    | Discussion of Lab One Material/Written Assignment | Handouts and downloads from open source Shibboleth System Package. Discuss Written Assignment |
| 7    | Work on Lab One | Work on Lab One |
| 8    | Discussion of Lab Two Material | Handouts and downloads from open source Shibboleth Package |
| 9    | Work on Lab Two | Work on Lab 2 |
| 10   | Lab Write-ups & Written Assignment | Written Assignment Due  
Work on Presentation |
| 11   | Presentations | Lab Write-ups Due |
8. LECTURE MATERIAL

Below are the outlines of three lectures with titles and content. For PowerPoint slides, see Appendix B:

Week 1 Material
Introduction to Identity Management

1.1 What is Identity? Identity Management?
1.2 Statistics revolving Identity Management
1.3 Core Issues in Identity Management
   1.3.1 For Users
   1.3.2 For Enterprises & Business-to-Business Networks
1.4 Security Vulnerabilities & Threats to User Identities
1.5 User Identity Terms & Definitions
   1.5.1 Identification
   1.5.2 Authentication
   1.5.3 Credentials
   1.5.4 Authorization
   1.5.5 Accounting
1.6 Functions of Identity Management
   1.6.1 Single Sign-On / Global Logout
   1.6.2 User Provisioning & Account Service Provisioning
   1.6.3 Roles and Groups
   1.6.4 Delegated Administration
   1.6.5 Audit Trails and Reporting
1.7 Identity Management Models
   1.7.1 Local Identity
      1.7.1.1 Host-Centric
      1.7.1.2 Advantages/Disadvantages
   1.7.2 Network Identity
      1.7.2.1 Network-Centric
      1.7.2.2 Advantages/Disadvantages
   1.7.3 Federated Identity
      1.7.3.1 Isolated IM Model (Local Profiling)
         1.7.3.1.1 Isolated IM Domains
         1.7.3.1.2 Advantages/Disadvantages
         1.7.3.1.3 IBM Tivoli Identity Manager
      1.7.3.2 Centralized FIM Model (Profiling by a Third Party)
         1.7.3.2.1 Delegated Third Party
         1.7.3.2.2 Identity Providers, Service Providers, Circle of Trusts
         1.7.3.2.3 Advantages/Disadvantages
         1.7.3.2.4 Microsoft .NET Passport
      1.7.3.3 Distributed FIM Model (Distributed Profiling)
         1.7.3.3.1 Distributed Authentication Tasks
         1.7.3.3.2 Identity Providers, Service Providers, Circle of Trusts
         1.7.3.3.3 Advantages/Disadvantages
1.7.3.3.4  Liberty Alliance Project
1.7.4  Global Web Identity
   1.7.4.1  MetaDirectories
   1.7.4.2  Affiliate Networks (Virtual Directories)

**Week 2 Material**

**Technologies and Standards in Identity Management**

2.1  Introduction to Web Services
   2.1.1  Operational Roles
   2.1.2  Operational Model
   2.1.3  Web Services Architecture and Building Blocks
   2.1.4  Web Services Security – Core Issues & Requirements

2.2  Web Services Standards
   2.2.1  Extensible Markup Language (XML)
   2.2.2  Simple Object Access Protocol (SOAP)
      2.2.2.1  SOAP Structural Format
   2.2.3  Web Services Definition Language (WSDL)
   2.2.4  Universal Description, Discovery, and Integration (UDDI)
   2.2.5  Web Services Communication
      2.2.5.1  RPC Style
      2.2.5.2  Documentation Style

2.3  Web Services Security
   2.3.1  XML Signature
      2.3.1.1  Enveloped Signature and Data Structure
      2.3.1.2  Enveloping Signature and Data Structure
      2.3.1.3  Detached Signature and Data Structure
   2.3.2  XML Encryption
      2.3.2.1  Message Level Encryption
      2.3.2.2  XML Encryption Data Structure
   2.3.3  XML Key Management Systems (XKMS)
   2.3.4  OASIS Web Services Security

2.4  Introduction to Security Assertion Markup Language (SAML)
   2.4.1  SAML Profiles
   2.4.2  SAML Assertions
   2.4.3  SAML Architecture
      2.4.3.1  SAML Domain Model
      2.4.3.2  Identity Attributes
      2.4.3.3  SAML Logical Architecture
   2.4.4  The Role of SAML in Web Services

**Week 3 Material**

**Identity Management Solutions & Consortiums**

3.1  Introduction to Liberty Alliance Project
   3.1.1  Liberty Alliance System Entities
   3.1.2  Identity Federated Framework (ID-FF) Phase 1.0 & 1.2
3.1.3 Logical Architecture

3.2 Microsoft .NET Passport Overview
   3.2.1 Registration Process
   3.2.2 Authentication Process
   3.2.3 Profile Management Process

3.3 Introduction to IBM Tivoli Identity Manager
   3.3.1 Manager Entities
      3.3.1.1 User, Accounts, Attributes
      3.3.1.2 Passwords
      3.3.1.3 Group Memberships
      3.3.1.4 Systems and Applications
   3.3.2 Management Entities
      3.3.2.1 Organizational Trees & Roles
      3.3.2.2 Groups & Access Control Items (ACIs)
      3.3.2.3 Policy (Provision, Identity, Service Selection)
      3.3.2.4 Audit Logs & Reports
   3.3.3 Tivoli Manager Functions

3.4 Introduction to the Shibboleth System
   3.4.1 SAML and Federated Identity
   3.4.2 Attribute-Based Authorization
   3.4.3 Shibboleth Software Components
   3.4.4 Shibboleth System Functionality
   3.4.5 Usage Scenarios

9. MIDTERM EXAM FORMAT

The midterm examination will compose of both short answer questions and essay questions. It is appropriate to examine the students on their knowledge of the subject in this format. This will determine if the students truly grasp how Identity management has emerged and what benefits it has to offer. It will also provoke the students to think more critically about how Identity Management relates to what they already know and have been taught in related courses as well as what its future outlook will be. As this course will also be a distance course, having an exam in this format leaves little to no room for students to share their answers. Since this will be the only examination for this course, short answer and essay questions will offer more of a challenge as opposed to multiple choice or true and false.
10. LAB 1 Demonstrating Authentication through Single Sign-On in an Intra-Domain

**Goal:**
Explore the architect and functionality of single sign-on using the Shibboleth System.

Students will be setting up a local environment that will consist of an Identity Provider (IdP), a Service Provider (SP), and a workstation as the user. The Operating System will be CentOS. The students will also be utilizing the Discovery Service technology provided by Shibboleth. The lab will work in this manner.

Shibboleth is a system designed to exchange information across realms for authentication and authorization. This system provides a means for the user to be able to access resources across security domains seamlessly. When a user attempts to access resources outside his or her home security domain, the user’s home domain can provide the service provider with trusted information that will allow the user to access resources.

**Activity One: The Environment**
Create, using virtual software, an environment that consists of a client and a server. The client machine will be the user and the server will be the Identity Provider. Another web server will be needed to act as the Service Provider.

