Report on Information Assurance Curriculum Development
June 1, 2002

Melissa Dark
CERIAS Purdue University
dark@cerias.purdue.edu

Jim Davis
Iowa State University
davis@iastate.edu

Abstract

This report details the participants, process, and output from two curriculum development workshops. The first was held in July 2001 (See Appendix A for a list of the participants) and the second was held in April 2002 (see Appendix B). The workshops were sponsored in part by the National Science Foundation Grant DUE # 0124409.

The objective for this project is to develop a curriculum framework for undergraduate and graduate programs in Information Assurance. The framework includes: identification of broad areas of knowledge considered important for practicing professionals in information assurance, identification of key learning objectives for each of these areas, identification of a body of core knowledge and skills that all programs should contain, and a model curriculum including scope and sequence. The framework's development is undertaken via workshops and working groups of leading information assurance educators leading to a draft document which will then be widely distributed for comment and dissemination.

The Task at Hand

Curriculum design and development means many things to many people. This is especially true in education where individuals have tacit understanding of curriculum design, development, and enactment. For the purpose of this workshop, we turned to the curriculum and instruction literature to establish a working definition that could serve as a guide for discussion. We used these working definitions to discuss and come to a common understanding of the task at hand and to guide our work. It should be noted that this work has really just begun. Therefore, the definitions provided below will continue to guide our work as we move forward.

Curriculum design is concerned with making decisions about the **scope, organization**, and **sequence** of the **content** at the macro level (Smith & Ragan, 1999). **Content** then can be considered as the topics to be taught (what should be taught?) **Scope** becomes a question of how much students should know (to what degree should students be taught this depends upon the degree of understanding/knowledge that you intend them to have upon completion). **Organization** becomes a question of how to sequence the topics (there are a variety of organization strategies: prior knowledge, job-function, super-ordinate concepts, etc). Finally, **sequence** is the suggested ordering of content based on answers to the three prior questions.

The output of curriculum design varies according to the uses of the curriculum design/development effort. The first goal of this project is to produce a document that defines the common body of knowledge in Information Assurance, i.e., what should be taught in Information Assurance program (content). A second goal of this project is to identify key learning outcomes for each of these areas, i.e., what students should know and be able to do (scope).

With regard to content, this group was seeking to define the core curriculum where core would be viewed as the intersection of various programs. We recognize that different programs will not only have different content, but even different emphases within the core. Furthermore, the group recognized that Information Assurance is multi-disciplinary in nature, including but not limited to disciplines such as psychology, sociology, political science, law, computer science, computer engineering, and management . The multi-disciplinary nature means that what students should know and be able to do will vary across disciplines and will require that we establish stronger involvement of experts from related disciplines not involved to date. The group also recognized that what students should know and be able to do will vary by the orientation of the specific program and the type(s) of career or advanced schooling being prepared for. Given that, the group felt that we could produce a working document that defined the content, i.e., the common body of knowledge across all disciplines and types of programs, but that meaningful definition of scope would need to be more detailed and granular according to program type.

We did not have time to adress depth of knowledge for different types. We think this is an important next step and should include a wider cross section of faculty from various programs. We recognize that when we define scope, an appropriate metric will be needed to indicate depth. Examples include: 1) number of hours of instruction devoted to a topic, 2) percentage of standard courses devoted to a topic, and/or 3) level of proficiency of student knowledge and skills.

The intent of this initiative is to provide a framework that serves multiple purposes including, but not limited to assisting:

- faculty and other stakeholders in identifying gaps in their existing programs,
- faculty and other stakeholders in developing new programs,
- faculty and other stakeholders in formulating articulation agreements,
- employers in assessing qualifications of graduates,
- students in understanding what is required of professionals in the field, and
- students and employees establish a common language for talking and working together on security projects, which are usually team efforts.

In terms of trying to conceptualize what a finished product might look like from this initiative, the group agreed that we were working toward a framework, but cautioned that we should not be constrained to a paper document. To provide a resource that serves the above uses requires representing a multi-dimensional manifold that includes 3 axes at a minimum; topics (content), audience, and depth (scope). It was noted that a database that allows us to extract and represent different views upon demand might be more versatile, informative, and useful.

