



Information Assurance & Security Program

Table of Contents

	Page
1. Mission	3
2. Motivation	3
3. Program Goals	3
4. Course Dependency Chart	4
5. Mapping of CNSS 4011 to IAS Courses	5
6. Mapping of CISSP Standard to IAS Courses	7
7. Information Assurance and Security Program Mapped to CIS Curriculum	16
8. IAS Required Courses	
• CIS 100 – Information Technology and Computer Applications	17
• CIS 105 – Structured Programming	19
• CIS 121 – Introduction to Computer Systems	22
• CIS 123 – Data Structures	26
• CIS 321 – Introduction to Software Engineering	29
• CIS 471 – Introduction to Algorithms	31
• CIS 472 – Computer Architecture	34
• CIS 473 – Introduction to Operating Systems	38
• CIS 474 – Introduction to Database Systems	41
• CIS 476 – Programming Languages and Compilers	45
9. CIS / IAS Courses	
• CIS 519 – Information Assurance Tools & DB Administration	39
• CIS 521 – Introduction to Information Security	43
• CIS 529 – Web Design and Development	47
• CIS 575 – Wireless Communications	50

Mission Statement

In line with the Department's mission of preparing undergraduate and graduate students for the industry, government and academia, the Information Assurance and Security Program is designed to meet the current industry, government and undergraduate studies requirements.

Motivation

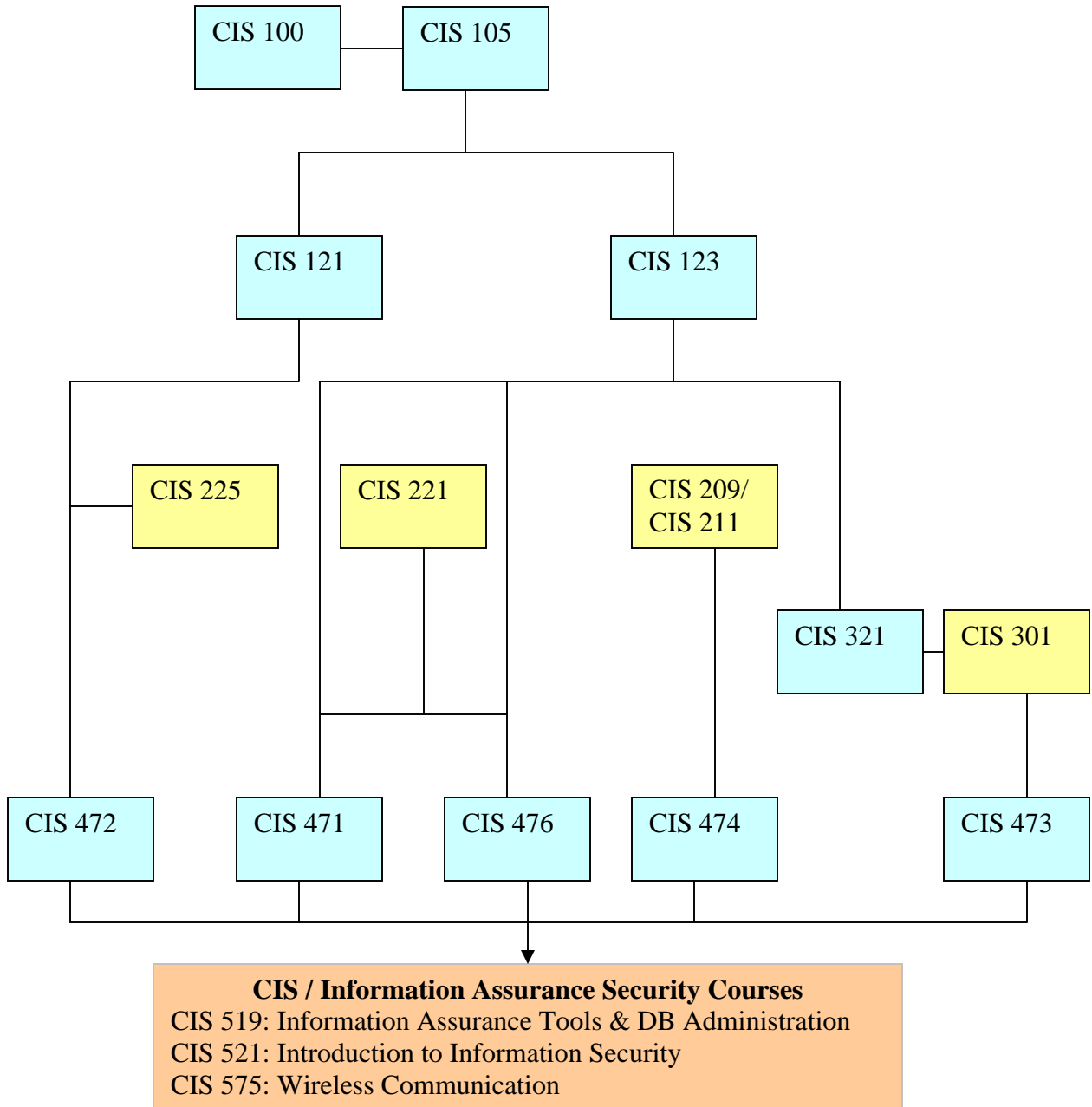
Due to increasing sophistication of online attacks on IT infrastructures, initiated both internal and external to organizations, it is now necessary to educate a large number of students in the field of IAS, so that the security of IT infrastructures can be improved at the design, implementation and operational levels.

Program Goals

To impart a thorough understanding of the field of IAS, so that students:

- Demonstrate an advanced level of knowledge in the field of IAS that is a superset of the knowledge requirements of CNSS 4011 and CISSP standard.
- Comprehend the security goals of confidentiality, integrity and availability.
- Apply their knowledge to real life situations.
- Can analyze the security requirements of an organization.
- Can synthesize security systems commensurate with security requirements.
- Can evaluate security systems against organizational and national security standards.

Course Dependency Chart



- CIS / IAS Courses
- IAS required Courses
- CS Curriculum Courses

Mapping of CNSS 4011 to IAS Courses

CIS 100 CIS 105 CIS 121 CIS 123 CIS 321 CIS 471 CIS 472 CIS 473 CIS 474 CIS 476 CIS 519 CIS 521 CIS 529 CIS 575

(A) Communications basics (Awareness)

- | | | | | | | | | | | | | | | |
|--|---|--|--|--|--|--|--|--|--|--|--|--|--|--|
| (a) Historical vs. Current Methodology | x | | | | | | | | | | | | | |
| (b) Capabilities and limitations | x | | | | | | | | | | | | | |

(B) AIS Basics (Awareness)

- | | | | | | | | | | | | | | | |
|---------------------------------------|---|--|---|--|--|---|---|--|--|--|--|--|---|--|
| (a) Historical vs. Current Technology | x | | x | | | | | | | | | | | |
| (b) Hardware | x | | | | | x | | | | | | | | |
| (c) Software | x | | | | | | x | | | | | | | |
| (d) Memory | x | | | | | | x | | | | | | | |
| (e) Media | x | | | | | | x | | | | | | | |
| (f) Networks | x | | | | | | x | | | | | | x | |

(C) Security Basics (Awareness)

- | | | | | | | | | | | | | | | |
|---------------------------------|--|--|--|--|--|--|--|--|--|--|---|---|---|---|
| (a) INFOSEC Overview | | | | | | | | | | | | x | | x |
| (b) Operations Security (OPSEC) | | | | | | | | | | | x | | x | |
| (c) Information Security | | | | | | | | | | | | | x | |
| (d) INFOSEC | | | | | | | | | | | | | x | |

(D) NSTISS Basics (Awareness)

- | | | | | | | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|--|--|---|---|---|
| (a) National Policy and Guidance | | | | | | | | | | | | x | | |
| (b) Threats to and Vulnerabilities of Systems | | | | | | | | | | | | x | x | |
| (c) Legal Elements | | | | | | | | | | | | x | | |
| (d) Countermeasures | | | | | | | | | | | | x | x | |
| (e) Concepts of Risk Management | | | | | | | | | | | | | x | |
| (f) Concepts of System Life Cycle Management | | | | | | | | | | | | x | | |
| (g) Concepts of Trust | | | | | | | | | | | | | x | |
| (h) Modes of Operation | | | | | | | | | | | | x | x | |
| (i) Roles of Various Organizational Personnel | | | | | | | | | | | | | x | |
| (j) Facets of NSTISS | | | | | | | | | | | | x | x | x |

(E) System Operating Environment (Awareness)

- | | | | | | | | | | | | | | | |
|---------|--|--|---|--|--|--|--|---|--|--|--|--|--|---|
| (a) AIS | | | x | | | | | x | | | | | | x |
|---------|--|--|---|--|--|--|--|---|--|--|--|--|--|---|

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
--	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

(b) Telecommunications Systems															X
(c) Agency Specific Security Policies															X
(d) Agency Specific AIS and Telecommunications Policies															X

(F) NSTISS Planning and Mgmt (Performance)

(a) Security Planning															
(b) Risk Management												X			
(c) Systems Life Cycle Management							x					X			
(d) Contingency Planning/Disaster Recovery												X			

(G) NSTISS Policies and Procedures (Performance)

(a) Physical Security Measures							x								X
(b) Personnel Security Procedures							x	x							
(c) Software Security	x		x	x	x	x	x		x			X			
(d) Network Security											X				X
(e) Administrative Security Procedural Controls							x					X	X		
(f) Auditing and Monitoring							x				x	X			
(g) Cryptosecurity					x			x	x			X			
(h) Key Management									x			x			
(i) Transmission Security															X
(j) TEMPEST Security															X

Mapping of CNSS 4014 to IAS Courses

CIS 100 CIS 105 CIS 121 CIS 123 CIS 321 CIS 471 CIS 472 CIS 473 CIS 474 CIS 476 CIS 519 CIS 521 CIS 529 CIS 575

(A) Access Control Systems and Methodology

Access Control										X	X		
Security Principles										X	X		
• Availability	X			X						X	X		
• Integrity	X			X						X	X		
• Confidentiality	X			X						X	X		
Identification, Authentication, Accountability, Authorization										X	X		
Access Control Models													
• Discretionary													
• Mandatory													
• Role Based													
Access Control Techniques and Technologies													
• Rule-Based Access Control													
• Constrained User Interfaces													
• Access Control Matrix													
• Capability Tables													
• Access Control Lists													
• Content Dependant Access Control													
Access Control Administration											X		
• Centralized													
• Decentralized													
• Hybrid													
Access Control Methods										X	X		
• Access Control Layers										X	X		
• Administrative Controls										X	X		
• Physical Controls										X	X		
• Technical Controls										X	X		
Access Control Types													
Access Control Practices													
Access Control Monitoring													
• Intrusion Detection				X						X			
Threats To Access Control													
• Dictionary Attack													
• Brute Force Attack													
• Spoofing At Logon													

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
--	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

(B) Applications and System Development

Software Importance					X						X			
Device Versus Software Security														
Different Environments Demand Different Security														
• Ecommerce														
• Client/ Server Model														
Environment Versus Application Control														
Complexity of Functionality														
Data Types, Format and Length														
Implementation and Default Issues														
Failure States														
Database Management											X			
• Database management software									X					
• Database Models									X					
• Database Interface Languages														
• Relational Database Components														
• Data Dictionary														
• Integrity									X					
• Database security issues									X		X			
• Data Warehousing and Mining									X					
System Development											X			
• Management of Development														
• Life Cycle Phases											X	X		
• Software Development Methods					X									
• Change Control														
• Capability Maturity Model														
Application Development Methodology														
• Object-Oriented Concepts				X	X					X				
• Data Modeling														
• Software Architecture				X	X									
• Data Structures				X	X									
• ORBS and CORBAs														
• Computer-Aided Software Engineering														
• Prototyping														
• COM, DCOM														
• Open Database Connectivity														
• Object Linking, Embedding					X									
• Dynamic Data Exchange														
• Distributed Computing Environment														
• Enterprise Java Bean														
• Expert Systems and Knowledge Based Systems														

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
--	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

- Artificial Neural Networks
- Java
- Attacks
- Malicious Software
- ActiveX

		X												
--	--	---	--	--	--	--	--	--	--	--	--	--	--	--

	X													
--	---	--	--	--	--	--	--	--	--	--	--	--	--	--

	X													
--	---	--	--	--	--	--	--	--	--	--	--	--	--	--

										X				
--	--	--	--	--	--	--	--	--	--	---	--	--	--	--

(C) Business Continuity Planning

Business Continuity and Disaster Recovery

Business Impact Analysis

Business Continuity Planning Requirements

- Developing Goals for Plans
- Developing the Team
- Enterprise-Wide
- Plan Development
- Identifying Business Critical Functions
- Identifying the Resources and Systems that support Critical Functions
- Estimating Potential Disasters
- Selecting Planning Strategies
- Implementing Strategies
- Testing and Revising Plan

End-User Environment

Backup Alternatives

- Hardware Backup
- Software Backup

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

Recovery and Restoration

Testing and Drills

- Checklist Test
- Structure Walk-Through Test
- Simulation Test
- Parallel Test
- Full-Interruption Test

(D) Cryptography

Cryptography

						X								
--	--	--	--	--	--	---	--	--	--	--	--	--	--	--

							X							
--	--	--	--	--	--	--	---	--	--	--	--	--	--	--

								X						
--	--	--	--	--	--	--	--	---	--	--	--	--	--	--

History of cryptography

Strength of the Cryptosystem

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

Goals of the Cryptosystems

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

Types of Ciphers

- Substitution Cipher
- Transposition Cipher
- Running and Concealment Ciphers

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

					X									
--	--	--	--	--	---	--	--	--	--	--	--	--	--	--

Steganography

Methods of Encryption

										X				
--	--	--	--	--	--	--	--	--	--	---	--	--	--	--

											X			
--	--	--	--	--	--	--	--	--	--	--	---	--	--	--

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
• Symmetric versus Asymmetric Algorithms						X								X
• Stream and Block Ciphers														X
• Types of Symmetric Systems														X
• Asymmetric Encryption Algorithms						X					X			X
• Hybrid Encryption Methods														
Public Key Infrastructure														
• Certificate Authorities						X								
• Registration Authority						X								
• PKI Steps						X								
Message Integrity														
• One-Way Hash														
• Digital Signatures														
• Various Hashing Algorithms						X								
• Attacks Against One-Way Hash Functions														
• One-Time Pad														
Key Management Principles														
Link Versus End-To-End Encryption														
Email Standards														
• MIME														
• Privacy Enhanced Mail														
• Message Security Protocol														
• Pretty Good Privacy (PGP)														
Internet Security														
Attacks														
• Cipher Only Attacks						X								
• Known Plain Text Attack														
• Chosen Plain Text Attack														
• Chosen Ciphertext Attack														
• Man in the middle Attack														
• Replay Attack														
• Side-Channel Attack														
(E) Law, Investigation and Ethics														
Many Facets of Cyberlaw	X			X						X			X	
Ethics													X	
• Computer Ethics Institute														
• Internet Architecture Board														
• Generally Accepted System Security Principles				X										
• Motive, Opportunity and Means				X										
Operations Security											X		X	
Identification, Protection and Prosecution				X							X			

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
--	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