Much of the services needed for this lab are provided with the Shibboleth System. Students are to go to the site listed below and install and build the components for the environment listed below using Shibboleth. There are also how to’s and demonstration sites for assistance.

https://spaces.internet2.edu/display/SHIB2/Installation

Setting up the Identity Provider:
- A common institutional directory service should be operational; Shibboleth comes with JNDI and JDBC capabilities built in, which encompasses SQL and LDAP, and the Attribute Authority has a Java API, which will allow specification of custom connectors to other types of data sources.
- A method to authenticate browser users must be in place, preferably in the form of an enterprise authentication service. Some form of an SSO or a WebISO service is not explicitly necessary for Shibboleth; however, it is highly recommended.
- Shibboleth is known to work on Windows, Linux, Mac OS X, and Solaris, but should function on any platform that has an Apache or Tomcat implementation.
- It is recommended that a web server such as Apache be deployed in front of Tomcat to provide authentication services and to control the flow of requests to Tomcat. There may be issues surrounding the number of maximum connections to the web server and to the servlet container.

Setting up the Service Provider:
- An IIS or Apache web server must be deployed which is capable of SSL and running Shibboleth.
• Web applications must be modified to be able to rely on attributes supplied by Shibboleth. Often this will overlap with the same header variables set by other authentication schemes, such as REMOTE_USER.

• Access control schemes can often be simplified and rewritten to take advantage of the inherent power of attribute-based protection.

Setting up the Client:

• The client, in this scenario, should be able to authenticate with the identity provider as its local server using a directory service.

**Activity Two: Demonstrate Single Sign-On**

The goal of this activity for the Service Provider to ask the Identity Provider to authenticate a user and issue a SAML assertion to the Single Sign-On Service to either grant or deny access to resources. The Single Sign-On Service is a part of the Shibboleth software and is installed on the IdP.

This page describes an approach to configuring a single Shibboleth IdP and SP to recognize each other and interoperate successfully with each other.

https://spaces.internet2.edu/display/SHIB/BilateralDeployment

**Activity Three: Questions**

1. What are the four primary components to the Identity Provider in this lab?

2. What are the three primary components to the Service Provider in this lab?

3. Where in your environment that you created do these components reside; and, what type of device or machine houses these components?

4. From the Identity Provider’s point-of-view, explain the functionality of the components you listed in question one.

5. From the Service Provider’s point-of-view, explain the functionality of the components you listed in question two.

6. Provide a diagram of the environment you created in this lab. Include component names and directional arrows to demonstrate what is happening.
11. LAB 2 Demonstrating Authentication and Authorization in an Inter-Domain Environment

Goal:
The goal of this lab is to explore the architecture and functionality of Single Sign-On in a federated environment.

In this lab, students will be using components from lab 1 and adding more components to create a circle of trust.

Shibboleth is a system designed to exchange information across realms for authentication and authorization. This system provides a means for the user to be able to access resources across security domains seamlessly. When a user attempts to access resources outside his or her home security domain, the user’s home domain can provide the service provider with trusted information that will allow the user to access resources. This trusted information comes in the form of attributes in which the user may have the ability to determine which attributes are shared with which sites. By this information, it will be determined what resources the user may be authorized to access.

Joining a Federation
In Lab One, we demonstrated how single sign-on works in a local domain. A user only signs in once to his or her local domain; and, metadata containing identity information is exchanged between the identity provider and the service provider to grant access to a web-based resource requested by the user. What happens when there is a Circle of Trust containing many identity providers and service providers? How will a user be able to authenticate with a particular service provider; and, how will the service provider know how to retrieve attribute information pertaining to the user if there are many identity providers?

Much of the information and components needed for this lab are provided with the Shibboleth System and can be found at the link below.

https://spaces.internet2.edu/display/SHIB2/Installation

- Use the environment created in Lab 1. In the same method in which you created the Service Provider and Identity Provider from Lab 1, create an additional SP and IdP.

- The Where Are You From Service (WAYF) in this lab is deployed as a part of the Service Provider and is responsible for allowing users to authenticate with an Identity Provider, such as an institution, and redirecting them to the SSO handler of that institution.

- Joining a federation is not required for the use of Shibboleth, as we saw in Lab 1. It does, however expand the number of Service Providers and Identity Providers that are able to interact and create a seamless environment for users.

- When an Identity Provider is accepted into a federation, the information is added to the WAYF service and to Service Provider sites as well as to the site of the IdP.

- Attribute release and acceptance policies, the use and caching of attributes, and definition of commonly traded attribute are then maintained by the federation.
• In the Shibboleth System, Relying Parties can be either an IdP or a SP. If there is a federation involved, then the federation is the single relying party according to either a SP or IdP.

• Shibboleth supports the use of federations in order to simplify trust interactions and policy in support of these exchanges. Membership and participation in multiple federations can be accomplished in most cases by simply pointing to other metadata files with additional Metadata Provider elements. For further information on how Shibboleth forms federations and uses metadata, go to this link. https://spaces.internet2.edu/display/SHIB/IdPRelyingConfig

Once you have downloaded and installed the Shibboleth Package, you can go to the link below to test the software. http://www.testshib.org/

**Deliverables:**

You are to create a trust environment containing as many Identity Providers and Service Providers as you wish, but it must be more than two of each. Use the testing software provided at the link above to make sure that your installation is working properly. Provide a diagram of the environment you created. Include in this diagram component names, directional arrows, and a description of what is actually taking pace. Also, provide necessary screen captures of both the installation process and deployment to verify that you have successfully completed this lab.

Be prepared to present your information to the class. Included in the presentation should be:

• Diagrams of the environment created
• Names of the components used
• Explanations of why certain components were used
• Explanations of the steps taken to achieve the overall environment
• Explanation of the processes taking place
• Demonstration of functionality from both labs
• What security risks are being mitigated with this environment?
• What security risks, if any, may prevail from this environment
• Any difficulties in setting up the environment
• Any further findings or additional functionalities discovered
12. WRITTEN ASSIGNMENT & PRESENTATION

Goal
The goal of this assignment is to explore Identity Management outside of the course and demonstrate the ability to educate users on the needs and benefits of implementing Identity Management solutions in various environments.

In addition to students gaining knowledge about Identity Management from the lecture material and labs, they will also have the opportunity to expand their knowledge through research. Although several Identity Management initiatives are covered through the course, there are a wide variety of research and developments taking place that are beyond the scope of the material covered in the course. This assignment gives students the opportunity to go beyond what is taught to see how this technology can benefit enterprises both now and in the future.

Part One:
Identify four usage scenarios for Identity Management. In your explanation, you are to answer the following three questions for each:
- How is it done today?
- What is the problem with the current approach?
- How can Identity Management solve this problem?

Part Two:
Identify two Identity Management solutions not covered in class. Give the background and functionality for each solution. Give detailed description of the system entities. Show diagrams where necessary. Also, give the architecture of the system.

Part Three:
After learning about the fundamentals of Identity Management and doing some research on your own, you were able to see that there are many other initiatives taking place. Some of these initiatives are advancements to solutions already in use while others may still be just theory. Identify two Identity Management initiatives currently taking place. Give the background, goal, and outcome, if any, of each.

