CS433 – Computer Systems Security

Student Module

NOTE: For pre-requisites, first night assignment, and required class materials, see course overview.

Course Description

CS 433 COMPUTER SYSTEMS SECURITY (3). Introduces the concept of security in computing. Topics include cryptography, program security, operating systems protection, database security, and network security. Students will explore current security models, internal and external security threats, privacy issues and security laws and regulations.

Course Outcomes

After successful completion of this course, you will be able to:

- Discuss the role of information in the world today along with the importance protecting that information from unauthorized disclosure.
- Explain the basic concepts involved with cryptography along with its contribution to the authentication and encryption schemes used to secure computer systems and resources.
- Discuss the protection of computer software in both an applications program and an operating systems environment including the identification and elimination of virus software.
- Describe methods used to secure wired and wireless networks from both the many well-known and documented attacks of today as well as those attacks yet to be developed.
- Describe the importance of the development of a security policy for the computer environments of today along with the contents of that security policy.
- Discuss the legal and ethical issues involved with securing computers systems, networks, and information.

Grading Scale

The course instructor may use either of the following grading scales:

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>93-100</td>
<td>A</td>
</tr>
<tr>
<td>90-92</td>
<td>A-</td>
</tr>
<tr>
<td>87-89</td>
<td>B+</td>
</tr>
<tr>
<td>83-86</td>
<td>B</td>
</tr>
<tr>
<td>80-82</td>
<td>B-</td>
</tr>
<tr>
<td>77-79</td>
<td>C+</td>
</tr>
<tr>
<td>73-76</td>
<td>C</td>
</tr>
<tr>
<td>70-72</td>
<td>C-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>90-100</td>
<td>A</td>
</tr>
<tr>
<td>80-89</td>
<td>B</td>
</tr>
<tr>
<td>70-79</td>
<td>C</td>
</tr>
<tr>
<td>60-69</td>
<td>D</td>
</tr>
<tr>
<td>59 or lower</td>
<td>F</td>
</tr>
</tbody>
</table>
67-69  D+
63-66  D
60-62  D-
59 or lower  F

Academic Dishonesty

Regis University is committed to intellectual integrity in its academic pursuits. Sanctions may, therefore, be imposed by the School for Professional Studies Undergraduate faculty, departments, or programs for cheating (defined as using inappropriate sources of information on a test) or plagiarism (defined as presenting as one’s own, the ideas, words, or products of another). Such sanctions may include a failing grade on the assignment, failure of the course, or expulsion of the student from the course or the department.

Attendance/Participation

The expectation is for students to attend all class sessions. Because of the accelerated nature of the course work in the School for Professional Studies, missing any class may have a negative impact on the student’s learning and course performance. Any student who misses the first class must contact the facilitator/instructor or the Faculty and Curriculum Department either prior to the first class session or as close to the first class session as possible. If a student fails to do so, he/she will automatically be dropped from the course. A student who has not attended the first class session may be admitted to the course only with facilitator/instructor permission.

Make up work may be required if the student misses a class. This work is arranged, in advance if possible, between the facilitator/instructor and the student. The student is responsible for contacting the facilitator for the additional assignments(s).

Grade of Incomplete

A grade of Incomplete or ‘I’ denotes that the required work for the course is incomplete due to unforeseen circumstances. Unforeseen circumstances mean, for example, that an accident, an illness, a death, or a major life transition has occurred. This grade is awarded at the discretion of the instructor and is submitted with an alternate grade of “I/F.”

A student must submit a written request to the instructor asking that an incomplete grade be assigned prior to the end of the term in which the course is taken. The course instructor will determine the length of time for course completion, and the remaining requirements to complete the course; however the maximum time for completion is the end of the following semester. Faculty will notify students in writing of the approval/denial of their request and provide instructions and guidelines required to resolve the incomplete grade. If the course work is not completed by the end of the next applicable semester and a grade change form submitted by the instructor, the incomplete grade reverts to the alternate grade assigned by the instructor and is calculated in the grade point average.