Liability and Ramifications

- Personal Information
- Hacker Intrusion

Intellectual Property Laws

Discarding Equipment and Software Issues

Computer Crime Investigations

- Incident Handling
- Admissible in Court?
- Surveillance, Search and Seizure
- Interviewing and Interrogating

Import – Export Laws, transborder information flow

Privacy X

X

Laws, Directives and Regulations

- HIPAA Act
- Gramm Leach Bliley Act of 1999
- Computer Fraud and Abuse Act
- Federal Privacy Act of 1974
- European Union Principles of Privacy
- Computer Security Act of 1987
- Security and Freedom through Encryption Act

(F) Operations Security

Operational Security

- Administrative Management X
- Accountability X
- Security Operations and Product Evaluation X
- Input and Output Controls X

Electronic Mail Security

- Facsimile Security X
- Hack and Attack Methods

(G) Physical Security

Physical Security

X X

Planning Process

Facilities Management

- Physical Attributes of Facility
- Construction
- Facility Components
- Computer and Equipment Rooms

Physical Security Risks

X

Physical Security Component Selection Process

CIS 100 CIS 105 CIS 121 CIS 123 CIS 321 CIS 471 CIS 472 CIS 473 CIS 474 CIS 476 CIS 519 CIS 521 CIS 529 CIS 575

- Security Musts
- Security Should
- Backups

Environmental Issues

- Ventilation, Fire Prevention, Detection, Suppression

Administrative Controls

- Emergency Response and Reactions

Perimeter Security

- Facility Access Control
- Personnel Access Control
- External Boundary Protection Mechanisms
- Intrusion Detection Systems

(H) Security, Architecture and Models

Computer Architecture

- CPU
- Memory
- CPU Modes and Protection Rings
- Process Activity
- Input/Output Device Management

System Architecture

- Defined Subset of Subjects and Objects
- Trusted Computing Base
- Security Perimeter
- Reference Monitor and Security Kernel
- Domains
- Resource Isolation
- Least Privilege
- Layering, Data Hiding and Abstraction

Security Models

- State Machine Models
- Bell-LaPadula Model
- Biba Model
- Clark Wilson Model
- Information Flow Model
- Noninterference Model
- Brewer and Nash Model

Security Modes Of Operation

- Dedicated Security Mode
- System-High Security Mode
- Compartmented Security Mode

CIS 100 CIS 105 CIS 121 CIS 123 CIS 321 CIS 471 CIS 472 CIS 473 CIS 474 CIS 476 CIS 519 CIS 521 CIS 529 CIS 575

- Multilevel Security Mode
- Trust and Assurance

Orange Book and rainbow series

Information Technology Security Evaluation
Criteria

Open versus Closes Systems

Threats to Security Models and Architectures

- Covert Channels
- Backdoors
- Asynchronous Attacks
- Buffer Overflows

X

(I) Security Management Practices

Security Management

X

Security Management Responsibilities

X

Security Administration and Supporting
Controls

X

X

Fundamental Principles of Security

X

X

- Availability

X

X

X

- Confidentiality

X

X

X

- Integrity

x

X

X

The Top-Down Approach

Organizational Security Model

Risk Management

X

Risk Analysis

X

X

- Value of Information and Assets

X

- Costs that make up the value

X

- Identifying Threats

X

- Quantitative Approach

X

- Analysis Inputs and Data gathering

X

- Automated Risk Analysis Methods

X

- Steps of a Risk Analysis

X

- Results of a Risk Analysis

X

- Qualitative Risk Analysis

X

- Qualitative versus Quantitative Risk
Analysis

X

- Protection Mechanisms

X

- Total Risk versus Residual Risk

X

- Handling Risk

X

Information Classification

- Private Business versus Military
Classifications

Layers of responsibility

Hiring Practices

CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

Security Awareness Training

(J) Telecommunications, Network and Internet Security

Telecommunications and Network Systems

X

Open System Interconnect Model

- Application Layer
- Presentation Layer
- Session Layer
- Transport Layer
- Network Layer
- Data Link Layer
- Physical Layer

Tying the layers together

TCP/IP

- TCP
- TCP Handshake
- Data Structures
- IP Addressing

Types of Transmission

- Analog and Digital
- Asynchronous and Synchronous
- Broadband and Baseband

Networking

Network Topology

- Ring Topology
- BUS Topology
- STAR Topology
- Mesh Topology
- LAN Media Access Technologies
- Cabling
- LAN Transmission Methods

LAN Media Access Technologies

- Token Passing
- CSMA
- Collision Domains
- Polling

Protocols

- Address Resolution Protocol
- Reverse Address Resolution Protocol
- Internet Control Message Protocol

Networking Devices

- Repeaters

	CIS 100	CIS 105	CIS 121	CIS 123	CIS 321	CIS 471	CIS 472	CIS 473	CIS 474	CIS 476	CIS 519	CIS 521	CIS 529	CIS 575
--	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------	---------

- Bridges
- Forwarding Tables
- Routers
- Routing
- Switches
- VLAN
- Gateways
- PBX
- Firewalls

X

Network Segregation and Isolation

Networking Services

- Network OS
- DNS
- Internet DNS and Domains
- Directory Services

Intranets and Extranets

- Network Address Translation

Metropolitan Area Network

WAN

- Telecommunications Evolution
- Dedicated Links
- T Carriers
- S/WAN
- WAN Technologies
- Multiservice Access Technologies

Remote Access

- Dial-Up and RAS
- ISDN
- DSI
- Cable Modems
- VPN
- Tunneling Protocols

X

Network and Resource Availability

- Single Points of Failure
- RAID
- Clustering
- Backups

Wireless Technologies

- Wireless Communication

X	X
X	X



**Information Assurance Program Mapped to
Undergraduate Degree in Computer Science Curriculum**

Suggested Program		Suggested Program	
Freshman Fall: 17hrs	Credit	Freshman Spring: 17hrs	Credit
CIS 100 Info tech & Com application	3	CIS 105 Programming Principles I	3
CIS 101 Computer Science Overview	3	CIS 121 Intro Computer Systems	3
GED 100 1 st Yr Seminar 1	1	GED 101 1 st Yrs Seminar II	1
MAT 111 Calculus 1	4	MAT 112 Calculus II	4
ENG 105 English Comp	3	ENG 106 English Comp	3
Humanities	3	STA 101 Fund of Speech	3
Sophomore Fall: 16hrs		Sophomore Spring: 17	
CIS 106 Programming Principles II	3	CIS 200 Structure Programming	3
MAT 214 or MAT 325	3	CIS 123 Data Structures	3
MAT 311 Math Logic	3	CIS 227 Discrete Structure	3
For Lang 201	3	For Lang 202	3
Science I Required	4	Science II Required	4
		PED 101/102	1
Junior Fall: 18 hrs		Junior Spring: 18hrs	
CIS 476 Programming. Languages	3	CIS 301 Comps System Software	3
CIS 474 Intro to Database	3	CIS 321 Software Methodology	3
BUS 207 Prin of Acct	3	CIS 472 Computer Architecture	3
HIS 201 History 1	3	HIS 202 History II	3
BUS 340 Principle of Management	3	BUS 313 Statistics	3
Rel/Phil Req	3	ENG 201/202	3
Senior Fall: 18hrs		Senior Spring: 15 hrs	
CIS 429 Web Design & E-Commerce	3	CIS 482 Intro Info Systems	3
CIS 475 Introduction to AI	3	CIS 473 Intro to Operating System	3
CIS Elective	3	CIS 471 Intro Comp Algorithms	3
ECO 107	3	CIS Design Project	3
Psychology	3	CIS Elective	3

Information Assurance & Security Courses

CIS 519 IA Tools & DB administrative	3	CIS 521 Information Security Systems	3
		CIS 575 Wireless Communications	3



Clark Atlanta University
Information Assurance and Security

CIS 100
Information Technology and Computer Applications Computer

Overview:

- Description
- Objective(s)
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours
Pre-Requisite : None

Target Audience

Levels	Disciplines		
	CS		CIS
Undergraduate	x		x
Graduate			

Description:

This course introduces students to the general concepts of Information Assurance. It includes a very brief overview of the threats posed by the Internet, legal and ethical issues relating to IA and the Internet, various types of computer crimes, and different methods of securing home computers.