Part Four:
It is very common for Systems Administrators to thoroughly research and test new technologies before integrating it with the current way of doing business. They must also have a sound understanding of the background of the technology to explain its benefits and necessity. Taking the information from the first three parts of this assignment, present your findings as if you are an IT Professional in an enterprise of your choosing. Your objective is to gain consensus on the implementation of one of the two solutions from Part Two.
13. CONCLUSION

It is evident that the future outlook of Identity Management will continue to evolve as researchers improve on current standards that strive to make the sharing of network resources and the use of digital identities more secure. Participants of collaborations at colleges and universities will find it more convenient when gaining authorization to access data across network domains by a single sign-in to their local domain. Enterprises that span the globe and those that have partnerships will lessen the burden on their administrators by joining Circle of Trusts to help manage user credentials. Even consumers, who are now showing more concern about how their digital identities are being stored, will reap the benefits of having to rely less on memorizing usernames and passwords as they freely use Web services over the Internet. Therefore, it is highly recommended that the Department of Networking, Security, and Systems Administration at Rochester Institute of Technology offer its graduate students a course such as this. Enrolled students would be able to increase their level of expertise whether their degree positions them as a Network Analyst, Security Specialist, Project Manager, or Identity Management Consultant. Employers will be more likely to hire candidates who are able to minimize cost, improve security, and manage company resources with less complexity. Students will even gain by continuing with Research and Development in Identity Management as the work that has been done has branched off in many directions leaving doors open for new technologies to emerge.
14. APPENDICES

14.1 Course Outline

B. Thomas Golisano College of Computing and Information Sciences

Department of Networking, Security, and Systems Administration

NEW (or REVISED) COURSE:

1.0 Title: Identity Management Solutions
   Date: May 25, 2008
   Credit Hours: 4
   Prerequisite(s): None
   Co-requisite(s): None
   Course proposed by:

2.0 Course information:

<table>
<thead>
<tr>
<th>Contact hours per week</th>
<th>Maximum students per section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classroom</td>
<td>4</td>
</tr>
<tr>
<td>Lab</td>
<td></td>
</tr>
<tr>
<td>Active Learning/Active Learning Extended</td>
<td></td>
</tr>
<tr>
<td>Other (specify)</td>
<td>Distance Course</td>
</tr>
</tbody>
</table>

Quarter(s) offered (check)
- Fall
- Winter
- Spring
- Summer

Students required to take this course: (by program and year, as appropriate)
None

Students who might elect to take the course:

Matriculated students in the MS in Information Technology, the MS in Computing Security and Information Assurance, and the MS in Applied Networking and Systems Administration

3.0 Goals of the course (including rationale for the course, when appropriate):
The Internet has become a popular resource for enterprises that strive to become more efficient in day-to-day processes by offering the ability to extend their networks and applications over the Internet in the form of web services. These web services help facilitate the sharing of resources within and across organizational boundaries. Identity Management Solutions assist these web services in authenticating and authorizing individual user access to protected online resources order to offer protection for both network resources and user’s personal information.

This course is intended to provide students with knowledge about Identity Management in modern enterprises and emerging Federated Identity Management solutions. This course will also provide students with the skills necessary to explore Circle of Trusts between enterprises and perform authentication and authorization functions for users.

4.0 Course description
This course involves the study of Identity Management and its core issues. Topics include web services architecture, security, and standards, such as XML and OASIS; Identity Management Standards and Technologies, such as federated identity, and SAML; Identity Management solutions, such as Liberty Alliance, Shibboleth, and Microsoft Passport .NET; and Identity Management best practices and challenges.

Prerequisites: None
Co-requisites: None

5.0 Possible resources (texts, references, computer packages, etc.)
Primary Texts:
5.2 A project of the Internet2 Middleware Initiative: Shibboleth System Package download and installation
https://spaces.internet2.edu/display/SHIB/WebHome.

Supplemental Texts:
5.3 Bückner, Axel, Davis B., Hastings T., Palacios J. C., and Yip I.  Identity Management Design Guide with IBM Tivoli Identity Manager. (2nd ed.). International Business Machines Corp. 2005

Supporting Materials:
5.5 Websites and publications from vendors such as Shibboleth and Liberty Alliance Project; journal articles; conference proceedings; white papers, etc as selected by the instructor(s).

6.0 Topics (outline):
6.1 Introduction to Identity Management
   6.1.1 Identity Management - Core Issues
   6.1.2 Identity Management Models
      6.1.2.1 Local Identity Model
      6.1.2.2 Network Identity Model
      6.1.2.3 Federated Identity Model
         6.1.2.3.1 Local Profiling
6.1.2.3.2 Distributed Profiling
6.1.2.3.3 Centralized Profiling
6.1.2.4 Global Web Identity
   6.1.2.4.1 Metadirectories
   6.1.2.4.2 Affiliate Networks
6.2 Introduction to Web Services
   6.2.1 Web Services Architecture and Building Blocks
   6.2.2 Web Services Security – Core Issues
6.3 Web Services Standards
   6.3.1 Extensible Markup Language (XML)
   6.3.2 Simple Object Access Protocol (SOAP)
   6.3.3 Web Services Definition Language (WSDL)
   6.3.4 Universal Description, Discovery, and Integration (UDDI)
   6.3.5 Web Services Communication – RPC & Document Style
6.4 Web Services Security
   6.4.1.1 XML Signature
   6.4.1.2 XML Encryption
   6.4.1.3 XML Key Management Systems (XKMS)
   6.4.1.4 OASIS Web Service Security
6.5 Introduction to SAML
   6.5.1 SAML Architecture
   6.5.2 SAML Usage Scenarios
   6.5.3 The Role of SAML in Web Services
6.6 Emerging Identity Management Solutions
   6.6.1 Introduction to Liberty Alliance and their Objectives
      6.6.1.1 Liberty Alliance Architecture
      6.6.1.2 Liberty Usage Scenarios
   6.6.2 Microsoft Passport .NET Overview
   6.6.3 IBM Tivoli Identity Manager
      6.6.3.1 Identity Manager Component Structure
      6.6.3.2 Operational Solution Design
   6.6.4 Introduction to the Shibboleth Project
      6.6.4.1 The Shibboleth System and Functionality
      6.6.4.2 SAML and Federated Identity
      6.6.4.3 Attribute Based Authorization
      6.6.4.4 User and Data Privacy
         6.6.4.4.1 Public Key Infrastructure
         6.6.4.4.2 Definition of Attributes

7.0 Intended learning outcomes and associated assessment methods of those outcomes
At the completion of this course, successful students will be able to:
7.1 Discuss the necessity of Identity Management within enterprises and evaluate the core security and network issues that these enterprises face. Assessed by laboratory exercises, written report, and exam.
7.2 Identify the architecture and components of web services, evaluate core security issues that these services face, and establish resolutions with Identity Management. Assessed by laboratory exercises, written report, and exam.
7.3 Discuss and compare emerging Identity Management solutions and their architecture, frameworks, and objectives. Assessed by written report and exam.
7.4 Explain the use of web services and Identity Management technologies such as XML, OASIS Web Service Security, and SAML. Assessed by laboratory exercises, written report, and exam.

7.5 Construct a Federated Identity environment using exemplar technologies and evaluate each component and demonstrate its purpose. Assessed by laboratory exercises and report writing.

7.6 Analyze the details and security implications of several case studies. Assessed by written report and graded class presentations.