The Process

The first goal of the April workshop was to identify the content of the common body of knowledge in IA undergraduate and graduate curriculum. The guiding question was "What topics should be included in every IA (undergraduate/graduate) program?" The second goal was to delimit the above by specifying scope. Questions to be considered at this step include: "Should the student have basic conceptual and factual understanding of the content? Should the student be able to apply the principles, procedures, processes, etc, in context? Should the student be able to synthesize principles, procedures, processes, etc., to form new ideas and solutions to ill-structured problems?"

Workshop participants split into two working groups focused either on undergraduate or graduate education, with the goal of defining the common body of knowledge for that type of program. The following day, presentations were made by each group to the entire group for discussion, review, and feedback. A current version of the working document from each group is provided later in this report. It should be noted that these documents are works in progress. The committee recognizes that they are by no means complete enough to serve their intended purposes. However, the group wants to circulate the documents throughout the development process to enable ongoing review and feedback, as well as to invite more IA educators and professionals to participate in the initiative.

The undergraduate document provides a list of main topics that should be covered in any undergraduate IA program. In an attempt to begin to establish cursory indicators of depth, three levels were assigned to each category. The levels are a derivative of the work of Robert Gagne and Benjamin Bloom in specifying types of knowledge in the cognitive domain (Gagne, 1979; Bloom, 1956). The three levels we used are: declarative, application, and synthesis. Declarative knowledge means that students should be expected to "*know that*" something is the case. Declarative knowledge includes knowing facts, concepts, principles, rules, algorithms, and so on. Application then is the ability to *use* learned material in new and concrete situations. Finally, synthesis refers to a level of understanding that is demonstrated by *creating new* (to the student) *solutions from existing knowledge*. The depth indicators on the working document represent a minimum level of understanding that all undergraduate IA students should have. We recognize that more work is needed to refine this and tailor it to different types of programs.

In the case of both the undergraduate and the graduate working documents, the group would like to note the following. The group is the most confident that the main groupings are accurate and sufficient (these are noted in bold). The group is also fairly comfortable with the second level under each of the main groupings. However, we would like to review this again ourselves and solicit the review and feedback of others not in the workshop group. The third level of topic (that which is indented the furthest) is not meant to be a comprehensive or exhaustive list of recommended topics, rather these are examples of subtopics that could be covered.

Throughout the process, we noted a number of meta-curricular issues that were documented as follows. Several terms have multiple meaning, e.g., threat, vulnerability, validation, verification, testing, secret key, certificate, one-way functions, social engineering, risk, security, proof, policy, security tools, undergraduate, graduate, curriculum (and more to come). Care should be taken to operationally define these terms so that others (including students) can better understand their multiple meanings in context. Throughout the undergraduate curriculum we should also discuss existing tools and resources such as BugTraq, and CERT Advisories, to name a few. Depending upon the students' interests, undergraduate programs might also want to discuss open research issues. Students should be required to write large programs, maintain programs overtime, and work in teams. Students are often not trained to be professional programmers working in teams on large codes. This is perceived as a source of many security problems. IA education encompasses the issues that arose from the military defense world and has grown to include e-commerce, e-government, e-learning (and others) and students need to understand this evolution and spectrum. Students need to understand the notion of "no such thing as absolutely secure".

There are also personal characteristics associated with being an IA professional that students should understand so they can self-assess whether or not they will be satisfied with a career in IA. Such characteristics include: detail-oriented, high level of self-discipline, voluntary "paranoia". To address how to integrate detail-orientation into the undergraduate curriculum, we can look at other disciplines where attention to detail is also paramount. Finally, at the undergraduate level, it was assumed that students graduating from programs that include these topics are expected to go into the following types of careers: Low Level IT Engineer, System Administrator with a Security Specialization, Programmer with a Security Specialization, Network Engineer with Security Specialization, or a Security Software Developer. It was also assumed that students would have taken more than one 4th generation language course so that students have the ability to program.

Before presenting the output of the workshop, we would like to share action items from the workshop. The current list of topics under consideration for an undergraduate curriculum is given in Appendix C; the graduate topics are provided in Appendix D.