Objective(s):

The primary purpose of this course is to:

- Introduce students to Information Assurance.
- Discuss threats posed by the Internet.
- Discuss legal and ethical issues relating to IA and the Internet.
- Discuss the various types of computer crimes.
- Discuss the many methods of securing home computers.

Goals/Outcome:

The students will be able to:

- Understand information assurance - what it is and why it is important
- Identify threats posed by the Internet (students will learn the various threats and how each of them are implemented by hackers)
- Identify the legal and ethical laws related to Information Assurance
- Identify computer crimes and how to safeguard their personal computers.

Outline:

- Information Assurance
 - What is Information Assurance ?
 - Why is it important ?
 - Who is at risk ?
- Threats Posed by the Internet
 - Viruses
 - Backdoors
 - Trapdoors
- Legal and Ethical Issues of Information Assurance
 - Understanding law and ethics
- Computer Crimes and how to Prevent Them
 - Computer Crimes
 - Hacking
 - Sniffing
 - Preventing Computer Crimes
 - Firewalls
 - Antivirus Software

Suggested Assignments:

- Select five different kinds of computer attacks and briefly discuss them.
- Write a paper on why IA is important and tips to protect yourself from computer crime

References:

- [An Introduction to Information Assurance](http://www.itea.org). International Test and Evaluation Association. April 1, 2005. <http://www.itea.org>
- [Information Assurance: Defense against the Dark Acts](http://www.randollarson.org/security/ia/). Estrella Mountain Community College. April 1, 2005. [<http://www.randollarson.org/security/ia/>](http://www.randollarson.org/security/ia/)
- [K-5 Information Security Curriculum](http://www.cerias.purdue.edu/education/k12/infosec_activities/k5_curriculum.php). CERIAS. May 28, 2005. [<http://www.cerias.purdue.edu/education/k12/infosec_activities/k5_curriculum.php>](http://www.cerias.purdue.edu/education/k12/infosec_activities/k5_curriculum.php)



Clark Atlanta University
Information Assurance and Security

CIS 105
Structured Programming

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3 class periods

Course Length: 3 Hours

Pre-Requisite : None

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	X	X
Graduate		

Description:

This course introduces students to the concepts of Information Assurance as it relates to Structured Programming. It includes a very brief overview of the topic of secure programming methods, ethical issues in programming security, and the use of class loaders and security managers.

Objective(s):

The primary purpose of this course is to:

- Introduce students to the importance of program security.
- Introduce ethical issues dealing with program security.

Goals/Outcome:

The students will be able to:

- Understand the importance of program security and how to implement secure control structures such as modularity and data hiding.
- Identify class loaders and their responsibility for determining when and how classes can be added to a running Java environment, as well as making sure that important parts of the Java runtime environment are not replaced by impostor code.
- Identify security managers and the methods that could be used with it.

Outline:

- Secure programs
 - What is a secure program?
 - Unexpected program behavior
 - Types of flaws
 - validation error (incomplete or inconsistent)
 - domain error
 - serialization and aliasing
 - inadequate identification and authentication
 - boundary condition violation
 - other exploitable logic errors
- Class Loaders
 - What is a class loader?
 - enable the JVM to load classes without knowing anything about the underlying file system semantics
 - allow applications to dynamically load Java classes as extension modules
 - How are they used?
- Security Managers
 - What are security managers?
 - Establishes a custom security policy for Java applications
 - What are the different security manager methods and how are they implemented?
 - checkRead
 - checkWrite
 - checkConnect

Suggested Assignments:

- Write a paper to discuss the security issues surrounding network class loaders.
- Install a security manager and write a program that uses one of the “check” methods of the security manager.

References:

- Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, N.J.: Prentice-Hall, 1977.
- Mahmoud, Qusay H. "Understanding Network Class Loaders." Sun Microsystems. October 2004. April 11, 2005.< <http://java.sun.com>>
- Oaks, Scott. Java Security. Sebastopol, CA : O'Reilly, 1999, 1998.
- Pfleeger, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ: Prentice-Hall, 2003.
- Venners, Bill. "Java security: How to install the security manager and customize your security policy." Java World. November 1997. April 11, 2005.< <http://www.javaworld.com>>



Clark Atlanta University
Information Assurance and Security

CIS 121
Introduction to Computer Systems

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 105

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

The information assurance module for this course focuses on concepts of information assurance related to computer architecture design, vulnerabilities commonly associated with computing environments, possible attacks, and methods of defense. It introduces students to survivability in the context of computer security, vulnerabilities and attacks associated with computer architecture, IA concerns involving hardware and data sharing and the role of security in operating systems, hardware, and software.

Objective(s):

The primary purpose of this course is to:

- Provide an understanding of information design principles related to computer organization.
- Describe basic information assurance concepts related to different components of a computer system such as memory, the operating system, hardware, and software.
- Identify vulnerabilities associated to data sharing, hardware sharing, and the complexity of computer systems.
- Describe different types of attacks that occur from vulnerabilities related to computer architecture.
- Identify methods of defense for computer systems.

Goals/Outcome:

The students will be able to:

- Identify the Principles of Survivability and Information Assurance and relate these principles to good design practices for computer systems.
- Identify several security vulnerabilities and the types of attacks that they expose systems to.
- Identify the cause of common vulnerabilities related to computer organization.
- Identify the basic architectural elements and discuss security implications of each element.

Outline:

- Principles of Survivability and Information Assurance
http://www.cert.org/info_assurance/principles.html
 - [Principle 1: Survivability is an enterprise-wide concern.](#)
 - [Principle 2: Everything is data.](#)
 - [Principle 3: Not all data is of equal value to the enterprise – risk must be managed.](#)
 - [Principle 4: Information assurance policy governs actions.](#)
 - [Principle 5: Identification of users, computer systems, and network infrastructure components is critical.](#)
 - [Principle 6: Survivable Functional Units \(SFUs\) are a helpful way to think about an enterprise's networks.](#)
 - [Principle 7: Security Knowledge in Practice \(SKiP\) provides a structured approach.](#)
 - [Principle 8: The road map guides implementation choices \(all technology is not equal\).](#)
 - [Principle 9: Challenge assumptions to understand risk.](#)
 - [Principle 10: Communication skill is critical to reach all constituencies.](#)
- Vulnerabilities commonly encountered in computing environments
 - Contamination and Interference
 - Changes Between Time of Check and Time of Use
 - Unenforced Restrictions
 - Covert Channels
- Possible Attacks as it relates to Computer Architecture:
 - Browsing
 - Trojan Horse
 - Virus
- Methods of Defense- Hardware and Software Security and Firmware
 - Application Controls and Security
 - Intrusion Detection Systems
- Legal and Ethical Implications
 - Introduction to Information Warfare
 - role of ethics in decision making and professional practice

Suggested Assignments:

- Students will be organized into four groups. Each group will give a presentation about one of the four vulnerabilities discussed in class. The presentation will include causes for the vulnerability, possible attacks, and methods of defense. The presentation will also include information about modern incidents involving this vulnerability or one or more of the attacks discussed in their presentation.
- Students will research security issues related to hardware, computer system design, or operating systems and present findings to the class.