7.7 Demonstrate the ability to educate users on the needs and benefits of implementing Identity Management solutions in various environments and for various reasons such as research collaborations in an educational setting or outsourced employee applications in enterprise networks. Assessed by written report and graded class presentations.

8.0 Program or general education goals supported by this course

8.1 Program Objective 1: Design, deploy, and manage the computing environment needed to meet the goals of an organization.

8.2 Program Objective 2: Interface and communicate effectively at all levels of an organization.

9.0 Other relevant information (such as special classroom, studio, or lab needs, special scheduling, media requirements, etc.)

9.1 Access to online lab system RLES with isolated environment and VMware workstation software.

10.0 Supplemental information

Other relevant books, journal articles, commercial publications, and websites as selected by the course instructor(s).

APPROVALS:

______________  ______________
NSSA Curriculum Committee Chair  Date

______________  ______________
NSSA Department Chair  Date
14.2 Lecture Presentations

14.2.1 Introduction to Identity Management

Slide 1

Introduction to Identity Management
In philosophy, identity is whatever makes an entity definable and recognizable, in terms of possessing a set of qualities or characteristics that distinguish it from entities of a different type. (Wiki)

“Identity is a computer representation of an active entity that can be physical (such as a human, a host system, or a network device) or can be a programming agent. Identity, instead of being an assigned identifier is rather an identifier that points to various attributes and entitlements, collectively referred to as a profile. Identity management has emerged to address the issues surrounding the proliferation of identity profiles among various computing platforms within the boundaries of an enterprise, cross enterprises, organizations, and the Internet.” (Benantar 2006)
Identity Management Issues

- For the User
  - Numerous digital identities
    - Accounts with different web sites
    - Many usernames and passwords
  - Information extracted and sold
  - Open to identity theft
  - Protection differs from website to website

Users create accounts with several different web applications. Information aggregators extract information from websites and sell them to corporations to house them in databases for marketing purposes. This exposes users to risks of identity theft. Websites do not follow a particular standard for protecting user’s data. Usually individuals administer the databases that house user’s identities, and users have no control over how their information is handled.
Enterprises usually have more than one internal application with customized mechanism and infrastructure to authenticate their users. Security implementations, such as PKI operations, are different and security infrastructure, such as authentication servers, policy, and directory are different. Users are then required to maintain several user accounts and passwords for each application. In order to overcome these issues, these applications need a common security mechanism for authentication and authorization. US federal regulations such as Sarbanes Oxley Act, HIPAA, and the Patriot Act mandate enterprises to follow a certain standard for auditing purposes, which often imposes on identity management infrastructures.
Users are still required to maintain accounts and passwords to log onto a partner's system. Administrators must manage user accounts. This includes maintaining changed passwords and staying up to date on when members leave the companies of their partners. If the participating partners have several different systems, there must be an agreement on how to create new user accounts for each. If these participating partners want to integrate their user authentication and authorization mechanisms, there will be integration issues and lots of testing.
Security vulnerabilities & threats to user identities

- Denial of Service
- Man-in-the-middle
- Session hijacking
- Spoofing/Rogue servers
- Data privacy & confidentiality violations
- Replay attacks
- Multiple sign-on issues
- Broken authentication and authorization issues
- Keyboard loggers, Trojans, Viruses
- Social Engineering

This slide covers the types of threats and vulnerabilities to user identities.
User Identity Terms

- Identification
- Authentication
- Credentials
- Authorization
- Accounting

Identification - provides user identity to the security system (usually a user ID)

Authentication - determining and validating user identity

Credentials – The evidence provided by the user for the process of authenticating. Examples can be: passwords (static passwords are convenient for users and offer more protection if it is strong); One-time password schemes such as S/KEY invented by Bellcore for UNIX systems that generates one-time passwords; RSA SecurID developed by RSA Security, which requires hardware, tokens, and a user pin for authentication; pin numbers, Keys and Certificates – Asymmetric/Symmetric cryptography using public and private keys; Biometrics-Static (pattern-based) such as fingerprints, retina scans, iris scans, hand or face geometry, voice pattern, skin pattern; and Dynamic (behavior-based) – handwriting.

Authorization – providing users with the access to resources that they are allowed to have and preventing users from accessing resources that they are not allowed to access

Accounting – Providing a trail of user actions. (also referred to as auditing)
Creating and maintaining user identities; defining roles or groups (which makes it easier to administer user profiles); provisioning user access rights, profiles, security policies, and passwords for different systems; delegating administration tasks such as user administration, group and role administration, security administration, and application-specific functions; tracking the history of user identities for risk management and compliance purposes; and providing single authentication and single logout across multiple systems and subsystems (which enhances the user’s experience and offers simplicity for administrators) are all functions of Identity Management.
Identity Management Models

- Four Classes of Identity Management
  - Local Identity
  - Network Identity
  - Federated Identity
  - Global Web Identity

This slide introduces the four Identity Management models.
This slide discusses the local identity model.

- Identity is Host-centric
  - Maintenance & management of registered identities are local
  - Registry & systems share host
  - Registry accessed by multiple systems
  - Identities are unique
The registry can be accessed by other subsystems that share the host. The registry can also be on a separate system in which multiple OS and subsystems can gain access.
Local Identity Model

- **Advantages**
  - Simplicity
    - Local scope
    - Flat name space
- **Disadvantages**
  - Scalability
    - Capacity
    - Performance
    - Flat name space
  - Password and Identity updates

It offers simplicity because of the local scope and flat name space. Attributes are easy to administer and are meaningful for the scope of the host system. Flat name space means that there is no clear relationship between names and no structure that organizes the names. Each entry is a peer to the other. As the population of users and subsystems grow, the capability of the system gets downgraded and ultimately affects the performance of the system. Flat names space can also be an issue as the population keeps growing, available names tend to run out. Users, Applications and subsystems need to maintain credentials to access various systems. This tends to get tedious for the administrator who manages a network with various subsystems and multiple identity registries. Solutions include password and attribute synchronization which communicates the password change or reset to all participating systems. This method also saves on revamping the network infrastructure. Attribute synchronization is more of a manual function which can be tedious and error-prone. Maintaining a single registry which can be accessed by multiple systems is another solution, although bottlenecks may occur. Single Sign-On (SSO) is another solution which allows the user to be authenticated only once and working across multiple systems is seamless. Identity Provisioning tools assist with the management tasks of creating, revoking, deleting, and maintaining accounts or identities.
Network Identity Model

- Identity is Network-centric
  - Authenticated through computing network nodes
  - Defined/confined to specific network
  - Network components perform identity services

This slide discusses the network identity model.
Network Identity Model

In A, the identity is confined to a single domain while in B it is meaningful in two domains.
In the Federated Identity Model, data elements for profile attributes are well defined and understood.
Here you see an established trust amongst organizations although each organization manages its own model of identity.
Federated Identity Topologies

- Local Profiling
  - Isolated IM Model
- Profiling by a Third Party
  - Centralized FIM Model
- Distributed Profiling
  - Distributed FIM Model

