ITM 643: Incident Handling

Sanjay Goel
School of Business
University at Albany, State University of New York

INSTRUCTOR INFORMATION

Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b, University at Albany
Office Hours: TBD

CLASS INFORMATION

Time: N/A
Location: Online
Dates: TBD
Credit(s): 3
Call #: TBD

RESOURCES

Website: http://www.albany.edu/~goel/classes/

There is one text for the class with separate readings assigned from various sources. In addition, there are several reference books and materials that you can refer to for further information if necessary.

Text:

References:

Scarfone, K., Grance, T., & Masone, K. (2008). Computer Security Incident Handling Guide. NIST SP 800-61. Revision 1. *National Institute of Standards and Technology.* http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

West-Brown, M.J., Stikvoort, D., Kossakowski, K-P., Killcrece, G., Ruefle, R., & Zajiceck, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). 2nd ed. *Carnegie Mellon University, CERT Coordination Center.* http://www.cert.org/archive/pdf/csirt-handbook.pdf

Readings: Reference readings will be posted at the end of each presentation. Available readings will be accessible via http://eres.ulib.albany.edu You must click on "Electronic Reserves & Reserve Pages" and then type in "ITM643" in the empty box. Click under the Course Number section (which is hyperlinked) you will be asked to input a password. The password to access this information will be provided via email and is case-sensitive. All of the readings is divided by Unit and contains readings in pdf format or web links to readings.

COURSE OVERVIEW

Responding to security incidents is an important part of managing information security in an organization. Despite the best security infrastructure and policies in place, security incidents are inevitable. Incident response capability is necessary for rapidly detecting incidents, minimizing their impact, remediating the vulnerabilities that led to the incident, and restoring services. In addition, if forensic analysis is required, data will be collected to preserve the evidence for an internal review or for use by law enforcement forensic team. These incidents can range from spread of malware to misuse of computers by employees. Each type of incident requires a specific handling process. This course will discuss detection, management, and recovery from

different types of incidents. It will also cover creation of Computer Emergency Response Teams (CERTs) / Computer Security Incident Response Teams (CSIRTs) and their roles. Finally, reporting and dissemination guidelines for security incidents will also be discussed including legal and policy mandated reporting of incidents.

Course Prerequisites

It is assumed that students will come in with varied backgrounds in information systems with some general background of computer security. It would be helpful if students have some knowledge of the following topics:

1. Computer Networks
2. Computer Architecture
3. Basic Information Security
4. Information Security Threats

Course Format

This course is being offered as an online course. However, the intent of the course is to provide students with an interactive learning environment through instructor audio, discussion groups, and interactive quizzes. The purpose of the course is to train students in the practice of risk analysis by elucidating the concepts through examples and case studies. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value. Even though the course is spread over 3 weeks, it is important that students stay on schedule so that they can participate with other students in discussions. The class work would include instruction video of lecture material, quizzes, discussion postings, final project, and readings.

Learning Objectives

At the end of the course, students should be able to:

1. Develop incident response policies and procedures
2. Create and train an incident response team
3. Detect and collect information for different types of incidents
4. Coordinate with other agencies and authorities in regards to incidents
5. Write incident reports, advisories, and bulletins

ASSESSMENT & GRADING

Academic Integrity Compliance: Students MUST comply with all University standards of academic integrity. As stated on the undergraduate and graduate bulletin, **"Claims of ignorance, of unintentional error, or of academic or personal pressures are not sufficient reasons for violations of academic integrity."** If a student is discovered to NOT comply with academic integrity standards, the student will be reported to the Office of Graduate Admissions or the Dean of Undergraduate Studies Office (whichever applies) AND receive either a warning, be told to rewrite the plagiarized material, receive a lowering of a paper or project grade of at least one full grade, receive a failing grade for a project containing plagiarized material or examination in which cheating occurred, receive a lowering of course grade by one full grade or more, a failing grade for the course, or any combination of these depending on the infraction.

Examples of violations include: Giving or receiving unauthorized help before, during, or after an examination; Collaborating on projects, papers, or other academic exercises which is regarded as

inappropriate by the instructor(s), Submitting substantial portions of the same work for credit more than once, without the prior explicit consent of the instructor(s) to whom the material is being (and has in the past been) submitted; misrepresenting material or fabricating information in an academic exercise or assignment; Destroying, damaging, or stealing of another's work or working materials; and presenting as one's own work, the work of another person (for example, the words, ideas, information, code, data, evidence, organizing principles, or style of presentation of someone else). This includes paraphrasing or summarizing without acknowledgment, submission of another student's work as one's own, the purchase of prepared research, papers, or assignments, and the unacknowledged use of research sources gathered by someone else. Failure to indicate accurately the extent and precise nature of one's reliance on other sources is also a form of plagiarism. The student is responsible for understanding the legitimate use of sources, the appropriate ways of acknowledging academic, scholarly, or creative indebtedness, and the consequences for violating University regulations.

If you ever have any questions about whether you could be violating academic integrity standards - ASK!

Grading Rubric

Quizzes/Exams (20%) – Please work individually on all quizzes/exams. Two exams will be offered after during the course. Please go to the Toolbar and click "Other Tools". Select "Assessments" and you will see the exams. This will be graded automatically via Blackboard.

Discussion Postings (30%) – Even though this is an online course, it is expected that students will be able to learn from each other and participate in a discussion. To promote this, you will be assigned discussion postings, which will be graded. Discussions will be able to be created and viewed by going to the "Discussions" link on the top right hand corner of the page. In addition to discussion postings, responses to other student posts are also required. Initial postings will generally be due on Wednesday and responses to other postings should be up by the Sunday of that week.

Assignments/Project (50%) – Students will receive assignments and exercises for this class.

COURSE SCHEDULE

	Topics	**Readings**
1	Computer Incident Handling Basics	TBD
2	Creating Teams and Setting Policies	TBD
3	Handling Malware Incidents	TBD
4	Network Probes and Attacks	TBD
5	Denial of Service Incidents	TBD
6	Unauthorized Access	TBD
7	Exam I	TBD
8	Espionage and National Security Incidents	TBD
9	Intellectual Property Theft	TBD
10	Inappropriate Use of Resources	TBD
11	CERTS/CSIRTS and their Role	TBD
12	Recording, Reporting and Dissemination of Incidents	TBD
13	Open	TBD
14	Exam II	TBD

Detailed Schedule

Week 1
Theme: Computer Incident Handling Basics
Topics:
Exercises:

Week 2
Theme: Creating Teams and Setting Policies
Topics:
Exercises:

Week 3
Theme: Handling Malware Incidents
Topics:
Exercises:

Week 4
Theme: Network Probes and Attacks
Topics:
Readings:
Exercises:

Week 5
Theme: Denial of Service Incidents
Topics:
Exercises:

Week 6
Theme: Unauthorized Access
Topics:
Exercises:

Week 7 Exam I

Week 8
Theme: Espionage and National Security Incidents
Topics:
Exercises:

Week 9
Theme: Intellectual Property Theft

Topics:
Exercises:

Week 10
Theme: Inappropriate Use of Resources
Topics:
Exercises:

Week 11
Theme: CERTS/CSIRTS and their Role
Topics:
Exercises:

Week 12
Theme: Recording, Reporting and Dissemination of Incidents
Topics:
Exercises:

Week 13
Theme: Open
Topics:
Exercises:

Week 14 Exam II