A Course In Computer Security
For Criminal Justice Majors

John Sokol
General Engineering
Penn State Fayette
Uniontown, PA 15601

Introduction

Computers have grown as a crime factor in the worlds of both public security and private security. In recent remarks, John Ashcroft, Attorney General, stated: “Although there are no exact figures on the costs of cybercrime in America, estimates run into the billions of dollars each year. And unlike more traditional crimes, cybercrime is especially difficult to investigate.” Computers are used to facilitate traditional crimes, such as child pornography, and are also used to attack networks in a business which, in turn, shuts down the business.

Dr. Richard Ball, a Professor of Administration Of Justice at Penn State Fayette, is also a member of the Advisory Board for the Training and Research Institute of the National White-Collar Crime Conference. Dr. Ball, emerging from the White-Collar Conference meetings, encouraged the development of a computer security course tailored for non-technical students majoring in criminal justice.

Since 1992, we have offered a course at Penn State Fayette using the topic of alarm systems to cover topics in analog and digital electronics. This earlier course includes a short module on computer security. We are not training electronic specialists, but security professionals who are consumers of these electronic services. In the case of computer security, the objective is to give criminal justice students a broad background in computer security and to enhance their understanding of computer crime and computer security.

For example, computer forensics is “the process of unearthing data of probative value from computer and information systems.” A course in computer forensics is suitable for computer science students, but computer forensics in-depth is not suitable for criminal justice students. Instead, this new course will train the criminal justice major to become an intelligent consumer of the computer forensics services provided by technical experts.
Most of the materials and training programs on computer security are oriented towards the technical specialist, such as computer scientists or network professionals. For example, the CERT (Computer Emergency Response Team) training and education program at Carnegie-Mellon has only a single, short course aimed at the non-computer professional. In another well-known case, the SANS (SysAdmin, Audit, Network, Security) Institute program courses are only for network professionals. A year was spent looking for a program that we could use as a starting point for a security program for criminal justice students. This was a fruitless search. We decided to start from scratch.

Basic Course Structure

An early decision was to have a basic prerequisite that will give the students a good start for the course, without requiring too many prerequisites that would greatly limit student attendance. The selected prerequisite is IST 110, which is the introductory course for the program in Information Science and Technology. This course provides a basic introduction to computer concepts, as well as an introduction to computer applications. “Computer Concepts by June Parsons and Dan Oja” is the book currently used for IST 110.

The course is broken into three parts:

The first part is an introduction to local area networks and wide area networks and will build on the material lightly covered in IST 110.

The second part of the course focuses on the nature of computer security threats and the basic responses to these threats. The second part will also include topics on organization and planning and an overview of the methods for securing networks.

The third part of the course focuses on specific interests for the criminal justice students.

Selecting A Textbook

No book could be found to cover all three parts of this course. The easiest task was to find a book for the first section of the course providing the introduction to local and wider area networks. The book, “How Networks Work by Frank Derfler and Les Freed,” was selected because it covers the material at the desired level and it has useful graphics for each of the topics. This book begins with earliest communication systems, the telegraph and the telephone, and then quickly covers local and wider area network systems for communications.

The search for an appropriate book on network security, containing information on both threats and responses, was a more difficult task. There are many books that provide up-to-date methods to protect various networks. These books are aimed at the computer
professional. These courses are not often published as textbooks. The book called “Counter Hack by Ed Skoudis” is a good example of the book for the computer professional. There is, for example, a discussion of programs used by hackers, those who launch attacks on computer systems. This book presents information on the tools (programs) available to help protect computer networks. For example, it includes a lengthy discussion about UNIX and other specific operating systems.

“Security In Computing by Charles Pfleeger” has been developed as a textbook. However, this text focuses on cryptology and the mathematical theory for analysis. This type of mathematics is far beyond the level that could be used in a course for criminal justice students.