This slide covers the three types of Federated Identity models
The entity is registered with the identity infrastructure at his home organization. Profile Attributes are maintained by the home organization. Other participating organizations are unaware of the privileges and entitlements unless service requests cross organizational boundaries.
This slide gives the advantages and disadvantages of the isolated Identity Management model.
This slide discusses the centralized Federated Identity Management model.
Centralized FIM Model

- Advantages
  - Trust establishments managed with IDP only
  - SSO convenience
- Disadvantages
  - Scalability
  - Single point of failure

Profile attributes that are unique to the member organization or SP can still be accessed through the IDP. When more member organizations start to contend for the retrieval and update of profile information, the single third party becomes overwhelmed. Adding additional third parties can solve this issue, although these third parties will have to maintain synchronization.
The entity can register with multiple participants in the federation starting with its home organization and then others as needed. Once a user is signed-in with an organization or SP, other participants will allow access due to the trust relationships of the federation. Liberty Alliance aims to be a distributed Federation Identity Management Model.
Distributed FIM Model

- **Advantages**
  - Flexibility
    - Organizational specific attributes are acquired
    - Users maintain segregated identities
  - SSO
  - Shared IM costs amongst members of Federation

- **Disadvantages**
  - Profile attributes duplicated
  - Synchronization

Attributes that are specific to registering with an organization can still be acquired without agreement issues. Users are portable across autonomous policy domains because they are able to register with each partner in the Federation. Because each partner trusts the identities vouched for by the other when a user signs in, SSO is an added convenience.
The global web identity will be uniquely known throughout the Internet Web. The identity is a representation of the entity or user who owns it.
Global Web Identity Model

- **Metadirectories**
  - Links bind global identity to participating enterprise networks
  - Attributes maintained by metadirectory
  - Attributes updated centrally
  - Not so scalable
  - Automatic Synchronization

“The metadirectory approach bridges disparate domains by exposing the user's identity to a higher level while retaining its relationship to various participating enterprise networks in which the identity is known. The relationships of the global identity to the corresponding enterprise-level identities are formed by the links binding metadirectory information to the directories of the participating organizations. Common user attributes are maintained by the metadirectory. Updating these attributes is centrally done, and synchronization is performed automatically.

“(Benantar 2006)
The metadirectory on the left joins multiple directories of the same organization, while the one on the right joins multiple directories across different organizations.
Affiliate networks participate in a tightly coupled structure by directly mapping an identity defined in one directory onto a corresponding identity in another enterprise directory. The main difference between this mapping approach and that enabled by metadirectories is that here the mapping is achieved without actually having to create an additional "join" in directory. This approach has a better scalability property over metadirectories in that the mappings are discretely distributed over the participating directories. Mapping users across all directories, however, creates management complexities as updating user-identity information requires updating $n$ directories.
This slide depicts the three-way identity-mapping problem presented by the affiliate networks architecture.
End
14.2.2 Technologies and Standards in Identity Management

Slide 1

Technologies and Standards in Identity Management
Administrative costs can be lowered with automated security service provisioning. Productivity is enhanced through streamlined user authentication processes.
Web services allow businesses to provide access available services over standard Web protocols and communication boundaries. They allow the integration of applications into business processes. Horizontal business processes are more functional with the increase in use of Web services. Web services also reduce infrastructure complexity, especially where customers and partners are concerned. Collaboration is convenient and almost seamless. Costs are reduced due to the simplified infrastructure. Most transactions can occur 24-7, and are processed electronically.
Web Service Security Requirements

- Authentication
- Authorization & Entitlement
- Auditability & Traceability
- Data Integrity
- Data Confidentiality
- Non-repudiation
- Availability & Service Continuity
- Single Sign-on & Delegation
- Identity & Policy Management
- Security Interoperability

Auditing and tracing monitors and records events and transactions made by the SP based on requests. It is a way to provide proof of the originating requests and replies to ensure accountability of the client’s requests. Data should be accurate and complete as well as protected. Non-repudiation ensures that the communication between requester and provider are accepted by both parties. Timestamps are a good way to ensure non-repudiation. “Availability and service continuity are mandatory requirements to ensure the Web services infrastructure is capable of sustaining operations after a security breach.” (Steel et al. 2006) Trust partnerships created through Federated Identity Management allows SP to share identities and trust policies across security boundaries. Security mechanisms and countermeasures should work together seamlessly.
Service Providers host Web services. The Service Registry hosts lookup information and descriptions of published services. The registry also stores and lists service types, descriptions, and locations to assist the service requester in finding and subscribing to services. Service Requesters locate Web services from the registry, invokes the service, and executes them from service provider.
This slide visualizes the operational roles from the previous slide.
This slide discusses the technology stack of Web services.
This slide gives an example of the Web services technology stack.
Web Service Standards: XML

- Extensible Markup Language (XML)
  - Endorsed by World Wide Web Consortium (W3C)
  - Standard data format for constructing data
  - Exchanging information between applications, systems, and devices across the Internet

- Role in WS
  - Common format in all communication for expressing complex data structures

This slide introduces XML.
SOAP allows communication to take place in a decentralized, distributed application environment. SOAP can also be a request/response model by exposing the application functionality using SOAP/RPC calls.
SOAP structural format: SOAP envelope contains the header and body of the message. SOAP header contains processing semantics and mechanisms for security, transactions, priority, and auditing. SOAP body contains information that either defines business documents in XML or other XML data during communication. SOAP message attachments contain data such as non-XML or text files.
Web Service Standards: WSDL

- Web Services Definition Language (WSDL)
  - Endorsed by W3C
  - XML representation for describing the services
- Role in WS
  - Metadata language for defining WS
  - Describes WS functionalities, location, & how to access the service

WSDL’s role describes how providers and requesters communicate with one another.
Web Services Standards

- WSDL definition of a WS represents:
  - Operations and Interface
  - Data types
  - Binding information about the protocol
  - Addresses for location

The operations and interface describes the exposed functions. The data types represent the request and responses of messages. The binding information is about the protocol that is used to access the Web service. The addresses are to locate and invoke the Web service. A service provider creates Web services by generating WSDL from its exposed business applications. Once the WSDL definition is created, the public WSDL address for lookup is published in a Web-services registry such as UDDI so that users may be able to locate and invoke the Web Service. The Web service requesters use the WSDL information to build SOAP requests.
Web Service Standards: UDDI

- Universal Description, Discovery, & Integration (UDDI)
  - Endorsed by OASIS
  - Defines Interface and mechanisms for registries of XML-based WS
  - Allows registering/categorizing Web Services
- Role in WS
  - Requester Queries UDDI registry for service
  - Returns location of WSDL description
  - Invokes services using SOAP messages

UDDI registries can be public or private.
In RPC, the client initiates a request and sends a SOAP messages that obtains method calls to the services exposed by the server. These messages also invoke the services with parameters that execute methods in the server. The server responds by first translating the requests into the back-end application method or object and returns a value to the requester. The requester then proceeds with the next operation.