© Regis University 2005 All Rights Reserved
CS433 10.29.2005
Learning Topics

Learning Topic #1: Overview of Computer Security
Learning Topic #2: Encryption and Cryptography
Learning Topic #3: Program Security and Viruses
Learning Topic #4: Operating System Security
Learning Topic #5: Database Security
Learning Topic #6: Network Security
Learning Topic #7: Security Administration
Learning Topic #8: Legal and Ethical Issues
Learning Topic #1: Overview of Computer Security

Computer security involves the protection of all facets of a computer system: the hardware that defines the computer system, the software that operates within the computer system, and the information that is stored and processed. Various types of attacks can be used to capture information, destroy information, deny access to information, etc. Access controls can be used to deny unauthorized access to the physical environment, the devices, the data, the communication links, the application software, and the operating system.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Define the major components of a computer system that may be subject to attack.
- Describe the basic attacks that can occur on computer systems.
- Discuss access controls that can be used to reduce the exposure of the various vulnerabilities.
- Describe the many categories of criminals involved in computer crime.

Suggested Discussion Questions

- Identify the damage that can be caused from electronic espionage.
- Identify the damage that can be caused when the integrity of a computer system has been compromised.
- Describe the differences between a threat and a vulnerability.
- Describe some different approaches to accomplishing security of the physical premises.
- Discuss a recent computer security failure that may have been reported in the newspaper.
Learning Topic #2:  Encryption and Cryptography

There are two general categories of computer security attacks: passive and active. Passive attacks, such as eavesdropping, are hard to detect because the intruder is only listening and not leaving any tracks. The primary approach to thwarting passive attacks is to use encryption to disguise the data. With active attacks we generally want to insure ourselves against damage. The process of authentication is used to help thwart active attacks by insuring the data was sent by the original sender and not modified in transit. Cryptography algorithms are used in both the encryption and authentication processes to conceal key information for accomplish adequate security of the computer system.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Describe how encryption protects against passive attacks, like eavesdropping, and how to protect against an active attach such as falsification of data, using authentication.
- Explain the basic process of encryption and decryption.
- Discuss efforts to compromise encrypted data using cryptanalysis.
- Explain approaches at cryptography using substitution ciphers and transpositions.
- Discuss encryption algorithms used today such as DES, RC4, and AES along with any advantages and disadvantages between them.
- Explain the process and benefits of public key encryption.
- Discuss the generation of digital signatures along with the use of certificates to protect information.

Suggested Discussion Questions

- What characteristics would make an encryption absolutely unbreakable?
- Given the speed of a current ordinary computer, estimate the amount of time necessary to crack a DES encryption by testing all $2^{56}$ possible keys.
- Make a similar estimate for a 128-bit AES key.
- List a type of data whose lifetime is approximately one day, one year, and one century.
Learning Topic #3: Program Security and Viruses

Viruses are a special type of security breach; they are programs that impact a computer system instead of a hacker, and they can be easily planted into an unprotected company network. This impact can be data that is either damaged, changed, or merely compromised, or it can affect computer services such as an e-mail server. There are many different types of viruses; some examples are worms, Trojan horse attacks, macro viruses, boot sector viruses, file infectors and VB scripts. Program controls exist to limit the impact of one program onto another.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

• Describe how virus programs attach to the vehicle used for penetration into the network.
• Explain how virus programs gain control of a computer system.
• Describe the signature of a virus and how that signature can be used to identify the virus.
• Describe the various types of viruses, how they are different, and how they attack the computer system.
• Discuss how anti-virus software works and eliminates virus software from a computer system.
• Explain the use of sound programming practices along with peer review to minimize exposures that exist in software applications.