Action Items

1. Complete this phase of the work. This includes:
    a. preparing a report for the group to review and edit,
    b. planning a follow up informal session for those who will be attending NCISSE,
    c. identify opportunities to invite review and feedback by others,
        i. NCISSE
        ii. Discussion forums, such as Fred Cohen's SECEDU Discussion forum
    d. looking for add-on funding to sponsor another workshop targeted for late summer or early fall 2002. Further work will be focused on identification of scope, i.e., what student should know and be able to do in different types of programs.
2. Form an advisory group to inform how to interleave this initiative with related existing curriculum efforts and other stakeholders
    a. Related existing curriculum efforts
        i. CNSS
        ii. NSTISSC
        iii. ISC^2
        iv. SANS
        v. Other
    b. Other stakeholders
        i. Accounting firms
        ii. ACM
        iii. American Society for Industrial Security
        iv. Association of Certified Fraud Examiners
        v. Banking industry
        vi. All 36 Centers of Academic Excellence in Information Assurance Education
        vii. CERT/CC
        viii. Cisco
        ix. Commercial IA/Network Security/Penetration training firms
        x. Disaster Recovery Institute international
        xi. DoD
        xii. FBI

xiii. FISSEA
xiv. HTCIA
xv. IEEE
xvi. ISACA
xvii. ICCP
xviii. IIA
xix. NIST
xx. NSF
xxi. Secret Service

c. Form a communications group that provides outreach on this initiative
d. Consider a related initiative to establish a repository of curriculum resources, documents, and links. The goal here would be to create an exchange of teaching materials of these topics specifically as it relates to the curriculum framework being developed.

References

Bloom, B.S. (Ed.), Englehart, M.D., Furst, E.J., Hill, W.H., & Krathwohl, D.R. (1956). *Taxonomy of Educational Objectives: Handbook I, Cognitive Domain.* New York: David McKay.

Gagne, R.M., & Briggs, L.J. (1979). *Principles of Instructional Design.* New York: Holt, Rinehart, & Winston.

Smith, P., & Ragan, T. (1999). *Instructional Design.* Upper Saddle River, NJ: Prentice-Hall.

Appendix A
July 2001 Curriculum Development Workshop Participants

Andy Bernat
National Science Foundation
4201 Wilson Boulevard
Arlington, VA 22230
EMAIL: abernat@nsf.gov
Phone: (703) 292-4647

Matt Bishop
Dept of Computer Science
University of California
Davis, CA 95616-8562
EMAIL: bishop@cs.ucdavis.edu
Phone: (530) 752-8060

Melissa Dark
CERIAS
1315 Recitation Building
Purdue University
West Lafayette, IN 47907-1315
Email: dark@purdue.edu
Phone: 765-496-6761

Jim Davis
Department of E CPE
Iowa State University
2413 Coover Hall
Iowa State University
Ames, Iowa 50011
Email: davis@iastate.edu
Phone: 515-294-0659

Lance Hoffman
Department of Computer Science
The George Washington University
801 22nd St. NW, Suite 704
Washington DC 20052
EMAIL: hoffman@seas.gwu.edu
Phone: (202) 994-4955

Cynthia Irvine
Code CSIc, Computer Science Department
Naval Postgraduate School
833 Dyer Road
Monterey, CA 93943-5118
Email: irvine@cs.nps.navy.mil
Phone: 831-656-2461

Barb Laswell
Technical Manager
Practices, Development and Training
Networked Systems Survivability Program
Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
Email: blaswell@cert.org
Phone: 412-268-7569

Barb Licklider
Educational Leadership and Policy Studies
N221A Lagomarcino Hall
Iowa State University
Ames, Iowa 50011
Email: blicklid@iastate.edu
Phone: 515-294-1276
www.educ2.iastate.edu/database/bios/113.html

Vic Maconachy
National Security Agency
9800 Savage Road
Fort George G. Meade
Maryland 20755-6752
EMAIL: wmaconac@radium.ncsc.mil
Phone: (410) 854-6206

Jack Marin
Senior Systems Engineer
Information Security Department
BBN Technologies
9861 Broken Land Parkway, Suite 156
Columbia, MD 21046
Email: jamarin@bbn.com
Phone: 410-312-6939

Daniel Ragsdale
The United States Military Academy
Electrical Engineering and Computer Science
Building 601, Room 113
West Point, NY 10996
Email: Daniel-Ragsdale@usma.edu
Phone: 845-938-2056

Charles Reynolds
281 East Grattan Street
Harrisonburg, Virginia 22801
Email: reynolds@cs.jmu.edu

