Information Assurance and Security (IAS)

In CS2013, the Information Assurance and Security KA is added to the Body of Knowledge in recognition of the world's reliance on information technology and its critical role in computer science education. Information assurance and security as a domain is the set of controls and processes both technical and policy intended to protect and defend information and information systems by ensuring their availability, integrity, authentication, and confidentiality and providing for non-repudiation. The concept of assurance also carries an attestation that current and past processes and data are valid. Both assurance and security concepts are needed to ensure a complete perspective. Information assurance and security education, then, includes all efforts to prepare a workforce with the needed knowledge, skills, and abilities to protect our information systems and attest to the assurance of the past and current state of processes and data. The Information Assurance and Security KA is unique among the set of KA's presented here given the manner in which the topics are pervasive throughout other Knowledge Areas. The topics germane to only IAS are presented in depth in the IAS section; other topics are noted and cross referenced in the IAS KA, with the details presented in the KA in which they are tightly integrated.

The aim of this KA is two-fold. First, the KA defines the core (tier1and tier2) and the elective components that depict topics that are part of an undergraduate computer science curriculum. Secondly (and almost more importantly), we document the pervasive presence of IAS within a computer science undergraduate curriculum.

The IAS KA is shown in two groups; (1) concepts that are, at the first order, germane to Information Assurance and Security and (2) IAS topics that are integrated into other KA's. For completeness, the total distribution of hours is summarized in the table below.

	Core-Tier1 hours	Core-Tier2 hours	Elective Topics
IAS	**2**	**6**	**Y**
IAS distributed in other KA's	**23**	**46**	**Y**

IAS. Information Assurance and Security (2 Core-Tier1 hours, 6 Core-Tier2 hours)

	Core-Tier1 hours	Core-Tier2 hours	Includes Electives
IAS/Fundamental Concepts	1	2	N
IAS/Network Security	1	4	N
IAS/Cryptography			Y
IAS/Risk Management			Y
IAS/Security Policy and Governance			Y
IAS / Digital Forensics			Y
IAS / Security Architecture and Systems Administration			Y
IAS/Secure Software Design and Engineering			Y

IAS. Information Assurance and Security (distributed) (23 Core-Tier1 hours, 46 Core-Tier2 hours)

Knowledge Area and Topic	Core-Tier1 hours	Core-Tier2 hours	Includes Electives
OS/ Overview of OS	1*		
OS/OS Principles	1*		
OS/Concurrency		3	
OS/Scheduling and Dispatch		3	
OS/Memory Management		1*	
OS/Security and Protection		2	
OS/Virtual Machines			Y
OS/Device Management			Y
OS/File Systems			Y
OS/Real Time and Embedded Systems			Y

OS/Fault Tolerance			**Y**
OS/System Performance Evaluation			**Y**
NC/Introduction	**1.5**		
NC/Networked Applications	**1.5**		
NC/Reliable Data Delivery		**2**	
NC/Routing and Forwarding		**1.5**	
NC/Local Area Networks		**1.5**	
NC/Resource Allocation		**1**	
NC/Mobility		**1**	
PBD/Web Platforms			**Y**
PBD/Mobile Platforms			**Y**
PBD/Industrial Platforms			**Y**
IM/Information Management Concepts		**2**	
IM/Transaction Processing			**Y**
IM/Distributed Databases			**Y**
PL/Functional Programming		**2**	
PL/Type Systems	**1**	**4**	
PL/Language Translation And Execution	**1**	**3**	
PD/Parallelism Fundamentals	**1***		**Y**
PD/Communication and Coordination	**1**	**3**	
SDF/Development Methods	**9**		

SE/Software Processes	**1**		
SE/Software Project Management		**3**	
SE/Tools and Environments		**1**	
SE/Software Construction		**2**	**Y**
SE/Software Verification Validation		**3**	**Y**
SP/Professional Ethics	**2**	**1**	
SP/Intellectual Property	**2**		
SP/Security Policies, Laws and Computer Crimes			**Y**
HCI/Human factors and security			**Y**
IS/Reasoning Under Uncertainty			**Y**

* Indicates not all hours in the KU are classified as cross referenced to IAS

IAS/Fundamental Concepts

[1 Core-Tier1 hours, 2 Core-Tier2 hours]

Topics:

[Core-Tier1]

- Nature of the Threats
- Need for Information Assurance.
- Basic Terminology that should be recognized by those studying the field. (Confidentiality, Integrity, Availability)
- Information Assurance Concepts that are key to building an understanding of the IA area.

[Core-Tier2]

- Industry and Government Guidelines and Standards concerning Information Assurance.
- National and Cultural Differences including topics such as HIPAA, Safe Harbor, and data protection laws.
- Legal, Ethical, and Social Issues (cross reference with SP KA)
- Threats and Vulnerabilities.
- Types of Attacks
- Types of Attackers.
- Defense Mechanisms.
- Incident Response.

Learning outcomes:

1. Describe the types of threats to data and information systems [Knowledge]
2. Describe why processes and data need protection [Knowledge]
3. Describe the context in which Confidentiality, Integrity, and Availability are important to given processes or data? [Application]
4. Determine if the security controls provide sufficient security for the required level of Confidentiality, Integrity, and/or Availability [Evaluation]
5. What are significant national level laws affecting the obligation for the protection of data? [Knowledge]
6. Describe how laws affecting privacy and data/IP protection differ based on country? [Evaluation]
7. Describe the major vulnerabilities present in systems today. [Knowledge]
8. Define the fundamental motivations for intentional malicious exploitation of vulnerabilities. [Knowledge]
9. Define the defense mechanisms that can be used to detect or mitigate malicious activity in IT systems. [Knowledge]
10. Define an incident. [Knowledge]
11. Enumerate the roles required in incident response and the common steps after an incident has been declared. [Knowledge]
12. Describe the actions taken in response to the discovery of a given incident. [Application]

IAS/Network Security

[1 Core-Tier1 hours, 4 Core-Tier2 hours]

Discussion of network security relies on previous understanding on fundamental concepts of networking, including protocols, such as TCP/IP, and network architecture/organization (xref NC/Network Communication).