References:

- Krause, Micki & Tipton, Harold . “Handbook of Security Management: Computer Architecture.” March, 2005.
<<http://www.cccure.org/Documents/HISM/404-407.html>>
- Pfleeger, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ: Prentice-Hall, 2003.
- “Principles of Survivability and Information Assurance.” CERT Coordination Center. March, 2005
<http://www.cert.org/info_assurance/principles.html#p1>



Clark Atlanta University
Information Assurance and Security

CIS 123
Data Structures

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 105

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

This course introduces students to the concepts of Information Assurance as it relates to Data Structures. It introduces students to secure programming methods, ethical issues in programming security, buffer overflows and their vulnerabilities, and survivability in the context of computer security. Technically this course examines the general dimension of providing security in software and data architectures.

Objective(s):

The primary purpose of this course is to:

- Make students understand the importance of program security and how to implement secure control structures such as modularity and data hiding.
- Introduce ethical issues dealing with program security.
- Introduce buffer overflows and explain why they are considered vulnerable.
- To provide an understanding of survivability and information assurance.

Goals/Outcome:

The students will be able to:

- Understand encapsulation - using classes and securing code against corruption.
- Understand modularity and its implementation in data hiding (modules should be specified and designed so that information – procedure and data – contained within a module is inaccessible to other modules that have no need for such information)
- Understand data hiding as a design criterion (because most data and procedure are hidden from other parts of the software, inadvertent errors introduced during modification are less likely to propagate to other locations within a software)
- Understand buffer overflows – what they are and why they are considered to be vulnerable.
- Understand survivability principles

Outline:

- Secure programs
 - What is a secure program?
 - Unexpected program behavior
 - Types of flaws
 - validation error (incomplete or inconsistent)
 - domain error
 - serialization and aliasing
 - inadequate identification and authentication
 - boundary condition violation
 - other exploitable logic errors
- Controls against program threats
 - Developmental Controls
 - Modularity
 - Encapsulation
 - Information Hiding
 - Cohesion
 - Coupling
- Ethical Issues in Computer Security
 - Understanding law and ethics
 - Protection of programs and data
- Buffer Overflows and Their Vulnerability
 - What is a buffer overflow?
 - Why are they vulnerable?
- Principles of Survivability and Information Assurance
 - http://www.cert.org/info_assurance/principles.html
 - What is a Information Assurance
 - [Principle 1: Survivability is an enterprise-wide concern.](#)
 - [Principle 2: Everything is data.](#)
 - [Principle 3: Not all data is of equal value to the enterprise – risk must be managed.](#)
 - [Principle 4: Information assurance policy governs actions.](#)
 - [Principle 5: Identification of users, computer systems, and network infrastructure components is critical.](#)

- [Principle 6: Survivable Functional Units \(SFUs\) are a helpful way to think about an enterprise's networks.](#)
- [Principle 7: Security Knowledge in Practice \(SKiP\) provides a structured approach.](#)
- [Principle 8: The road map guides implementation choices \(all technology is not equal\).](#)
- [Principle 9: Challenge assumptions to understand risk.](#)
- [Principle 10: Communication skill is critical to reach all constituencies.](#)

Suggested Assignments:

- Review a previous programming assignment and identify possible insufficient programming techniques that could lead to various vulnerabilities.
- Write a program to simulate buffer overflow.

References:

- Cowan, Crispin. [Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade.](#) Oregon Graduate Institute of Science & Technology. April 7, 2005.
<http://csdl.computer.org>
- Hoffman, Lance J. [Modern Methods for Computer Security and Privacy.](#) Englewood Cliffs, N.J.: Prentice-Hall, 1977.
- Mader, Chris. [Information Systems: Technology, Economics, Application, and Management.](#) Chicago: Science Research Associates, 1979.
- Pfleeger, Charles P. and Shari Lawrence. [Security in Computing.](#) Upper Saddle River, NJ: Prentice-Hall, 2003.
- Shooman, Martin L. [Software Engineering: Design, Reliability, and Management.](#) New York: McGraw-Hill. 1983.



Clark Atlanta University
Information Assurance and Security

CIS 321
Introduction to Software Engineering

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 123

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:
This course will discuss Information Assurance concepts related to Software Engineering. It will highlight design principles and vulnerabilities related to Software Engineering and discuss how to effectively incorporate Information Assurance to software-based systems. The course will also discuss standards for Information assurance in Software Engineering and explain how to apply standards to software design.

Objective(s):

The primary purpose of this course is to:

- To provide an understanding of information design principles related to computer organization.
- To describe basic information assurance concepts related to different components of a computer system such as memory, the operating system, hardware, and software.
- To identify vulnerabilities associated to data sharing, hardware sharing, and the complexity of computer systems.
- To describe different types of attacks that occur from vulnerabilities related to computer architecture.
- To identify methods of defense for computer systems.

Goals/Outcome:

The students will be able to:

- Learn about different attack methods and predictive analysis techniques.
- Learn strategies for developing and measuring the economics of information security solutions.
- Identify vulnerabilities related to Software Engineering.
- Identify good IA practices for Software Engineering.
- Identify several IA standards for Software Engineering.
- Understand how and when to use standards.

Outline:

- Vulnerabilities that must be considered in Software Engineering
 - Possible stop-fail mechanisms and procedures
 - Fallback, contingency solutions for both direct and secondary effects of failure modes.
 - Unenforced Restrictions
 - Covert Channels
 - Buffer Overflows
- Best-Practices in IA Software Development Systems:
 - Usage Scenarios
 - Modeling and analysis of a system's interaction with external factors
 - Mission Assurance
 - Documentation
 - Information Assurance Policies
 - Encapsulation
 - Modularity
 - Data Hiding
- Software Survivability
 - Software Disaster Recovery
 - Software Risk Mitigation
 - Software Backups
- Challenges and Questions
 - IA Standards related to software engineering: Do we have the right standards in place?
 - How to determine which standards apply and when they apply.

Suggested Assignments:

- Students will incorporate an information assurance module in to their semester project. The module will discuss good practices of IA in Software engineering that were used and implement IA polices in their software design. Students will provide accurate documentation where applicable
- Students will assess semester project for better development methodologies against IA Standards

References:

- "Information Assurance." Federal CIO Certificate Program
April 11, 2005 <http://ieeieia.org/>
- Pfleeger, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ: Prentice-Hall, 2003.



Clark Atlanta University
Information Assurance and Security

CIS 471
Introduction to Algorithms

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 4 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 221, CIS 123

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:
This course will discuss Information Assurance concepts related to computer algorithms. It will highlight methods of securing computing systems using cryptographic algorithms. It will also discuss vulnerabilities concerning these algorithms, password cracking, and determining an acceptable level of risk.

Objective(s):
The primary purpose of this course is to:

- Provide an understanding various methods of encryption and cryptography.
- Identify methods of cryptanalysis.
- Provide an understanding of terminology related to secure algorithms.
- Discuss methods for password cracking.
- Provide an understanding of risk analysis and developing and acceptable level of risk.

Goals/Outcome:

The students will be able to:

- Learn about different encryption algorithms.
- Identify elements of a good encryption algorithm.
- Differentiate between secret key cryptography and public key cryptography and identify methods of implementing each.
- Learn methods of cryptanalysis.
- Identify vulnerabilities encryption and cryptographic algorithms.
- Identify good IA practices for Software Engineering.
- Identify several techniques for password cracking
- Understand how to assess risks.