Sujeet Shenoi
Computer Science Department
University of Tulsa
600 S. College Avenue
Tulsa, OK 74104
EMAIL: sujeet@euler.mcs.utulsa.edu
Phone: (918) 631-3269

Gene Spafford
CERIAS
1315 Recitation Building
Purdue University
West Lafayette, IN 47907-1315
Email: spaf@cerias.purdue.edu
Phone: 765-494-7841

Dan Ryan
380 Forelands Road
Annapolis, Maryland 21401
Email: danryan@danjryan.com
Phone: 443-994-3612

Ed Schneider
IDA/CSED
1801 N. Beauregard St.
Alexandria, VA 22311-1772
EMAIL: eschneider@ida.org
Phone: (703) 845-6626

Corey Schou
College of Business, Room 509
Idaho State University
Pocatello, Idaho 83209-8059
Email: Schou@Mentor.Net
Phone 208 282 3194

Michael S. Stohl
Political Science Department
Purdue University
1363 Liberal Arts and Education Bldg
West Lafayette, IN 47907-1363
Email: mstohl@purdue.edu
Phone: 765-494-9399

Appendix B.
April 2002 Curriculum Development Workshop Participants

Mustaque Ahamad
Professor
College of Computing
Georgia Institute of Technology
Atlanta, GA 30332
mustaq@cc.gatech.edu

Peter Bloniarz
College of Public Affairs and Policy
Suny at Albany
Draper 118
135 Western Avenue
Albany, NTY 12222
Phone 518-442-3306
p.bloniarz@albany.edu
www.albany.edu/rcinf

Curt Carver
Program Director,
Information Systems Engineering
Department of Electrical Engineering
and Computer Science
United States Military Academy
West Point, NY 10996
(845) 938-3933
dc8177@exmail.usma.army.mil

Bojan Cukic
Computer Science and Electrical Engineering
West Virginia University
PO Box 6109
Morgantown, WV 26506-6109
Phone 304-293-0405 ext. 2526
cukic@csee.wvu.edu
www.csee.wvu.edu/faculty/bcukic.htm

Tom Daniels
CERIAS
Purdue University
1315 Recitation Building
West Lafayette, IN 47907
Phone 765-496-6768
daniels@cerias.purdue.edu
www.cerias.purdue.edu

Melissa Dark
CERIAS
Purdue University
1315 Recitation Hall
West Lafayette, IN 47907
Phone 765-496-6761
dark@cerias.purdue.edu
www.cerias.purdue.edu

Jim Davis
Electrical and Computer Engineering
Iowa State University
2413 Coover Hall
Ames, Iowa
Phone 515-294-0659
davis@iastate.edu
vulcan.ee.iastate.edu/~davis

Mich Kabay
Computer Information Systems
Norwich University
158 Harmon Drive
Northfield, VT 05663-1035
Phone 802-479-7937
mkabay@compuserve.com
www2.norwich.edu/mkabay/ondex.htm

Peng Ning
Department of Computer Science
NC State University
105 Venture 1
Centennial Campus
Raleigh, ND 27695-7534
Phone 919-515-7925
ning@csc.ncsu.edu
www.csc.ncsu.edu/faculty/ning

Rene Peralta
Research Scientist
Yale University
New Haven, CT 06520-8285
Phone 203-432-1245
peralta-rene@cs.yale.edu

John Pinkston
University of Maryland, Baltimore County
Department of Computer Science & Electrical Engineering
1000 Hilltop Circle
Baltimore, MD 21250
Phone 410-455-1338
pinkston@umbc.edu

Charles W. Reynolds, Ph.D.
Professor of Computer Science
Department of Electrical Engineering and Computer Science
United States Military Academy
West Point, New York 10996
(845)938-5577
charles.reynolds@usma.edu

John Saunders
National Defense University
198 Marshall Hall
Ft. McNair
Washington DC 20319
Phone 202-685-2078
saunders@ndu.edu

Sean Smith
Dartmouth College
6211 Sudikoff Laboratory
Hanover, NH 03755-3510
Phone 603-646-1618
sws@dartmouth.edu
www.cs.dartmouth.edu/~sws?

Eugene Spafford
CERIAS
Purdue University
1315 Recitation Hall
West Lafayette, IN 47907
Phone 765-494-7825
spaf@cerias.purdue.edu
www.cerias.purdue.edu

Jessica Watts
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Phone 561-357-8305
jewatts@cisco.com
www.cisco.com

Mike Wenstrom
Cisco Systems, Inc.

