



Applied Business &
Technology Center



Introduction to Computer and Network Security

(2 days)

Computer Security, Network Security,
Security Management

April 28-29, 2003

Foundations of Applied Security

(3 days)

Security Architecture, Cryptography,
Operations Security, Applications and Systems
Development, Law, Investigations, and Ethics,
BCP/DR, Physical Security

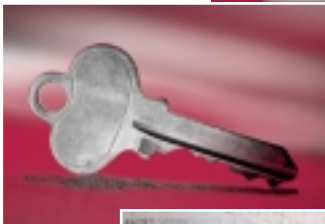
April 30-May 2, 2003

One Main Street, Houston, Texas 77002

Phone: 713-221-8032

Fax: 713-221-8166

www.uhd.edu/abtc



Security breaches cause more than U.S. \$15 billion
damage worldwide annually.

—Datamonitor

Q & A



Who should attend these classes?

Any information technology professional working in the private or public sector needs to be security aware. Combined, these classes provide a solid information system security foundation.

What technical background should the students have?

Students should be familiar with information technology. Students who are knowledgeable about networking and operating systems will readily absorb the class materials.

What will the students learn?

Essential information that includes security concepts that all professionals in a security related position should know. Specific topics include Internet, network, and computer security. Technologies covered include cryptography and access control. Preventive, detective, and reactive aspects of security are also covered.

Will the classes include hands-on labs?

Each student will have access to a personal computer to work on the lab exercises. Each student will install and configure Windows 2000 and Linux. In addition to security tools, each student will work with multimedia simulations and tutorials.

Why is security important?

In 2000, corporations worldwide due to network security breaches lost an estimated \$15 billion. The latest Computer Security Institute annual report indicates that losses due to information security compromises continue to get worse.

According to CSI Director Patrice Rapalus, even though 90 percent of their survey respondents use antivirus software, 85 percent of them were hit by viruses or worms.

Another example, the original Code Red Worm, spreads slowly. After modification, it flooded the Internet, reaching more than 350,000 servers in less than 24 hours. (Data collected by the Cooperative Association of Internet Data Analysis.)

My company just spent \$50,000 dollars on a firewall, should I go to these classes?

According to Gene Spafford, Director, Center for Education and Research in Information Assurance and Security (CERIAS), security comes from understanding systems, goals, and methods. Strong tools applied in the wrong way for the wrong reasons don't help.

For example, the CSI survey showed that even though 89% of respondents had firewalls, 40% reported system penetration from the outside. Technology alone is not the answer.

Security is only partly dependent on technology. It is also dependent on appropriate tools applied in an appropriate manner guided by an appropriate security policy.

Is the future going to be less threatening?

Statistics gathered by the Computer Emergency Reaction Team Coordination Center (CERT/CC) indicate that the number of reported security incidents doubled from 2000 to 2001. Current year information indicates that security incidents will double again from 2001 to 2002.

Information Security Magazine (September 2000), shows trends with increases in electronic theft, viruses, and employee computer access control abuse.

Are security certifications important?

The Gartner Group reports that:

Certification of information security professionals and practitioners is becoming more common as a condition of employment or as a preferred credential. Most often seen on role descriptions and resumes is the CISSP certification from (ISC)². With the growth in the use of the Internet, the GIAC certification will likely become a preferred credential for security personnel having day-to-day technical operations responsibility for ensuring an enterprise's information assets.

Will the classes help me prepare for the CISSP certification exam?

Yes. The course follows the 10 domain Common Body of Knowledge that the CISSP exam is based upon. For more information about CISSP certification visit:

<http://www.isc2.org>

It's clearly a dangerous world, and has been for years. It's not getting better, even given the widespread deployment of computer security technologies. And it's costing American businesses billions.

—Bruce Schneier, *Counterpane Internet Security*



Course Outlines

Introduction to Computer and Network Security (2 Days)

Security Management Practices

- Basic concepts: confidentiality, integrity, and availability
- Data classification systems
- Change Control
- Risk and Risk Management: threats, vulnerabilities, and informational asset valuation
- Roles and responsibilities of an information: owner, custodian, and user

Computer Security

- Mandatory (MAC) and Discretionary (DAC) access control
- Rules, roles, and lattice based control systems
- Passwords, tokens, and biometrics
- Centralized vs. decentralized methodologies
- Penetration testing and intrusion detection

Telecommunications and Network Security

- Basics: media, protocols, and standards
- Models: ISO/OSI, TCP/IP
- TCP/IP functionality: addressing, three way handshake, sliding windows
- Communication devices: firewalls, routers, switches, gateways, and proxies
- WAN services: HDLC, SDLC, X.25, and Frame Relay
- Secure communication technologies: VPNs and NAT
- Basic network attacks: ARP poisoning, flooding, sniffing, and spoofing
- E-mail and fax security

Introduction to Computer and Network Security

Length of Training:
2 Days (16 hours)

Class Dates:
Weekdays
9:00 a.m.–4:30 p.m.
April 30-May 2, 2003

Tuition:
\$595.00
includes all course materials and campus parking

Foundations of Applied Security (3 Days)

Security Architecture and Models

- Formal security standards: Common Criteria, ITSEC, TSEC, and the IETF
- Computer and network system principles: addressing, operating states, modes, and protection mechanisms
- Information System certification and accreditation
- Common architectural flaws: covert channels, initialization and failure states, input and parameter checking, EMI.