Suggested Discussion Questions

• What is the most important characteristic of good design to be considered when creating secure applications?
• What computing environments are susceptible to virus attack?
• Make a list of hazards that should be included on a hazard list for a new program.
Learning Topic #4: Operating System Security

A computing environment consists of a number of elements such as memory and the information stored in it, application software, files stored on disk, and CPU cycles used to process information. The single entity charged with the responsibility of managing all of these elements is the operating system; it supplies efficient access to the elements in a multi-user environment while maintaining their integrity. Computer resources are protected using a number of techniques ranging from architecture issues such as memory fence registers, to access control lists that are used to determine privileges to resources, to user authentication which is used to determine who has access to the entire computing environment. The goal is to develop trusted operating systems that allow the sharing of computer resources without subjecting them to unauthorized disclosure.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Discuss the elements of a computer system whose access must be controlled in a multi-programming, multi-user environment.
- Describe techniques used by an operating system to ensure the integrity of the memory resource.
- Describe techniques used by an operating system to protect stored data from unauthorized disclosure or malicious damage.
- Discuss various approaches used by operating systems to authenticate the users that want access.
- Explain the importance of adopting a strong password policy.
- Explain the use of biometrics when authenticating users.
- Discuss the contents of a security policy along with some of the security models in existence.
- Compare the security features found in ordinary operating systems and trusted operating systems.
- Describe the security advantages of a layered design for operating systems.
- Explain methods used in the assuring a system against its vulnerabilities.

Suggested Discussion Questions

- Compare the merits of using an access list approach versus a capability list approach when determining the access rights to a protected resource.
- Explain the benefits of combining paging and segmentation in a memory protection system.
- What are the advantages and disadvantages of using a challenge-response system for user authentication?
- Make a list of security rules combining the secrecy controls of the Bell-La Padula model with the integrity controls of the Biba model.

© Regis University 2005 All Rights Reserved
CS433 10.29.2005
Learning Topic #5: Database Security

Computer security includes the protection of electronic information from access, use, alteration, or destruction by unauthorized users. Much of the data maintained within a computer system may be sensitive in that we need to insure its accuracy (data integrity) and safeguard its content (confidentiality) by restricting access based on a need-to-know policy. Databases of today house all of our credit card information, salary information, banking information, investment information, medical information, etc. This is data whose confidentiality is of the utmost importance. The database environment is managed using a database management system (DBMS), a collection of software applications that control the accessibility and utilization of data stored within the database. Yet, over the past few years there have been several occurrences of the security that protects this data being compromised. As the amount of sensitive information stored within databases is continuing to increase rapidly, the need to secure that data is a high priority task. One of the more recent approaches to security is the multi-level database environment. By presenting the hacker with multiple levels of security, you provide an environment in which the level of effort required may be greater than most attackers will want to apply. Each layer of the defense serves to deter the attacker from going further in the attack, and may eventually give up without successfully penetrating the security.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Discuss database and DBMS terminology.
- Identify the advantages and disadvantages of hosting information from a database repository.
- Describe the requirement to protect the integrity and confidentiality of sensitive information.
- Explain various approaches used by a DBMS to maintain database integrity such as transaction logging, the two-phase update, data consistency, database recovery, range comparisons, and state and transition constraints.
- Explain various approaches used by a DBMS to maintain the confidentiality of data such as user authentication and access controls.
- Describe some of the attacks that can be perpetrated on a data repository such as an indirect attack, a tracker attack, and an inference attack along with some of the resulting costs.
- Explain the advantages of organizing the security policy for database protection into multiple layers (a multi-level database).
- Discuss design issues of the multi-level database.

Suggested Discussion Questions

- Using the two-step commit we discussed earlier, describe how to avoid assigning the same seat to two different people in an airline reservation system.
- Can a database contain two identical records without a negative effect on the integrity of the database? Why?
• Cite an example where the sensitivity of an aggregate is greater than that of its constituent values.

• What security features of an operating system can be used to simplify the design of the DBMS?
**Learning Topic #6: Network Security**

The proliferation of computer networks has done much to change the way people work, live, and get educated. The rampant increase in the popularity of wireless networks has added another level of urgency to the issue of protecting information while it is being communicated between computer sites. Today, many resources are deployed by organizations to face the daily challenge of network security. Passive attacks like a sniffer attack, a man-in-the-middle attack, or a war driving attack threaten the confidentiality of our data. Active attacks like the replay attack, a data modification attack, or even a virus attack threaten the integrity and reliability of the transmitted information. As with database security, one good approach to network security is the layered defense. Again, the idea is to present successive layers of protection so that the failure of one security component will not result in the complete compromise of the network. Each layer of the defense serves to deter the attacker from going further in the attack, and may eventually cause him/her to give up without successfully penetrating the network.