Appendix C
Undergraduate Knowledge and Skills

General Information Assurance Knowledge and Skills Basic IT and traditional definitions of INFOSEC ○ History and concepts ○ IA Mindset ○ Survey/overview of the field ○ Survey/overview of the context/environment ○ Crimes and laws ○ Business ○ Fundamentals of authentication and authorization ○ Awareness of INFOSEC hardware products ○ E-Commerce	**Declarative**
Risk Assessment Identifying threats and vulnerabilities ○ Classes of attacks ○ Classes of attackers ○ Methods and models for testing systems ○ Assessing risk ▪ Methods, models, and theories and how these interleave into IA *(this is a gap we need to address with risk assessment specialists)* ○ Asset classification ○ Cost benefit analysis *(this is a gap we need to address with cost benefit specialists)* ○ ROI of INFOSEC investments ○ Security posture assessment ○ Testing, validation, and verification	**Application**

Information Security Management Security policy o Policy development process o Classifications of policies o Policy implementation and management Organizational behavior, cultural, societal, and ethical implications o How do humans make trust judgments?	**Application**
Networking Fundamentals o TCP/IP o http and other protocols o lan technology o wireless networking technology o OSI (open systems infrastructure – model for teaching networks) o Ports o Pipes o Network components, including bridges, routers, switches o Network topologies o Issues that arise in very large scale systems	**Application**

Cryptography Fundamentals (f) and usage (u) o F - Symmetric/asymmetric, one-way functions, digital signatures, secure hash, digital authentication (declarative knowledge) o U - Code digital signatures, how PGP actually works (by taking it apart and explaining how it works), representative cryptographic protocol (e.g., blind signatures)(applicative knowledge) o Subverting cryptography (minimally declarative • Social engineering (the three Bs, bribery, burglary, blackmail…..) • Bad randomness • Algorithm weaknesses (including poor/insufficient implementation of) • Side channel analysis • Long-term implications of insufficiency of present algorithms, e.g., quantum computing • How do we build our systems so that we may implement the necessary technology changes without massive cost and disruption (if we assume failure and also assume that we will see it coming)	**Declarative** **Application** **Declarative**
PKI Fundamentals (cryptography PLUS implementation/usage issues) o Protocols o Infrastructure o Certificates o Standards o Interoperability o Scalability o Name spaces o CA topologies Examples of tools dealt with daily that have security issues	**Declarative**

Operating Systems o Functions of an OS • Process management • Memory management • Auditing • File management • Interface management o "Brands" of OSs (compare and contrast is the intent) o Characteristics of a good OS o Installing services, applications, servers	**Application**
Software Engineering Practices o Security of large software systems o Programming language issues o Awareness of the field of software engineering, techniques used, software security issues o What can we do in the software process to build quality into that process?	**Declarative**
Legal, Ethical INFOSEC (have to be preparing students to FUNCTION in the current environment. This means that they have to understand what they can and cannot do.) o Privacy o Intellectual Property o Investigation o Digital evidence • Legal aspects of computing practices o Forensic examination and associated tools o Seizure concepts o Legal principles of computer related investigations o Presenting evidence in court o Ethics • Prepared to engage in discussion on ethical issues that remain open/not yet resolved	**Declarative**

<table>
<tr><td>Intrusion Defense and Response

IDS

Functions of IDS
Types of IDS
Anomaly
Misuse
Advantages and drawbacks of different IDS

Vulnerability scanners
Firewalls

Proxy
Filtering

Application
Incident response

Notification
Manual response
Automated response

Disaster recovery

Back up
Redundancy
Replicated sites

Post attack network analysis and computer forensics
</td><td>Declarative</td></tr>
<tr><td>Emerging Technologies (what they are, what are the issues, how to evaluate and use these in a security system)

INFOSEC hardware
Biometrics
Digital cash
Wearable computing, etc…
</td><td>Declarative</td></tr>
<tr><td>E-commerce related issues (this is a gap where we need to get input from e-commerce specialists)</td><td>Declarative</td></tr>
<tr><td>Develop secure network applications, server, and distributed applications.</td><td>Application</td></tr>
<tr><td>IT System and Network Security Design

Discuss definitions for “secure” operating system, “secure” server
Secure an operating system (minimally students should experience the process of securing some mainstream operating system and ideally have experience in multiple mainstream operating systems)
Configure and manage security tools (minimally be able to install and configure one, ideally more than one)
e.g., Tripwire, TCP wrapper, etc.
Configure and secure web browsers and web servers.