Outline:

- Terminology
 - Cryptosystem
 - Encryption/Decryption
 - Cipher
- Cryptography
 - Secret Key Cryptography
 - Block Ciphers
 - Hash Algorithms
 - Stream Ciphers
 - Public Key Cryptography
 - Vulnerabilities
 - Trapdoors
- Encryption Algorithms
 - Symmetric and Asymmetric Keys
 - Representing Characters
 - Substitutions
 - Popular Encryption Algorithms (Student Assignment)
 - Vulnerabilities of Encryption
 - Hackers
 - Cryptanalysts
- Properties of “ Trustworthy Encryption Systems”
 - Sound Mathematics
 - Reliable Analysis
 - Time (Pfleegler pg. 59)
- Methods of Cryptanalysis
 - Finding Patterns
 - Inferring Meaning
 - Key Deduction
 - General Encryption Weaknesses

- Password Cracking
 - Dictionary Attacks
 - Exhaustive/Brute Force Attacks
 - Probable Passwords
 - Encrypted Password List
 - Hybrid Attacks
- Protecting Passwords
- Acceptable Level of Risk
 - Risk Analysis
 - Error Analysis
 - Fault Tolerance

Suggested Assignments:

- Students will write a program to simulate an encryption or cryptographic algorithm.
- Students will develop a software program for cracking a password. Students may use any method for password cracking.

References:

- “Cryptographic Algorithms.” Kremlin Powerful Security for a Powerful World April 19, 2005 <http://www.kremlinencrypt.com/algorithms.htm>
- Pfleeger, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ: Prentice-Hall, 2003.



Clark Atlanta University
Information Assurance and Security

CIS 472
Computer Architecture

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3 Class Periods

Course Length: 3 Hours
Pre-Requisite : CIS 121, CIS 225

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

The information assurance module for this course focuses on the introduction of security architecture. It will identify the elements of security architecture and describe the services it must provide in order to ensure security, the system elements required to implement the architecture, and the performance required to ensure that it functions properly. It also examines unintentional errors, intentional attacks, and layered security architecture.

Objective(s):

The primary purpose of this course is to:

- To provide definitions to terminology related to information assurance issues in computer organization.
- Identify Information Assurance issues related to the basic components of computer architecture.
- Identify the elements of security architecture and discuss the security services provided, required system elements, and required performance levels.
- Discuss layered security architecture and its problems
- Identify unintentional and intentional threats that affect computer architecture.

Goals/Outcome:

The students will be able to:

- Identify terminology related to Information Assurance and computer/security architecture.
- Identify the basic components of computer architecture and discuss their importance in Information Assurance.
- Define the term security architecture and identify the elements that it should include.
- Understand the concept of a layered security architecture and its problems
- Discuss the threat of unintentional errors and intentional attacks to computer security.

Suggested Assignments:

- Students will write a paper discussing the implications of overtaxed and mismatched security layers.

Outline:

- Terminology
 - Security Policy
 - Security Measures
 - Security Mechanism
 - Security Perimeter
 - Security Model
 - Threat Action
- Information Assurance and the Basic Components of Computer Architecture
 - Domains
 - States
 - Finite State Machines
 - Security Domains
- Introduction to Security Architecture
 - Security Services
 - Required System Elements
 - Required Performance Levels
- Elements of Security Architecture
 - Administrative security
 - Communication security
 - Computer security
 - Emanations security
 - Personnel security
 - Secure storage
 - Physical security
 - Hardware
 - Software
- Firmware Intentional and Non-intentional Attacks to Computer Architecture
- Layered Security Architecture- Common Data Security Architecture(CDSA)
 - Applications
 - Layered services and middleware
 - Common Security Services Manager (CSSM) infrastructure
 - Security Service Provider Modules
- Problems with Layered Security Architecture
 - Overtaxing
 - Mismatching

References:

- Krause, Micki & Tipton, Harold. "Handbook of Security Management: Computer Architecture" March, 2005 <<http://www.cccure.org/Documents/HISM/404-407.html>>
- Mackey, Richard. "Layered Insecurity." Information Security. June 2002 April 23, 2005 <<http://infosecuritymag.techtarget.com/2002/jun/insecurity.shtml>>
- "Security Forum." The One Group. 1995-2005 April 23, 2005 <<http://www.opengroup.org/security/l2-cdsa.htm>>
- "Strong, Layered WLAN Security Architecture Protects Users, Data, Network." 3com Corporation. 1995-2005 <http://www.3com.com/wireless/FIPS/fips_architecture.html>



Clark Atlanta University
Information Assurance and Security

CIS 473
Introduction to Operating Systems

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 3-4 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 301

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

The information assurance module for this course focuses on concepts of information assurance dealing with operating systems. It introduces IA concepts related to secure operating systems and discusses protected objects, access control, separation in OS, memory and file protection, as well as vulnerabilities and attacks that are commonly associated with operating systems.

Objective(s):

The primary purpose of this course is to:

- Provide an understanding of information design principles related to computer organization.
- Identify general objects controlled by the operating system and discuss methods of their protection.
- Identify vulnerabilities associated with operating system design.
- To describe different types of attacks targeted at Operating Systems.
- Identify the importance of separation in the protection of operating systems.
- Identify methods of defense for computer systems.

Goals/Outcome:

The students will be able to:

- Identify IA concepts relating to operating systems.
- Identify several security vulnerabilities and the types of attacks that operating systems are susceptible to.
- Discuss attacks that are target operating systems
- Identify methods for protect operating systems from intruders.

Outline:

- Introduction to IA Concepts related to Operating Systems
 - Privilege
 - Integrity
 - Trusted System
 - Secure Operating System/subsystem
- Protected Objects
 - Memory
 - Sharable I/O Devices
 - Serially reusable I/O Devices
 - Sharable Programs and Sub-procedures
 - Networks
 - Sharable Data
- Levels of Protection in Operating Systems
 - Do not Protect
 - Isolate
 - Share all of nothing
 - Share access via limitation
 - Classification levels
 - Control of Access to General Objects
- Vulnerabilities related to Operating System
 - Incomplete Parameter Checking
- Possible Attacks on Operating Systems:
 - Bomb
 - Trojan Horse-Rootkit
 - Exploitation
 - Pseudo-Flaw
 - Negative Acknowledgement Attack
- Separation in Operating Systems
 - Physical Separation
 - Temporal Separation
 - Logical Separation
 - Cryptographic Separation
- Memory and Address Protection
 - Fence
 - Relocation
 - Base/Bounds Registers
 - Tagged Architecture
 - Segmentation
 - Paging
 - Combined Paging and Segmentation
- File Protection Mechanisms
- Trusted OS
 - Design Elements
 - Security Features
 - Assurance in Trusted Operating Systems
- Other Methods of Defense
 - Host-Based Security
 - Operation System Controls
 - Reference Monitor

Suggested Assignments:

- Alfred insurance needs a security policy in order to protect their organization's computers from attack. Research security policies and develop one for Alfred Insurance that adequately protects the resources of their computers.
- Write a paper discussing the meaning of separation in operating systems and discuss its importance. Be sure to include mechanisms for ensuring separation in operating systems.

References:

- Pleegar, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ : Prentice Hall, 2003
- "Principles of Survivability and Information Assurance." CERT Coordination Center. March, 2005
<http://www.cert.org/info_assurance/principles.html#p1>



Clark Atlanta University
Information Assurance and Security

CIS 474
Introduction to Database Systems

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 4 class periods

Course Length: 3 Hours

Pre-Requisite : CIS 209 or CIS 211

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

This course introduces students to the concepts of Information Assurance as it relates to databases. It introduces students to various database vulnerabilities, inference, and cryptography. Technically this course examines the general dimension of providing security in database systems.

Objective(s):

The primary purpose of this course is to:

- Introduce inference as a database security issue.
- Introduce cryptography and how it can be used in databases.
- Introduce various database vulnerabilities.
- Introduce the importance server security, user authentication, and session security as it relates to database security.

Goals/Outcome:

The students will be able to:

- Identify what inference is and understand how it can be controlled.
- Identify what cryptography is and how it can be used with databases.
- Identify various database vulnerabilities.
- Identify the importance of server security, user authentication, and session security as it relates to database security.