The book “Defending Your Digital Assets by Randall Nichols, Daniel Ryan, and Julie Ryan” has some promise as a text for the coverage of threats and responses. This book is aimed at managers to read on their own, but has also been used by these authors in an MBA course. The basic areas of this book are:

1. Digital Espionage Warfare and Information Security (INFOSEC)
2. INFOSEC Concepts
3. Practical Countermeasures
4. Enterprise Continuity Planning
5. Order Of Battle

However, there are some problems. This book draws on the military outlook rather than the view of criminal justice. For example, information security quickly becomes INFOSEC. The section on cryptography is somewhat technical. For example, the topic of the Elliptical Curve Cryptosystems is somewhat technical, but these sections do not reach the technical level of the book by Pfleeger. On the positive side, there is an interesting section on various ways to look at access controls. The section on Information Warfare covers an interesting topic, but this is not required in a course for criminal justice majors. Overall, this book is a suitable textbook for this course. If the next book had not been found, this book would have been selected as the main book for the course.

The book “Network Security: A Beginner’s Guide” was recommended early in our search for a textbook by Galen Grimes, Assistant Professor, Information Science and Technology, Penn State McKeesport, as one of the few books suitable for non-technical students. The major sections of this book are:

1. Information Security Basics
2. Ground Work (Information Security Practice)
3. Practical Solutions
4. Platform Specific Implementations

The book covers the material at a reasonable level. There are still some portions on
cryptography, but this can be covered lightly without a problem. The last section on specific platforms (operating systems) will not be used since this is material beyond the scope of a course for criminal justice majors. This is not a perfect book. For example, the discussion of hackers is at the end of the book\textsuperscript{18}; however, it might be useful as part of the beginning of the book.

Dealing With Specific Topics In Computer Crime

There are a number of criminal topics that might be covered at the end of this course:

1. Child pornography
2. Internet gambling
3. Identity theft
4. Intellectual property theft
5. Electronic stalking
6. Industrial espionage
7. Electronic fraud
8. Cyber-terrorism

The number of topics will be growing over time. The “Computer Security Handbook by Seymour Bosworth and M.E. Kabay” provides a gateway to many of these topics.\textsuperscript{19} One approach would be to use this book to cover selected topics. We decided on a different method to cover criminal justice topics.

The current plan for this last portion of the course is to make each of these major topics a special project for a number of teams consisting of three students per team. Each student will be required to research a team topic drawn at random, prepare an individual ten-to-twenty-page paper with at least five references, and participate in a 30-minute team presentation to the rest of the class. It is assumed that the class will have about thirty students.

Future Activities

Approvals for the courses in Electronics For Criminal Justice (ADMJ 432) and Computer Security For Criminal Justice (ADMJ 433) should be completed by the spring of 2003, before the ASEE 2003 meeting. They will be part of a curriculum in Private Security at Penn State Fayette. Students will be advised to take IST 110 in the fall 2003 semester and the computer security course will be offered in the following spring 2004 semester.

It is not surprising that an engineer has developed a set of criminal justice courses within the nature of the multidisciplinary environment at Penn State Fayette. Since Penn State Fayette is a small campus, creative curriculum integration is more feasible than at larger institutions. For example, Dr. Nathan Viswanathan, Professor of Chemistry, has developed a set of chemistry-related courses in the area of forensics for criminal justice students. Mr. David Meredith, Associate Professor of Engineering, teaches a course about the history of...
metals to non-technical students. The science and engineering faculty recognize the need to convey the nature of our very technical world to our students who will graduate in non-technical majors.

Bibliographic Information


10. Skoudis. pp. 73-103


Biographical Information

John P. Sokol  
Dr. Sokol is an Associate Professor who teaches courses in Electrical Engineering and Electrical Engineering Technology at the Penn State Fayette campus since 1988. He also teaches a course in Electronics for Administration Of Justice and courses in the networking program of Information Science and Technology. Dr. Sokol received an M.S. (1972) and PhD. (1975) degree in Physics from the University of Notre Dame, followed by 14 years at nuclear divisions of Westinghouse Electric Corporation.