Develop secure web applications.</td><td>Application</td></tr>
</table>

Integrative experience to address an ill-defined problem with no single correct answer. The problem has social, economical, ethical, and political constraints. Involves the consideration of more than one design alternative and requires students to work in a team environment. The end result of this integrative experience is a real product (an implementation of a server, service, etc.). Students also produce a written and oral report. There is a requirement for self-assessment. (This can be done with a real customer. This usually requires additional time. If this approach is desired, it is suggested that this be a two semester experience). E.g.: o Configure and manage routers o Configure and manage Ethernet switches to include content-aware/Layer 1-3 and 4-7 o Configure and manage firewall systems ▪ Software and appliance-based o Configure and manage VPN networks o Design and secure wireless and voice over IP applications	**Synthesis**

Appendix D
Graduate Knowledge and Skills

Cryptography

- The development of cryptography
  - First principles
    - Protecting confidentiality
    - Ensuring integrity
    - Guaranteeing authenticity
    - Classical cryptosystems
  - Historical cryptography
    - Substitution ciphers
    - Transposition
    - Frequency-based cryptanalysis
    - Codes
    - Code machines
    - One-way hash functions
- Fundamentals
  - Block vs stream ciphers
  - Chaining
  - Threshold cryptography
  - Zero-knowledge proofs
  - Oblivious transfer
  - Pseudo-random number generators
  - Secret sharing
  - Key management and key distribution
  - Keyspace
- Important symmetric algorithms
  - DES
  - AES
  - Clipper / Skipjack
  - RCn
- Asymmetric algorithms
  - Public key cryptography
  - RSA
  - Elliptic curve cryptosystem
  - Digital Signature Algorithm
- Cryptographic protocols
  - Identification, authentication and authorization
  - Role of encryption
  - Frameworks for secure e-commerce
  - Third-party certification authorities
  - Single sign-on
  - Interoperability
  - Products
  - Web sites
  - Overview of network applications of crypto
  - Electronic voting
  - E-commerce
  - Electronic contracts & non-repudiation
- Hardware implementations
  - Cost/benefit analysis
  - Network Topology
  - Enforcement
  - Digital rights
  - Vulnerabilities
  - Crypto processors
- Digital signatures
  - Definitions
  - Benefits
  - Mechanisms
  - Certificates
- Public key infrastructure and certificate authorities
  - Need for public key cryptosystem
  - Need for public key infrastructure
  - Public key certificate
  - Enterprise public key infrastructure
  - Certificate policy
  - Global public key infrastructure
    - Trusted paths
    - Trust models
    - Choosing a public key infrastructure architecture
    - Public key infrastructure interoperability
  - Forms of revocation
    - Types of revocation-notification mechanisms
    - Certificate revocation lists and their variants
    - Server-based revocation protocols
  - Rekey
  - Key recovery
  - Privilege management
  - Trusted archival services and trusted time stamps
- Implementation issues
  - Algorithmic weakness vs implementation weakness
  - Secrecy of the algorithm is not a defense
  - Types of attacks
  - Overview of non-brute-force attacks
  - Product certifications
    - Common Criteria
    - Commercial standards
  - Key escrow
- Applications of cryptography
  - Cryptography in the OSI model
    - TCP/IP
    - IPv4
    - IPv6
  - IPSec
  - Smartcards
  - Biometrics

- Cryptanalysis
  - Strategies
    - Brute-force
    - Linear and differential cryptanalysis
    - Meet-in-the-middle/birthday attack
    - Timing analysis
    - Side-channel analysis
  - Analysis of randomness
  - Interception techniques
  - Reverse engineering
  - Hardware failures
- Steganography
  - Definitions
  - Examples
  - Analysis
  - Defenses
- Latest developments
  - Chaffing and winnowing
  - Recent algorithms
  - New products
  - Quantum computing effects on cryptanalysis
  - Quantum cryptography

Secure Computing Systems

Access control
- ACLs
- capabilities
- Data- and user-oriented access control
- multi-level security
- Simultaneous access

