

**School of Information Science & Policy
State University of New York at Albany**

Inf 766 Incident Handling (1 Cr) ([PDF](#)) ([DOC](#))

Spring, 2004 (Call #8933)

George Berg & Jagdish S. Gangolly

Welcome

Welcome to the course on Incident Handling. The emphasis in the course will be on gaining an in-depth understanding of the information technologies necessary for dealing with computer security incidents as well as digital evidence. The course will deal with the forensic as well as computing aspects of preventive, detective, corrective, and protective measures to provide assurance that the digital evidence is admissible and the chain of custody of such evidence is maintained. The course also will consider the legal and reporting aspects of handling incidents.

The course will involve a healthy mixture of theory, applications, and exposure to the relevant technologies. While we assume that you are familiar with the use of computers, much of the background will be provided in the course. It is important that you get familiar with the working of UNIX as well as windows environments to the extent required in forensic investigations.

The course is rather fast paced. It is therefore important that you keep up with the class at all times and not be left behind. Should you need help, seek it immediately.

Enjoy the course!

Administrivia

Semester: *Spring, 2004*

Time: *Tuesdays 8:30 — 11:30 PM*

Room: *BA 222 on April 6, 2004. Venue of the rest of the sessions will be announced.*

Instructor: *George Berg and Jagdish S. Gangolly*

Phone: *(518) 442-4267 / (518) 442-4949*

Fax: *(518) 442-5638 / (707) 897-0601*

Office Hours: *TBA*

Instructor Homepages: *www.cs.albany.edu/~berg / www.albany.edu/acc/gangolly*

Course Homepage: *http://www.albany.edu/acc/courses/ia/inf766*

Class Conduct:

The course consists of lectures, discussion of book assignments, discussion of assigned cases, and laboratory sessions.

Course Objectives:

- Understanding of events and incidents and the relevant standard terminology
- Familiarity with the information technologies relevant to incident handling
- Familiarity with the technologies relevant to the storage, extraction, and preservation of digital evidence
- Familiarity with the legal and reporting aspects of incident handling

Catalog Description:

The objectives of the course are to learn what are incidents, why they occur, who/what causes them, how to detect them, what are the preventive/protective measures that organizations can take, what to do when they do occur, when do they need to be reported and to whom. We will learn the various types of incidents, what to do in case of each to protect the evidence, prevent gaps in chain of their custody. In particular, we will learn how and what kinds of evidence to obtain, how to prevent evidence from getting lost or destroyed, how to ensure that the evidence is admissible. We also will learn what is evidence, what are different types of evidence, basic rules on collecting, handling, and documenting evidence.

Textbooks and Readings:

Digital Evidence and Computer Crime (EC in the schedule)

by [Eoghan Casey](#)

Academic Press; 2nd edition (October 3, 2004)

ISBN: 0121631044

In addition, the following important documents are provided for your reference. You will find important materials there relevant to incident handling.

DRAFT Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, by Tim Grance, Karen Kent, Brian Kim, NIST Special Publication 800-61

An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce

Information Security Guideline for NSW Government – Part 1 Information Security Risk Management, Office of Information & Communications Technology, Department of Commerce, NSW Government, Australia (1997)

Information Security Guideline for NSW Government – Part 2 Examples of Threats and Vulnerabilities, Office of Information & Communications Technology, Department of Commerce, NSW Government, Australia (1997)

Information Security Guideline for NSW Government – Part 3 Information Security Baseline Controls, Office of Information & Communications Technology, Department of Commerce, NSW Government, Australia (1997)

Tentative Schedule

April 6, 2004

Theme: Introduction ([PPT](#)) ([PDF](#))

Topics: What is an incident, what are various types of incidents, How do they happen, and how they affect systems? What are the sources of information about incidents? How to use such information to learn about incidents?

Readings: Read EC Ch. 1-6.

Assignment: [Lab exercises](#), [ICAT Database](#), [CVE-FULL](#), [CVE-Candidates](#)

April 13, 2004

Theme: Introduction ([PPT](#)) ([PDF](#))

Topics: What is an incident, what are various types of incidents, How do they happen, and how they affect systems? What are the sources of information about incidents? How to use such information to learn about incidents?

Readings: Read EC Ch. 7-9. Browse 15-17.

Assignment: [Lab exercise](#)