In document style Web service, the client sends a message that includes a business document to the service provider, instead of sending method calls or parameters. The service provider receives and processes the document. It is optional for the services provider to return a message.
Web service threats and vulnerabilities can affect the entire host network, Web service providers, users, data, applications, and systems infrastructure; therefore making identity management difficult and lessening the benefits of Web services. DoS in WS are fake service requests made with the intention of taking too long to process, generating faults, or preventing authorized users from accessing the service. MITM hackers intercept the communication between the requester and service provider without them even knowing it only to manipulate messages or inject false messages. If a Web service uses sessions to identify its requesters, a hacker can sniff the conversation to get the session identifier and steal the session. Identity spoofing is self-explanatory. The hacker uses an authorized identity for malicious intent. Replay attacks on a Web service is when an attacker duplicates a request to a service provider, similar to DoS attacks. Message validation attacks occurs when an attacker abuses the mechanisms used to validate XML encryption/decryption and signatures by sending malformed messages that can cause loops or failures. Just like message validation abuse, XML schemas are used to well-form and valid XML messages. The XML schemas are publicly accessible and are vulnerable to tampering. Publicly accessible UDDI registries and WSDL information are vulnerable to attacks, such as tampering, by adding arbitrary input and output parameters.
This slide introduces XML Signature.

XML Signature

- Basis for securely exchanging XML documents
- Conducting secure business transactions
- Goals
  - Ensure data integrity
  - Message authentication
  - Non-repudiation of services
XML Signature

- Signatures are applied to digital content indirectly
  - Digital content is digested (digest algorithm)
  - Hash value is placed in an XML element
  - The element is digested & cryptographically signed

- Three representations of XML Signatures
  - Enveloped signatures
  - Enveloping signatures
  - Detached signatures

Digital content or digital objects include xml or html documents, binary data, images.
Enveloped signatures are embedded within the original XML content where the XML signature is represented.
Enveloping signatures - The XML signature envelopes the original XML content.
Detached signatures – The XML content and signatures are independent.

(XML code)

```xml
<xml-document>
  <signature>
    ...
    ...
  </signature>
  <business-element/>
</xml-document>
```
XML Encryption

- Basis for securing data and communication
- Conducting secure transactions between partners
- Goals
  - Provide data confidentiality
  - Ensure end-to-end security

XML Encryption encrypts any digital content or digital object like XML, binary data, images, or html. It builds on industry standard encryption algorithms and utilizes a standard XML-based representation and processing model for encryption and decryption.
XML Encryption

- XML encryption applies:
  - encryption for portions of the message
  - Multiple encryption to different parts of a message
  - Message level encryption
  - Multiple encryptions to a message meant for multiple parties, a workflow, or multi-hop communication

Standardized encryption mechanisms like Secure Sockets Layer (SSL) or Transport Layer Security (TLS) are designed to provide encryption from point-to-point as well as encrypt the message in its entirety.
XML Encryption Structure

```xml
<EncryptedData Id? Type? MimeType? Encoding/>
    <EncryptionMethod/>
    <ds:KeyInfo>
        <EncryptedKey/>
        <AgreementMethod/>
        <ds:KeyName/>
        <ds:RetrievalMethod/>
        <ds:*/>
    </ds:KeyInfo>
    <CipherData>
        <CipherValue/>
        <CipherReference URI?>
    </CipherData>
    <EncryptionProperties/>
</EncryptedData>
```

Tags in the XML Encryption Structure:

- `<EncryptedData>` - root element with 4 optional attributes. Id=unique id for encrypted data; Type=defines encrypted data. Either content or an element for the decryption application; MimeType=defines the content MIME type; encoding=spefies the transfer encoding of encrypted data
- `<EncryptionMethod>` - optional specifies the applied encryption algorithm
- `<ds:KeyInfo>` - mandatory specifies information about the key used for encrypting the data
- `<CipherData>` - mandatory provides the encrypted data
- `<EncryptedKey>` - used to transport encrypted keys between sender and receiver
- `<EncryptedProperties>` - optional any additional information about XML encryption, such as date, timestamp, serial #, hardware, application-specific attributes.
PKI issues private keys to service providers and public keys to clients to secure business applications and transactions. In order for Web services from different companies to provide PKI solutions that are interoperable, a trusted provider will facilitate the XKMS service. Then XML-based requests are made to the trusted service to obtain PKI services.
OASIS Web Services Security (WS-Security) WSS

- Basis for building interoperable WS-security infrastructure
- Defines end-to-end message-level security mechanisms for SOAP messages.
- Emerging as de facto standard

WSS is the basis for securing WS by integrating multiple security standards & technologies.
WS- Security

- **Goal**
  - Provide secure SOAP messages that can handle multiple security token formats for authentication, authorization, signature formats, encryption technologies, & trust domains.
- **Digital Signatures - XML Signature**
- **Encryption - XML Encryption**
- **Security Tokens for authentication/authorization**
  - Username/password
  - Binary security tokens (Kerberos, X.509 certificate)
  - XML security tokens (SAML, REL)

This slide discusses WS-Security.
Security assertions are exchanged about entities that have identity related information that link to a security domain or network. SAML enables SSO standards-based mechanisms without needing to know the security architecture of a service provider. Prior to SAML, heterogeneous applications were forced to use a centralized security infrastructure, which was not cost effective, caused interoperable issues, security loopholes, and was difficult to administer (deployment & troubleshooting). Another approach before SAML was the use of security tokens or encapsulated user credentials in the HTTP-POST header. This method was imposing to corporations because they had to develop mechanisms in their applications that intercepted the HTTP header for the security token containing the user’s credentials.
This slide discusses the benefits of SAML.

- No duplicates of security mechanisms and associated directory information.
- Interoperability between applications
- Scalable remote authorization
- No mandatory definition for authentication & authorization services
- Designed to be used with other standards
  - Liberty Alliance Project
  - Shibboleth project
  - OASIS WS-Security
This slide gives the background of SAML.

- **SAML 1.0**
  - OASIS standard November 2002
  - Endorsed by industry for SSO & interoperability
  - Addressed how identity information can be communicated from one domain to another
SAML Background

- **SAML 1.1**
  - September 2003
  - Supports Network Identity specified by Liberty Alliance
  - Delegated administration
  - Policy management
  - Web account Linking
  - Role-based federation
  - Guidelines for digital certificates
  - Defined protocols for SSO

SAML 1.1 allows user’s authentication and authorization information to be exchanged security between Web sites within an organization or between organizations over the Internet. Digital certificates allow digital signing of SAML assertions. SAML 1.1 does not address the issue of having a standard authentication protocol to support different authentication devices and methods. SAML 2.0 attempts to address this issue.
SAML Background

- SAML 2.0
  - OASIS standard March 2005
  - Additions based on ID-FF 1.2 and Shibboleth
  - Global sign-out (Session management)
  - Liberty opt-in account linking across Web sites

This slide gives the background of SAML.
SAML Profiles

- SAML Profiles
  - Rules/Guidelines to embed/extract SAML assertions from protocols
- SAML Attribute Profiles
  - Rules for mapping attributes in SAML to other attribute representation systems

SAML Profile examples:
- Web browser SSO Profile – SSO using standard browsers to multiple SPs
- Single Logout Profile – how to terminate the sessions managed by the session authority (IdP)
- Identity Provider Discovery Profile – how a SP discovers the IdP

SAML Attribute Profiles examples:
- Basic Profile – string-based SAML attribute names
- X.500/LDAP Profile – SAML attribute naming using object identifiers in Uniform Resource Names
- UUID Profile – SAML attribute names as Universal Unique Identifiers expressed in URNs
SAML Assertions