Identification, authentication and authorization
- accounting
- authentication
- authorization
- biometrics
- identification
- passwords
- tokens

Design of secure systems
- architectural implications of OS for security
- design principles
- hardening OSs
- high-availability / sustainability
- inference control
- Protection based on an operating system mode
- Protection of memory
- reference monitor
- security kernels
- survival
- system design principles
- trusted operating systems; e.g., trusted LINUX
- malicious software: analysis, prevention

Evaluation
- Common Criteria
- covert channels
- evaluation of secure systems
- penetration testing
- virus prevention

Databases and applications
- application security -- Web servers
- database security
- developing secure distributed applications (JAVA etc.)
- secure file systems
- security databases (active directory, RADIUS, token servers, Kerberos…)

Software development
- authenticating libraries, DLL, run-time
- buffer overflows
- develop security tools (e.g., IDS, sniffer, integrity check)
- how to write secure software
- open-source vs proprietary software and security
- quality assurance and security
- software security
- writing code
- writing patches

Auditing
- application logging
- computer forensics/auditing and system logs, utilities, data
- known vulnerabilities
- logging
- intrusion detection

Operations management
- patching systems
- physical security
- version control

Network Security

Protocols
- IPSec
- IPv6
- key management protocols
- multicast security
- raw sockets
- routing authentication
- routing protocols
- SSH
- TCP / UDP
- TCP state analysis
- tunneling
- VPN

Network basics
- ISO/OSI model
- Network design
- topology
- transport-level security

Vulnerabilities
- NOS weaknesses
- protocol vulnerabilities
- sequence-number prediction
- vulnerabilities at the different layers of the OSI

Attacks
- DoS
- eavesdropping
- man-in-the-middle attacks
- sniffing
- spoofing
- steganography
- types of attacks (exploitation of protocol weaknesses)

Application-layer services
- DNS Domain Name System
- E-commerce payment systems
- e-mail
- NAT
- SMTP
- Web

Management, monitoring, auditing & forensics
- management
- SNMP
- honeypots
- intrusion detection
- monitoring
- network forensics
- traceback

Infrastructure
- dialup security
- Ethernet switching (VLANs, . . .)
- grid security
- media
- middleware
- PKI
- protection of network infrastructure (e.g., secure routing protocols)
- RFI radio frequency interference
- TEMPEST / emanations control
- WANs

Wireless & broadband
- Bluetooth
- broadband
- DSL
- satellite
- Cable
- GB Ethernet security
- WEP

Filtering
- filtering mechanisms: static, stateful, proxy, . . .
- firewalls

Management, Policy and Response

- Security policy guidelines
  - Terminology
  - Resources for policy writers
  - Writing the policies
  - Organizing the policies
  - Presenting the policies
  - Maintaining policies
- Security awareness
- Ethical decision-making and high technology
- Employment practices and policies
  - Hiring
  - Management
  - Termination of employment
- Operations security and production controls
  - Basic concepts
  - Operations management
  - Providing a trusted operating system
  - Protection of data
  - Data validation
- E-mail and Internet use policies
- Using social psychology to implement security policies

- Auditing and assessing computer systems
- Cyberspace law and computer forensics
  - Contracts
  - Defamation
  - Due diligence and private liability
  - Indecency and obscenity
  - Litigation
  - Criminal acts
  - Investigation
- Privacy in cyberspace
  - Worldwide trends
  - European approaches to privacy
  - United states
  - Compliance models
- Protecting intellectual property
- Security standards for products
  - Security assessment standards associated with security implementations
  - Establishing trust in products and systems and managing risks
  - Common criteria paradigm
- Management responsibilities and liabilities
  - Responsibilities
  - Liabilities
  - Computer management functions
  - Security administration
- Developing security policies
- Risk assessment and risk management
- Incident Response and Recovery
  - Computer emergency quick-response teams
  - Data backup and recovery
  - Business continuity planning
  - Disaster recovery
  - Insurance relief
  - Working with law enforcement
    - Goals of law enforcement
    - History of law enforcement and computer crime
    - Anatomy of a criminal investigation
    - Establishing relationships with law enforcement
  - Northwest computer technology and crime analysis seminar
    - Organizational policy
    - Developing internal investigative capabilities
    - Internal investigations
    - International investigations
    - Computer evidence
    - Decision to report computer crime