Outline:

- Inference
 - What is inference?
 - What can be done about inference?
 - The use of polyinstantiation – technique that allows different records to exist in the same table at various security levels.
- Cryptography Principles
 - What is cryptography?
 - Use of encryption to secure information
 - Public key infrastructure
 - Digital signatures
- Database Vulnerabilities
 - Server Security
 - Database Connections
 - Table Access Control
 - Restricting Database Access
- Primary Areas of Database Security
 - Server Security
 - ensuring security relating to the actual data or private HTML files stored on the server
 - User-authentication security
 - ensuring login security that prevents unauthorized access to information
 - Session security
 - ensuring that data is not intercepted as it is broadcast over the Internet or Intranet
- How sensitive data can be obtained from queries
 - Direct Attack
 - Indirect Attack
 - Sum
 - Count
 - Median
 - Tracker Attacks
 - Linear System Vulnerability

Suggested Assignments:

- Create a database that contains students' username and password information. Write an encryption program that encrypts the password as it is input into the database.
- Research various ways data can be obtained from a database. Chose one and write a two page paper explaining what it is and how it is used.

References:

- Cannady, James. "Security Models for Object-Oriented Databases". April 18, 2005. <www.cccure.org>
- Rahmel, Dan. "Database Security". Internet Systems. April 1997. April 18, 2005. <<http://www.governmentsecurity.org>>
- Wiedman, Blake. "Database Security (Common-sense Principles)". April 18, 2005. <<http://www.governmentsecurity.org>>





Clark Atlanta University
Information Assurance and Security

CIS 476
Programming Languages and Compilers

Overview:

- Description
- Objective
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 221, CIS 123

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:
This course introduces students to the concepts of Information Assurance as it relates to various programming languages and compilers. It includes a very brief overview of the topic of secure programming methods, ethical issues in programming security, and the security issues related to encapsulation and data abstraction.

Objective(s):
The primary purpose of this course is to:

- Make students understand the importance of program security and how to implement secure control structures such as modularity and data hiding.
- Discuss ethical issues dealing with program security.
- Discuss the use of encapsulation and data abstraction as it relates to program security.

Goals/Outcome:

The students will be able to understand the following concepts:

- The importance of program security and how to implement secure control structures such as modularity and data hiding.
- Encapsulation using classes and securing code against corruption. Hiding a component's implementation details.
- Data abstraction as a design criterion (because most data and procedure are hidden from other parts of the software, inadvertent errors introduced during modification are less likely to propagate to other locations within a software).

Outline:

- Secure programs
 - What is a secure program?
 - Unexpected program behavior
 - Types of flaws
 - validation error (incomplete or inconsistent)
 - domain error
 - serialization and aliasing
 - inadequate identification and authentication
 - boundary condition violation
 - other exploitable logic errors
- Ethical Issues in Computer Security
 - Understanding law and ethics
 - Protection of programs and data
- Encapsulation
 - What is encapsulation?
 - The wrapping of data and functions into a single unit (called class)
- Data Abstraction
 - What is data abstraction?
 - How is it used?
 - ensures security of data from unexpected viewing, changing, or

Suggested Assignments:

- Students will write a paper discussing a programming language and some of the specific vulnerabilities for that language.
- Students will chose a programming language and write a program to implement encapsulation and/or data abstraction.

References:

- Cannady, James. "Security Models for Object-Oriented Databases". April 18, 2005. www.cccure.org
- Hoffman, Lance J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, N.J.: Prentice-Hall, 1977.
- Pfleeger, Charles P. and Shari Lawrence. Security in Computing. Upper Saddle River, NJ: Prentice-Hall, 2003.

Clark Atlanta University
Information Assurance and Security

CIS 519
IA Tools and DB Administration

Overview:

- Description
- Objective(s)
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours

Pre-Requisite : CIS 123, CIS 474

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

An introduction to the various technical and administrative aspects of Information Security and Assurance. This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system and Database Administration, with appropriate intrusion detection and reporting features.

Objective(s):

The primary purpose of this course:

- Knowledge of the importance of Database Security and how it affects our changing world.
- Knowledge of the basic concepts of Security Requirements, especially the close relation between the objective of machine security and human factors
- Understand the basic concepts of database reliability and integrity
- Understand the basic concepts of Encryption, Program Threats, and Trusted Operating Systems
- Be capable of developing a Security Policy for an Organization
- Understand the relationship between software development and information security
- Identify the key areas of Security in Networks
- Learn how to critically analyze situations of Threats in Networks

Goals/Outcome:

Upon completion of this course, students should understand the following concepts:

Knowledge of Administering Security (the passwords, files, and data)

- Knowledge of protections against malicious logic
- Identify and prioritize security Planning
- Identify and prioritize threats to information assets.
- Define an information security strategy and architecture.
- Plan for and respond to intruders in an information system
- Describe legal and public relations implications of security and privacy issues.
- Present a disaster recovery plan for recovery of information assets after an incident
- Be aware of Legal, Privacy, and Ethical Issues in Computer Security
- Understand the Right of Employees and employers
- Understand the fundamental concepts of Cryptographic Systems

Outline:

- Introduction to Information Assurance and Databases and its Security
- Multilevel secure databases: partitioned, cryptographically sealed, filtered
- General procedures in facilities (standards operation)
- The threats to security in computing: interception, interruption, modification, fabrication
- Controls Available to Address these Threats and its consequences:
 - Investigative analysis
 - Encryption, programming controls, operating systems
 - Network controls, administrative controls
 - Law and ethics (criminal consequences).
- Threats against networked applications, including denial of service, web site defacements, malicious mobile code, and protocol attacks.
- Controls against network attacks:
 - Physical security;
 - Control and modify policies and procedures;
 - Control range of technical issues.
 - Discuss specific agency security policies
 - Countermeasures to reduce the impact of threats.
- Security goals: the confidentiality, integrity, and availabilities
- Vulnerabilities control (hardware and its peripheral devices, software, data and other exposed assets)
- Program development controls against malicious code and vulnerabilities-software engineering principles and practices
- Administering Security: Security Plan, Risk Analysis, Assessments, System Life Cycle Management
- Security Policy- high-level standards for users and managers
 - Identifies and organizes the security activities for the users and managers
 - Access control authorization
 - Accountability (train users about the computer security principles)
 - Monitoring users computer systems (access authorization)
 - Intrusion detection
 - Law regulations, and other public policy
- Physical Security and standards (protecting outside the computer system)
 - Contingency planning- recovery adequate preparation based on the standards
 - Tempest- U.S. government program under which computer equipment is certified as emission-free.
 - Natural threats (flood, fire, earthquake, etc...)
 - Environmental control (flood, fire, safety, etc...)
 - Facilities management (disaster recovery plan testing)
 - Network storage
- Legal, Privacy ACT (1974, 1986, 2001), and Ethical Issues in Computer Security
- Protection of programs and information, equipments by patents, copyrights, and trademarks
- Ethical analysis of computer security situations
- Code of professional ethics, standard of conduct (monitoring keystroke)
- Introduction to Operation Security
- Protecting in General-purpose Operating Systems
 - User authentication
 - Controlled access to voice and data communications
 - Protecting memory, files and the execution environment
- Cryptography Concepts
 - Concepts of Encryption (clearly address the need for confidentiality of data)
 - Asymmetric encryption and RSA algorithm
 - National policies and procedures (enforcing security through hardware or software means)
- Security Networks Concepts, Traffic Control, Firewalls, IDS, Secure e-mail/phone mail, and modems



Clark Atlanta University
Information Assurance and Security

CIS 521
Introduction to Information Security

Overview:

- Description
- Objective(s)
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours
Pre-Requisite : CIS 123, CIS 474

Target Audience

Levels	Disciplines	
	CS	CIS
Undergraduate	x	x
Graduate		

Description:

This course provides an overview of Information Security. It is designed to teach Computer Science students' important issues in Information Security from both the computational and administrative viewpoint. Thus the while the primary emphasis of this course is technical – it examines the issues of providing security for information processing systems--secure operating systems and applications, network security, cryptography, security protocols, etc., this course also examines security from an administrative perspective- the importance of management and administration, and the place information security holds in overall business risk.

