IS414T
User Authentication Systems and Role-Based Securit
[Onsite]

Course Description:

The course introduces various systems and techniques that are used to authenticate users. The course also discusses how users can be assigned permissions based on the role they perform in an organization.

Prerequisite(s) and/or Corequisite(s):

Prerequisites: IS312T Information Security Essentials or equivalent, IS314T Security Architecture of Common IT Platforms or equivalent

Credit hours: 4

Contact hours: 60 (36 Theory Hours, 24 Lab Hours)

SYLLABUS: User Authentication Systems and Role-Based Security

Instructor: _____

Office hours: _____

Class hours: _____

MAJOR INSTRUCTIONAL AREAS

1. History and need for user authentication systems.

2. Various user authentication systems.

3. Three factors of authentication.

4. Difference between role and account-based security.

5. The implementation of role-based security in operating systems and the use in various access control models.

6. Application of digital signatures.

7. Various biometric techniques.

8. Enrollment, verification, and authentication.

9. Biometric authentication technology.

 Date: 8/25/2006

10. Application of cryptography to authentication through IPSec.

COURSE OBJECTIVES

After successful completion of this course, the student will have the opportunity to:

1. Explain token-based authentication system in the “something you have,” “something you know,” and “some thing you are” technologies.
2. Explain the factors to be considered in deploying a biometric system according to accuracy, cost, error rate, and intended use as well as the value of the assets that are being protected.
3. Explain the provisions of a multi-factor authentication system to strengthen the identification and authentication process.
4. Configure Kerberos on a Linux System.
5. Explain the need for physical security and the technologies available to implement physical security.
6. Explain the current cryptographic techniques used in authentication system.
7. Research the cross-over error rate and its significance.
8. Configure Kerberos on Windows 2003 Domain to include IPSec.
9. Compare the current access control technologies and the value of using biometrics with access control technologies.
10. Use the ITT Tech Virtual Library to conduct detailed research into existing and evolving biometric authentication systems.
11. Discuss examples of physical security in the preventive, investigative, and remedial control measures model.
12. Explain Tempest as it relates to physical and electronic security.

Related SCANS Objectives

- Interpret security data and effectively communicate the related information on the user Authentication system.
- Apply knowledge for multiple systems for “Defense in Depth principals.”
- Determine if mixing of system is appropriate for different technologies.
- Identify the effects of the calibration of the Biometric system.
- Acquire security related data and evaluate it for the purpose of implementing security policy of the organization.
- Create new security policies and improves existing security policies to ensure effective security system implementation in the organization.

TEACHING STRATEGIES

The curriculum is designed to promote a variety of teaching strategies that support the outcomes described in the course objectives and that foster higher cognitive skills. Delivery makes use of various media and delivery tools in the classroom.

COURSE RESOURCES

Textbook Package:

Components include, but are not limited to, the following items:

- Student Textbook Package:
  - Textbook: Smith, Richard E. and Paul Reid. *User Authentication Systems and Role-Based Security. Indianapolis: Pearson Learning Solutions, 2006.*
  - LabSim CD: Security +
- Other:
  - Database Security LabSim CD

References and Resources

- ITT Tech virtual Library (with Path)

  - Books > Books 24x7 > ***Advanced CISSP Prep Guide: Exam Q&A*** *> Chapter 2:* Access Control
  - Books > Books 24x7 > ***Advanced CISSP Prep Guide: Exam Q&A*** *> Chapter 10:* Physical Security
  - Books > Books 24x7 > ***Certified Information Systems Security Professional Study Guide*** *> Chapter 1: Accountability and Access Control CISSP*
  - Books > Books 24x7 > ***Cisco Security Bible >*** *Chapter 10: Cisco AAA*
  - Books > Books 24x7 > ***Data Integrity Digital Signatures*** *> Chapter 4*
  - Books > Books 24x7 > ***Privacy Protection and Computer Forensics, Second Edition*** *> Chapter 15: Biometrics: Privacy versus Nonrepudiation*
  - Books > Books 24x7 > ***Security+ Certification Training Kit (CompTIA Exam SY0-101)*** *> Chapter 7: User Security*
  - Books > Books 24x7 > ***Security Professional Certification Bible*** *> Chapter 2:* Basic Principles of System and Network Security CIW
  - Books > Books 24x7 > ***Study Guide, Second Edition (SYO-101)*** *> Chapter 6:* Securing the Network and Environment Security
  - Books > Books 24x7 > ***Technology, Policy, and Legal Issues Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves*** *> Chapter 9: Digital Signatures and Certification Authorities*
  - Books > Books 24x7 > ***Timesaving Techniques For Dummies*** *> Technique 30-* Customizing Authentication with PAM Linux

Other:

- Books: NIST 800-12>Physical Security>Chapter 12
- Websites:
    - http://www.searchsecurity.com

      This website provides some of the best security-specific information resources for enterprise IT professionals.