**Topic Outcomes**

Upon completion of this learning topic, students will be able to:

- Discuss computer network terminology.
- Identify the advantages and disadvantages of the use of a computer network.
- List the vulnerabilities of a computer network.
- Explain the types of threats to network security and the importance of security requirements.
- Identify and describe the various attacks that can occur on a computer network.
- Describe the use of WEP, WPA, and WPA2 protocols to accomplish encryption and authentication used to identify users and protect data.
- Discuss the use of a virtual private network (VPN) to establish a secure networking environment.
- Explain the multi-level approach to protecting your computer network environment.
- Describe the many types of firewalls an organization can use along with their benefits.
- Describe the use of intrusion detection systems and how they work with customer firewalls.
- Explain the security protocols used today such as IPSec, SSH, and SSL.
- Explain the need for email security and how it is accomplished.

**Suggested Discussion Questions**

- How can a customer protect against the single point of failure involved with the last mile of a computer network connection?
- How can networking hardware be designed for fault tolerance?
- List the major security issues dealt with at each level of the OSI protocol stack.
- Describe a social engineering attack you could use to obtain a user’s password.
Learning Topic #7: Security Administration

Computer security does not happen by accident. It requires commitment, resources, and planning. Management support is needed to convey the importance of security and that each and every employee and user are responsibility for it. One of the first and most important steps is the development, implementation, and enforcement of a security policy. This policy should address risk assessment, asset identification, physical security, systems management, incident management and disaster recovery, and user education and responsibility. The policy should clearly define what the expectations and responsibilities are for each individual in the organization.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Determine the risks and vulnerabilities to a computing environment.
- Identify the steps involved in a risk analysis.
- Describe the need for and the contents of an appropriate security policy.
- Discuss the characteristics of a good security policy.
- Discuss the importance of physical security and ensuring all potential natural disasters and perpetrated crimes are covered in the security policy.
- Develop appropriate contingency plans for each potential risk or vulnerability.
- Describe the importance of periodically testing an organization’s disaster recovery procedures.

Suggested Discussion Questions

- Identify, and justify your choices, the three most probably threats to a personal computing system in an office with fewer than 10 employees.
- List 5 types of harm that could occur to your PC; then estimate the likelihood of each along with the potential cost.
- Determine an adequate disaster recovery plan for your personal computer.
Learning Topic #8: Legal and Ethical Issues

Computer resources, just like any other resources, deserve the protections afforded by the law. These resources include software programs, data, and corporate trade secrets in addition to the actual computer system itself. However, the traditional approaches that have been taken to protect computer resources have just, for the most part, been extensions of the current laws. This has resulted in the prosecution of a computer crime being difficult at best. Issues like the lack of physical evidence and the lack of understanding of the computer environment by much of the legal profession make these crimes hard to prove. New laws that address computer crime are needed to reverse this trend. Computer ethics is an even more vague subject. The problem is that it is difficult to always understand what the morally correct choice of action is in conflicting situations.

Topic Outcomes

Upon completion of this learning topic, students will be able to:

- Identify computer resources that deserve legal protections from computer crime.
- Discuss the applicability of laws governing copyrights, patents, and trade secrets to the protection of computer resources.
- Discuss the rights of employees and employers.
- Define what is meant by computer crime.
- Discuss the reasons for developing new and separate laws to govern computer crime.
- List recent laws that help define computer crime.
- In this age of information availability, discuss issues of personal privacy.
- Discuss the difficulty of always making appropriate ethical decisions in today’s world.

Suggested Discussion Questions

- What are the drawbacks and benefits to using computer voting machines at all precincts?
- Cite at least three examples of our privacy being for sale.
- What kinds of penalties should be applied to those that hack into computer systems in order to compromise the data stored there.

Resources

http://en.wikipedia.org/wiki/Main_Page
http://www.infosyssec.com/infosyssec/index.shtml
http://www.cosead.com/