- Encoded in an XML package
- Architect
  - Basic Information
  - Conditions
  - Advice
- Three types
  - Authentication Assertion
  - Authorization Assertion
  - Attribute Assertion

Basic information - unique identifier, date, time
Conditions - dependency or rule
Advice - specifications for policy decision

Authentication Assertion – business data about successful authentication performed
Authorization Assertion – business data about an authorization decision. (An example could be an entity that can access certain resources)
Attribute Assertion – business data about attributes of an entity.
Authentication credentials are information used to authenticate an identity such as a username, password, or pin number. The entity doing the authenticating must have a copy of the user’s identity credentials. Transaction Attributes are information that describes the user’s affiliates and entitlements, such as groups that the user belongs to or his or her roles. For Federation Identity Management it can include account numbers such as health care numbers, credit card numbers, and 401k account numbers. The Roles information can include primary care physician, supervisor, or stockbroker. Profile Attributes are information that is not necessarily needed for authentication or authorization. This additional data can include addresses, birth dates, telephone numbers, and so forth. Other information can be tied to the user’s preferences such as frequent flyer number or subscription information. This information is often managed by the user, and can be used as a secondary form of authentication incase the user looses his or her password. Provider-Specific Attributes are both transaction and profile attributes that are specific to the specified SP or Web service. This can include buying history or other preferences.
These entities provide Single Sign-on service to a service requester:

- Credential Collector- collects credentials to authenticate with the authentication authority, attribute authority, and policy decision point.
- Authentication Authority- produces authentication assertions
- Session Authority- (IdP) maintains state related to session
- Attribute Authority- produces attribute assertions
- Attribute Repository- place where attribute assertions are stored
- Policy Repository- place where policies are stored
- Policy Decision Point- makes authorization decisions for itself or other entities that request authorization.
- Policy Enforcement Point- enforces security policy for granting or revoking access to resources to service requester
- Policy Administration Point- where policies are defined and maintained
Here, the system entity is the client. The client sends an application request in order to access company resources. The system entity then presents his or her credentials to the credentials collector. In order to gain access, a policy must be enforced. Therefore, the credential collector uses the credentials to authenticate with the Authentication Authority, the Attribute Authority, and the Policy Decision point. Each of these authorities uses assertions that carry the specified data to allow or deny access for the system entity. Once the Policy Enforcement Point receives these assertions, it will process the application request and grant or deny access.
Here the client authenticates with the authentication service at the source site. An application request is created to access remote resources. The SAML Responder at the remote or destination site issues an authentication assertion requesting SAML authentication assertions from the source site to see if the client has authority to assess those resources. The SAML authentication service at the source site processes the assertion and issues a response to the destination site. Now the client can access the resources without having to re-login at the destination site. This all happens seamlessly without the client’s contribution. This is SSO.
End
14.2.3 Identity Management Solutions & Consortiums

Slide 1

Identity Management Solutions & Consortiums
Instead of Liberty having participants as technology vendors, its participants include American Express, Ericsson, Fidelity Investments, Sun Microsystems, Verisign, Intel, GM, HP, and many more.

Liberty Alliance Project aims to be a distributed federated identity management model. Therefore, their standards must support all current and emerging network access devices as well as have an open SSO standard for authentication and authorization. The entire project is based on four key objectives:

1. “Enable consumers to protect the privacy and security of their network identity information”
2. “Enable businesses to maintain and manage their customer relationships without third-party participation”
3. “Provide an open single sign-on standard that includes decentralized authentication and authorization from multiple providers”
4. “Create a network identity infrastructure that supports all current and emerging network access devices” (Steel et al. 2006)
Liberty Alliance uses different terms from SAML although their protocol is an extension of SAML. Principal can be an entity such as a user that acquires a federated identity. An Identity Provider creates, maintains, and manages identity information for principles. This system entity also authenticates for SPs. A service provider offers services or goods to principles. Circle of Trusts are a federation of SPs that are partners through the Liberty architecture. Business transactions can be seamless within the CoT. Liberty-enabled Clients know how to obtain knowledge about IdPs in order for the principle to use a SP. Liberty-enabled Proxy is an HTTP proxy that acts as a Liberty-enabled client. (Steel et al. 2006)
Single Sign-on involves using context-sensitive cookies and multi-authentication systems. Cross-domain SSO is seamless logins across security domains within a CoT. Federated SSO is seamless logins across multiple CoTs. IdPs therefore must communicate with each other.

Global logout in Liberty Alliance is done when the user agent requests a logout through the SP, which then requests a global logout within the CoT. The federated identity of the user and the session index, which are maintained through the IdP, are required to perform this task.

Federated Data Exchange uses extensive schema, mappings, and strong cryptographic mechanisms between partners. B2B transaction support provides asynchronous communication and non-repudiation. Web Services are business services that SPs use SOAP protocol profiles to allow Liberty-enabled entities to communicate with one another. (Steel et al. 2006)
The Federated Identity Life Cycle involves the principle registering his or her federated identity. The single sign-on process is performed. Upon completion of user activity, the principle performs global logout and the federated identity is terminated. The meta-data used in Liberty Alliance is a framework or schema that describes cryptographic keys, service end-point information, and support protocols and profiles. Digital signatures are used to verify the origin and documents containing these meta-data. There are three classes of meta-data listed above. These lists the type of information and formats exchanged between the different entities. The information includes user account identity information, authentication context or authentication methods, and provider meta-data (information about the provider exchanged before authentication data is exchanged). Static conformance requirements define profiles Liberty Alliance entities (i.e. SPs, IdPs, and Liberty-enabled entities). Interoperable conformance and validation is a process used for vendors who want to be a licensed as Liberty-interoperable. Security mechanisms, such as channel security mechanisms (certificates and HTTPS for redirects) and message security mechanisms for data integrity and non-repudiation (digital signatures) are used. (Steel et al. 2006)
ID-FF 1.2 includes opt-in account linking, simplified sign-on, basic session management, user affiliation with Web sites, anonymity of user identities, real-time discovery protocol, and exchange of meta-data.

ID-SIS includes these two profiles that define the user attributes for exchanges of information among SPs and IdPs over ID-WSF.

ID-WSF includes permission-based attribute sharing, identity service discovery, interaction service, SOAP protocol binding, support for non-HTTP devices, and identity service templates. The ID-WSF defines security mechanisms to secure the exchange of identity information between applications and participants. These mechanisms address Request Authentication, Response Authentication, Request/Response Correlation, Replay Protection, Integrity Protection, Confidentiality Protection, Privacy Protections, Resource Access Authorization, Mitigation of DoS attack risks. (Steel et al. 2006)
Using URIs in the headers of the HTTP-redirect-based redirection allows Liberty-enabled entities to locate IdPs and SPs when performing authentication procedures. For instance, in this example, the SP redirects to the IdP with the IdP’s URI in the HTTP GET header (http://www.myidentityprovider.com/auth). The same goes for the IdP responding with a different URI for the SP. (Steel et al. 2006)
Microsoft .NET Passport

- Suite of services to authenticate users
- Purpose: To allow companies to outsource part of its administration tasks
- Objective: To make company Web sites easier for customers
- Centralized Identity Management Model
- .NET Passport Single Sign-in Service

.NET Passport Single Sign-in Service allows users to create a single set of credentials that will allow them to sign into participating sites.
Users are given the convenience of only having to remember one username and password. They can also update their Passport profile with other personal information that identifies them so that participating sites that recognize this data will allow the user to have a more personalized experience. Reduced cost and ease of administration are achieved by the participating site not having to build, host, or maintain authentication services. There is also no need for development and support. A downside to Microsoft .NET Passport is that it will not work if the user does not have cookies enabled. Cookies are a security risk.
In the registration process, the user can explicitly define what information gets stored in his or her profile. Credentials are the user’s email address, password, security questions and answers, and security keys. Profile information is the user’s personal data such as his or her name, birth date, country, occupation, address, and so forth. The credentials are never shared with participating sites; however, the personal information can be shared at the user’s request.