    - http://csrc.nist.gov/rbac/

      This website deals Role-Based Access Control, which is one of the most challenging problems in managing large networks.

    - http://csrc.nist.gov/rbac/RBAC-case-studies.html (Role-Based Authentication Case Studies for use as supplemental labs)

      This website provides links to a number of Role-Based Access Control case studies, which may be useful in planning for RBAC implementations.

- Other:

    - AVI short Video showing the:
        - Enrollment phase for a representative Biometric System for Eye and Voice recognition used together
        - Eye tracking portion
        - Iris tracking portion

EVALUATION & GRADING

COURSE REQUIREMENTS

1. **Attendance and Participation**

   Regular attendance and participation are essential for satisfactory progress in this course.

2. **Completed Assignments**

   Each student is responsible for completing all assignments on time.

3. **Team Participation (if applicable)**

   Each student is responsible for participating in team assignments and for completing the delegated task. Each team member must honestly evaluate the contributions by all members of their respective teams.

Evaluation Criteria Table

The final grade will be based on the following weighted categories:

Categories	Weights (%)
Participation	10%
Research Assignments	15%
Lab Assignments	20%
Quizzes	10%
Project 1	10%
Project 2	10%
Project 3	10%
Final Exam	15%
Total	100%

Grade Conversion Table

Final grades will be calculated from the percentages earned in class as follows:

A	90-100%	4.0
B+	85-89%	3.5
B	80-84%	3.0

C+	75-79%	2.5
C	70-74%	2.0
D+	65-69%	1.5
D	60-64%	1.0
F	<60%	0.0

COURSE OUTLINE

Unit #	Activities for the unit

1	• Read
	  ○ Chapter 1: Authentication Technologies
	  ○ ITT Tech virtual Library Books > Books 24x7 > Security Professional Certification Bible > Chapter 2
	• Research Assignment: 1
	• Lab: 1
	• Lab: 2 from Appendix II
	• Quiz: 1

2	• Read
	  ○ Chapter 2: Protecting Privacy with Biometrics and Policy
	  ○ ITT Tech Virtual Library > Books > Ebrary > Biometrics Personal Identification in Networked Society > Chapter 3
	• Research Assignment: 1
	• Quiz: 1
	• Lab: 1 from Appendix II

3	• Read

	○ Chapter 3: Authentication Tokens • Research Assignment: 1 • Quiz: 1 • Lab: 1 from Appendix II • Project: 1 Start
4	• Read ○ Chapter 5: Design Patterns • Lab: 1 • Lab: 2 from Appendix II • Project: 1 Submit
5	• Read ○ Chapter 7: Local Authentication • Research Assignment: 1 • Lab: 1 • Lab: 2 from Appendix II
6	• Read ○ Chapter 6: Challenge Response Passwords • Research Assignment: 1 • Quiz: 1 • Lab: 1 from Appendix II

7	• Read
	  ○ Chapter 4: Kerberos and Windows 2000
	  ○ ITT Tech Virtual Library > Books > Books 24X7 > Cisco Security Bible > Chapter 10
	• Lab: 1
	• Lab: 2 from Appendix II

8	• Research Assignment: 1 • Lab 1: Kerberos Lab for Linux • Lab: 2 from Appendix II
9	• Read ○ ITT Tech virtual Library > Books > Books 24x7 > Advanced CISSP Prep Guide: Exam Q&A > Chapter 10 • Research Assignment: 1 • Quiz: 1 • Lab: 1 from Appendix II • Project: 2 Initiation and Submission

10	• Read
	  ○ Chapter 11: Recommended Biometric for Network Security
	  ○ Chapter 13: The Future of Biometric Authentication
	• Research Assignment: 1
	• Lab: 1 from Appendix II
	• Quiz: 1
	• Project: 3 Start

11	• Project: 3 Submission

	• **Final Exam**

INTENT/INTERFACE

The purpose of this course is to understand the methods of insuring the identity of a user in order to determine the appropriate level of access. The student will learn the difference between identification and authorization as it applies to information security. The student will understand the need for strong authentication in today's systems. The goal is to analyze and discuss the strengths and weaknesses of various systems within various industry sectors. This course supports the tenants of authorization and accountability in the CIAAAA and non-repudiation model.