Objective(s):

The primary purpose of this course:

- Understand the importance of information security and how it affects our changing world.
 - Understand the basic concepts of Information Security, especially the close relation between the objective of machine security and human factors
 - Understand the basic concepts of Encryption, Program Threats, and Trusted Operating Systems
- Be capable of developing a Security Policy for an Organization
- Understand the relationship between software development and information security
 - Identify the key areas of information security and how they work.
 - Learn how to critically analyze situations of computer use, identifying the issues, consequences, and viewpoints

Goals/Outcome:

Upon completion of this course, students should understand the following concepts:

Identify and prioritize information assets.

- Identify and prioritize threats to information assets.
- Define an information security strategy and architecture.
- Plan for and respond to intruders in an information system
- Describe legal and public relations implications of security and privacy issues.
- Present a disaster recovery plan for recovery of information assets after an incident

Outline:

- Security Problems in Computing- What does “Secure” means?
- The risks involved in computing:
 - Risk assessment, acceptance, and management;
 - Risk assessment—information states and valuation;
 - Validation testing;
 - Traffic analysis;
 - Information processing and storage.
- The goals of secure computing: information characteristic, confidentiality, integrity, and availability
- The threats to security in computing: interception, interruption, modification, fabrication
 - Security investigation procedures
- Controls Available to Address these Threats:
 - Human-threats
 - Encryption, programming controls, operating systems,
 - Network controls, administrative controls
 - Law (enforcement interface) and ethics.
 - International laws and legal bodies
- The meaning of Computer Security
- Plan security program for users and managers
- Computer Criminals:
 - The career computer criminals and understanding of the targets of computer crime
 - Accountability of the employees for accessing information and protecting their organization (fraud, waste, & abuse)
- Vulnerabilities management and analysis
 - Records management
 - Records retention
 - Hardware asset management,
 - Software asset management
 - Mail retention
 - Exposed assets
- Program security and development controls against malicious code and vulnerabilities-software engineering principles and practices
- Protecting in General-purpose Operating Systems
 - User authentication
 - Controlled access to objects
 - Protecting memory, files and the execution environment
- Methods of Defense
 - Concepts of Encryption (clearly address the need for confidentiality of data)
 - Asymmetric encryption and RSA algorithm
 - Key exchange protocols and certifications
 - National policies and procedures (enforcing security through hardware or software means)
 - Controls (software, hardware, physical controls)
 - Handling media (complying with rules and regulation, etc.)
- Designing Trusted Operating Systems
 - What makes operating systems “secure”? or “trustworthy”?
 - How are trusted systems designed (employee clearance)
 - How do we develop “assurance” of the correctness of a trusted operating system?
 - Evaluation of the “Trusted Computer Systems”
 - Security clearances
- Management of Information Security: Review Policies and Procedures.
 - Key management rules
 - Introduce to users and manger about COMSEC/security profiles
 - COMSEC custodian process and relevant to users and mangers
 - Program budget and evaluation
 - Ethical procedures
 - Deliberate planting of apparent security weaknesses

- Information Systems Security Policies
 - Incorporate technical security policies
 - Train users about policies (physical controls, transportation)
 - Evaluate security policies (control disgruntled employees)
 - Ensure adaptive security policies implementation
 - Define computer security principles
 - Risk involve operation security
 - Auditing tools (policy and procedures)
- Emerging Trends in Certification and Accreditation
- Network security evaluation
 - Products
 - Third party
 - Cost & benefit analysis
- Information Security oversight Office (ISOO) rules
 - Marking of media
 - Labeling
 - Marking of sensitive information
 - Discuss the list of command security policies and safeguards



Clark Atlanta University
Information Assurance and Security

CIS 429
Web Design and E-Commerce

Overview:

- Description
- Objective(s)
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours
Pre-Requisite : None

Target Audience

Levels	Disciplines		
	CS		CIS
Undergraduate	x		x
Graduate			

Description:
This course briefly introduces students to various web based attacks and defenses. It discusses the vulnerabilities for languages such as HTML, JAVA and discusses various countermeasures that are available. It also elucidates various Web-hacking .tools that are available along with their countermeasures

Objective(s):
The primary purpose of this course is to:

- Introduce students to Web based attacks and defenses
- Discuss threats posed in various Web development languages
- Discuss various web vulnerabilities and defenses
- Elucidate various Web Hacking Tools and countermeasures

Goals/Outcome:

The students will be able to:

- Understand the concept of Web security - what it is and why it is important.
- Identify the key areas of Security in certain Web Development Languages
- Understand Application servers, their loopholes and countermeasures
- Learn about various Web Hacking Tools
- Identify and understand SQL Attacks, HTML and URL vulnerabilities
- Brief understanding of Assembly Language through Buffer Overflows

Outline:

- HTML
 - Information leakage through HTML
 - Clues to look for
 - HTML Comments
 - Internal/External Hyperlines
 - Hidden Fields
 - Client Side Scripts
- URL
 - URL Structure
 - URL Parameter Passing
 - URL Encoding
 - Abusing URL Encoding
- Application Servers
 - Architecture of JAVA Application Servers
 - Attacking a JAVA Web server
 - Identifying loopholes in JAVA Applications
 - Countermeasures
- Web Hacking Tools
 - Achilles
 - Cookie Pal
 - Whisker
 - Brutus
- Buffer Overflows
 - Introduction to Assembly Language
 - Disassembly
 - Blind Stress Testing
- Database Access
 - Direct SQL Attacks
 - Input Validation
 - Counter Measures
 - Patches

Suggested Assignments:

References:

- Web Hacking, Attacks and Defenses, Stuart McClure, Saamil Shah and Shreeraj Shah



Clark Atlanta University
Information Assurance and Security

CIS 575
Wireless communications

Overview:

- Description
- Objective(s)
- Goals/Outcome
- Outline
- Suggested Assignments
- References

Suggested Time: 2 class periods

Course Length: 3 Hours
Pre-Requisite : None

Target Audience

Levels	Disciplines		
	CS		CIS
Undergraduate	x		x
Graduate			

Description:

This course introduces students to the concepts of Information Assurance in Wireless Communications. It discusses various security measures that are available for wireless communication networks along with various transmission security countermeasures.

Objective(s):

The primary purpose of this course is to:

- Introduce students to Information Assurance in Wireless Communications.
- Discuss threats posed in Wireless Communications
- Discuss various security measures available for wireless communication networks
- Discuss various transmission security countermeasures.

Goals/Outcome:

The students will be able to:

- Understand the concept of transmission security - what it is and why it is important.
- Identify the key areas of Security in network communications
- Learn how to critically analyze situations of Threats in Networks
- Knowledge of tempest Security methods, shielding, grounding, banding, filtering...
- Identify and prioritize threats to information assets from tempest protection.

Outline:

- Transmission Security
 - Burst Transmission
 - Convert channel control
 - Dial back
 - Directional Signals
 - Frequency Hopping
 - Jamming
 - Line-of-sight
 - Line Authentication
 - Low Power
 - Masking
 - Optical Systems
 - Protected wireline
 - Screening
 - Spread Spectrum Transmission
- Tempest Security
 - Attenuation
 - Shielding, Filtering Power
 - Cabling
 - Zone of control and protection
- Transmission security countermeasures
 - Call signs
 - Frequency
 - Pattern forewarning protection
- AIS
 - Firmware
- Telecommunications Systems
 - Hardware
- Agency Specific AIS and Telecommunications Policies
 - Points of contact