The Authentication Process entails signing in and out of .NET Passport, email address and password controls, operational communication, SSL channels, using security keys, cookies, and the use of profile information.

The Profile Management Process allows the user to change their settings and profile information by signing directly into memberservices.passport.com.
IBM Tivoli Identity Manager

- One of IBM’s many Tivoli software products
- Purpose:
  - deliver quality service
  - manage risk and compliance
  - maximize return on investments
  - accelerate business growth
- Objective: Provide a secure, automated, and policy-based solution that helps effectively manage user privileges across heterogeneous IT resources.
- Isolated Identity Management Model

IBM Tivoli Manager is one of IBM’s Tivoli software products to help corporations cope with the demands of increased scale, scope, and availability surrounding them as they grow in Information Technology.
IBM Tivoli Identity Manager

- User Access Roles and Entitlements
- Streamlined Self-Service Interface
- Wizards and Templates
- Auditor Compliance Reports
- Pre-installed Adapters
- Customizable User Interface

This slide lists some benefits of using IBM Tivoli Identity Manager. (http://www-306.ibm.com/software/tivoli/products/identity-mgr/)
IBM Tivoli Manager Entities

- Users, Accounts, Attributes
  - Person
  - Business Partner Person (BPPerson)
  - Custom Person
- Passwords
  - Password Synchronization
- Group Memberships
- Managed Systems and Applications
  - Operating Systems
  - Database & Business Applications

Users with multiple accounts benefit from password synchronization, which affects:

- Creating a new account
- Changing a password for an existing account
- Provisioning an account
- Resetting an expired or forgotten password for an existing account
- Restoring an account that was suspended
Tivoli Manager uses an organizational tree to define the structure of the organization it is managing. The tree starts with the organization itself, then the locations of the organization, then the departments in each location. Business partners are also included in the tree as well as administration domains are defined in the tree. Again, users are delegated to groups to define functions that they can perform in Identity Manager. ACIs define the access privileges a user has. A provisioning policy defines what accounts can be created for a user, and defines a specific approval workflow process that has to be applied to the accounts. A password policy sets parameters that all passwords must meet (length, type of characters allowed and disallowed, and password expiration). An Identity Policy defines how a user's ID is. A service selection policy provisions a specific instance of a service based on personal attributes (for instance printing). A workflow is a set of steps or activities that define a business process. Like most software, multiple types of logs are maintained by the system. With Tivoli Manager, reports can be generated from these logs. Tivoli also provides 22 predefined template reports for auditing and compliance.
Users can manage their own login functions, design what appears on their home page, have optional password synchronization, and challenge questions. Administrators can manage people and accounts from a centralized location (creating accounts, applying policies, searching for entities, flagging accounts, and applying workflows to accounts). Email notifications, customized or templates, can be either system notifications that require no action or manual activity notifications. Much of the data, such as policies and groups, can be imported and exported from Identity Manager.
Shibboleth

- Middleware Architecture Committee for Education (MACE)-Internet2 Middleware Initiative
- released June 2003 - v. 2 March 2008
- Purpose: To support authenticating users and authorizing access between IM and resource provider domains while enabling user privacy.
- Objective: To facilitate sharing of resources and collaboration
- Goal: To protect servers, communications, networks, hosts, personal information & build Trusts
- Open source software

Using open source software allows the Shibboleth system to gain input from various organizations in academics and Industry.
This slide lists benefits of the Shibboleth System.

- Single Sign-On
- Account management
- Access Management
- Protected web-based resources
- Privacy Based on Policies
- Just-in-time authorization decisions
- Authorization tools for sites
This slide discusses why Shibboleth uses SAML and how it works in a Federated environment.
This slide discusses how Shibboleth provides applications with user attributes to make authorization decisions where these applications would not have had the ability to access directory information to make these decisions.
Identity Provider – Authentication and attributes

Service Provider – requested resources

Where Are You From – directory of service providers

Assertion Consumer Service - Consumes SAML authentication assertions

Attribute Requester – requests defined SAML attribute assertions of identity to be sent to the SP

Attribute Authority – provides attributes of the user’s identity to SP from defined policies and preferences in directory of IDP

Handle Server – provides redirection mechanisms to handle the queries made between SP and IDP

Federation – Key management and provider of metadata

*The Shibboleth System Flow was obtained from the publication below:*

The user goes to a protected resource, e.g. www.acm.com. The user then requests to be authenticated by Shibboleth. Resource passes control to the SP’s Assertion Consumer Service.

*The Shibboleth System Flow was obtained from the publication below:*

The SP’s Assertion Consumer Service redirects user to the “Where Are You From” service (WAYF). WAYF asks the user who their Identity Provider is. WAYF redirects user to their IdP’s single sign-on system.

*The Shibboleth System Flow was obtained from the publication below:*

The user then logs in to their IdP’s single sign-on system. The IdP’s single sign-on system authenticates user.

*The Shibboleth System Flow was obtained from the publication below:*

IdP’s single sign-on system redirects the user to the SP’s Assertion Consumer Service providing a unique handle for session.

*The Shibboleth System Flow was obtained from the publication below:*

The SP’s Attribute Requester uses handle to request needed information about the user from the IdP’s Attribute Authority. The IdP’s Attribute Authority retrieves requested attributes about the user from the campus directory and transmits securely to the SP. Upon receiving appropriate attributes, the SP authorizes the user’s request to access resource.

The Shibboleth System Flow was obtained from the publication below:

This slide gives some usage scenarios for the Shibboleth System.

- Digital Library Resources
- Distance Education
- Research Web Sites
- Co-taught Classes
End
14.3 Lab Diagrams

Lab 1 Network Diagram
Demonstrating Authentication through Single Sign-On in an Intra-Domain

OS – Windows or Linux-based
Should be able to authenticate with IdP as its local server

Client

Identity Provider

OS – CentOS 4 or 5; Windows (under IIS or Apache)
Shibboleth SP Software

Service Provider

OS – Windows / Linux-based
Shibboleth IdP Software
Directory Service (LDAP or Active Directory)
Apache HTTP
Tomcat

(Single Sign-On)

(Initial Login)

(Authentication Information Shared)
Lab 2 Network Diagram

Demonstrating Authentication and Authorization in an Inter-Domain
15. REFERENCES


   http://www.xml.com/lpt/a/2005/01/12/saml2.html/


   http://shibboleth.internet2.edu/about.html