Cryptography

- Symmetric (private key) and asymmetric (public key) methods
- Message authentication and digital signatures
- Methods: PGP, DES, RSA, SHA, MD5, and triple-DES
- Public Key Infrastructure and certificates
- Kerberos, ISAMP, and IPSEC

Operations Security

- Hardware and media security controls
- Operators and resource access privileges
- Principles: separation of duties, least privilege, need to know
- Preventive, detective, and recovery controls
- Internal and external auditing
- Intrusion Detection

Application and System Development

- Security and controls for systems development
- Basic tools for data/application integrity
- Security control architecture
- Malicious code
- Attacks: spoofing, logic bombs, trap doors, and traffic analysis

Law, Investigation, and Ethics

- Major U.S. laws: three major types of laws.
- Ethical issues
- Model codes of conduct
- Evidence gathering
- Incident handling

Business Continuity Planning and Disaster Recovery Planning (Day Three)

- Business continuity planning
- Recovery plan development, implementation, and restoration
- Business impact assessments
- Recovery strategy alternatives

Physical Security

- Physical security threats
- Personnel access controls
- Audit trails
- Basic fire detection and suppression
- Facility management and planning requirements

Foundations of Applied Security

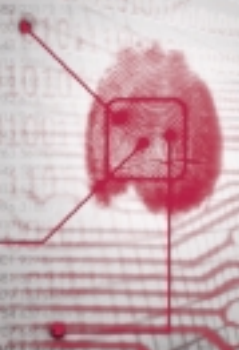
Length of Training:
3 days (24 hours)

Class Dates:
Weekdays
9:00 a.m.–4:30 p.m.
April 28-29, 2003

Tuition:
\$795.00
includes all course materials and campus parking

There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders and business partners or report to law enforcement. Incidents are widespread, costly, and commonplace....

—Patrice Rapalus
Computer Security Institute
(CSI) Director



About the Instructor

Ed Crowley is a clinical assistant professor at the University of Houston. There, he has developed and taught computer and network security courses at both graduate and undergraduate levels.

Prior to joining the College of Technology, Ed was a director at Daytona Beach Community College (DBCC). There, he created the Academic Computing Department and was responsible for the security of the college's 42 computer labs. After completing plans to network DBCC's four campuses, he directed the Computer and Communications Services Department.

He is U.S. Army Military Police Academy graduate. And he is also a graduate of USARPAC's Basic Sentry Dog School.

How to Register

By Phone

Call 713-221-8032 and give us the information requested on the registration form. Phone registration will assure you a place in the class. Mail in the completed form with your check, purchase order or credit card information to confirm your registration.

By Mail

Complete the registration form and mail it in with your check, purchase order or credit card information to:

Applied Business & Technology Center
University of Houston-Downtown
One Main Street
Houston, TX 77002

By Fax

Complete the registration form and fax it to the Applied Business & Technology Center at 713-221-8166. Mail a copy of the completed registration form with your check, purchase order or credit card information to the above address. The fax registration will assure you a place in the class.

By Internet

Access the secure webserver of the Applied Business & Technology Center website at www.uhd.edu/abtc.

Registration Form (Form may be duplicated.)

Please enroll me in the following course(s):

- Introduction to Computer and Network Security** \$595.00
 January 20-21, 2003
- Foundations of Applied Security** \$795.00
 January 22-24, 2003

NAME _____

ADDRESS _____

CITY _____ STATE _____ ZIP _____

PLACE OF EMPLOYMENT _____ DAYTIME PHONE _____

E-MAIL ADDRESS _____

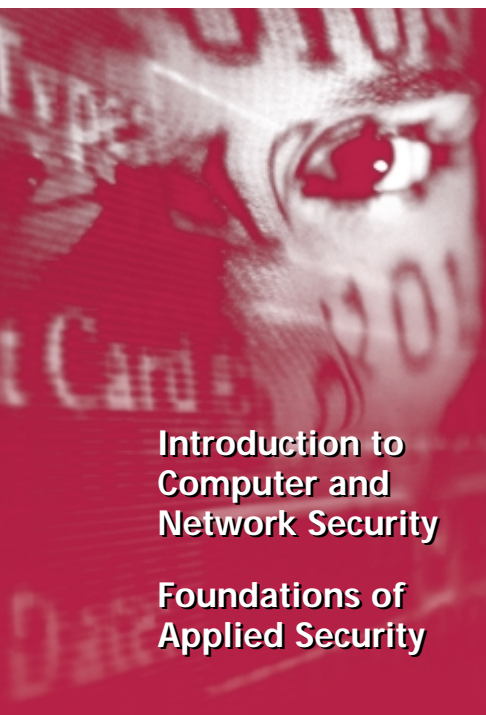
- Enclosed is check or money order for \$ _____ made payable to the University of Houston-Downtown.
- Please charge to my:
 Visa MasterCard American Express

CARD NO. _____ EXPIRATION DATE _____

NAME ON CARD _____ SIGNATURE _____

Refund Policy

All refunds must be made in writing. Individuals requesting refunds 48 hours prior to the start of a program will receive a full refund less \$25 handling fee. Within 48 hours prior to the start of a program, no refunds shall be granted. An individual may defer registration for one semester if the Applied Business & Technology Center is notified in writing at least 48 hours prior to the start of the program. The registration may be applied to any other Applied Business & Technology Center class offered. If the alternative course selected has a higher fee, the additional cost must be paid. ABTC reserves the right to postpone or cancel scheduled training courses.



Applied Business & Technology Center

University of Houston-Downtown
One Main Street
Houston, TX 77002

Call 713-221-8032 Today!

NONPROFIT ORG.
US POSTAGE
PAID
PERMIT NO. 9078
HOUSTON, TX

**Introduction to
Computer and
Network Security**

**Foundations of
Applied Security**