Topics:

[Core-Tier1]

- Application of Cryptography
- TLS
- Secret-key algorithms
- Public-key algorithms
- Hybrid

[Core-Tier2]

- Network attack types: Denial of service, flooding, sniffing and traffic redirection, message integrity attacks,
- Identity hijacking, exploit attacks (buffer overruns, Trojans, backdoors), inside attacks, infrastructure (DNS hijacking, route blackholing, misbehaving routers that drop traffic), etc.)
- Authentication protocols
- Digital signatures
- Message Digest
- Defense Mechanisms /Countermeasures. (Intrusion Detection, Firewalls, Detection of malware, IPSec, Virtual Private Networks, Network Address Translation.)
- Network Auditing.

Learning outcomes:

1. Identify protocols used to enhance Internet communication, and choose the appropriate protocol for a particular [Knowledge]
2. Discuss the difference between secret key and public key encryption. [Knowledge]
3. Discuss the fundamental ideas of public-key cryptography. [Knowledge]

4. Discuss the role of a certificate authority in public-key cryptography. [Knowledge]
5. Discuss non-repudiation [Knowledge]
6. Describe a digital signature[Knowledge]
7. Describe how public key encryption is used to encrypt email traffic. [Knowledge]
8. Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message. [Application]
9. Describe how public key encryption is used to secure HTTP traffic. [Knowledge]
10. Describe the security risks present in networking. [Knowledge]
11. Discuss the differences in Network Intrusion Detection and Network Intrusion Prevention. [Knowledge]
12. Describe how the basic security implications of a hub and a switch. [Knowledge]
13. Describe how a system can intercept traffic in a local subnet. [Knowledge]
14. Describe different implementations for intrusion detection. [Knowledge]
15. Identify a buffer overflow vulnerability in code [Evaluation]
16. Correct a buffer overflow error in code [Application]
17. Describe the methods that can be used to alert that a system has a backdoor installed. [Knowledge]
18. Describe the methods that can be used to identify a system is running processes not desired be the system owner. [Knowledge]
19. Analyze a port listing for unwanted TCP/UDP listeners. [Application]
20. Describe the difference between non-routable and routable IP addresses. [Knowledge]
21. List the class A, B, and C non-routable IP ranges. [Knowledge]
22. Describe the difference between stateful and non-stateful firewalls. [Knowledge]
23. Implement firewalls to prevent specific IP's or ports from traversing the firewall. [Application]
24. Describe the different actions a firewall can take with a packet. [Knowledge]
25. Summarize common authentication protocols. [Knowledge]
26. Describe and discuss recent successful security attacks. [Knowledge]
27. Summarize the strengths and weaknesses associated with different approaches to security. [Knowledge]
28. Describe what a message digest is and how it is commonly used. [Knowledge]

IAS/ Cryptography

[Elective]

Topics:

- The Basic Cryptography Terminology covers notions pertaining to the different (communication) partners, secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their characteristics, signatures, etc.
- Cipher types:, Caesar cipher, affine cipher, etc. together with typical attack methods such as frequency analysis, etc.
- Mathematical Preliminaries; include topics in linear algebra, number theory, probability theory, and statistics. (Discrete Structures)
- Cryptographic Primitives include encryption (stream ciphers, block ciphers public key encryption), digital signatures, message authentication codes, and hash functions.
- Cryptanalysis covers the state-of-the-art methods including differential cryptanalysis, linear cryptanalysis, factoring, solving discrete logarithm problem, lattice based methods, etc.
- Cryptographic Algorithm Design covers principles that govern the design of the various cryptographic primitives, especially block ciphers and hash functions. (Algorithms and Complexity - Hash functions)
- The treatment of Common Protocols includes (but should not be limited to) current protocols such as RSA, DES, DSA, AES, ElGamal, MD5, SHA-1, Diffie-Hellman Key exchange, identification and authentication protocols, secret sharing, multi-party computation, etc.
- Public Key Infrastructure deals with challenges, opportunities, local infrastructures, and national infrastructure.

Learning outcomes:

1. What is the purpose of Cryptography? [Knowledge]
2. What is plain text? [Knowledge]
3. What is cipher text? [Knowledge]
4. What are the two basic methods (ciphers) for transforming plain text in cipher text? [Knowledge]
5. Describe attacks against a specified cypher. [Knowledge]
6. Define the following terms: Cipher, Cryptanalysis, Cryptographic Algorithm, Cryptology. [Knowledge]
7. What is the Work Function of a given cryptographic algorithm? [Knowledge]
8. What is a One Time Pad (Vernam Cipher)? [Knowledge]
9. What is a Symmetric Key operation? [Knowledge]
10. What is an Asymmetric Key operation? [Knowledge]
11. For a given problem and environment weigh the tradeoffs between a Symmetric and Asymmetric key operation. [Evaluation]
12. What are common Symmetric Key algorithms? [Knowledge]
13. Explain in general how a public key algorithm works. [Knowledge]
14. How does "key recovery" work? [Knowledge]
15. List 5 public key algorithms. [Knowledge]
16. Describe the process in the Diffie-Hellman key exchange. [Knowledge]
17. What is a message digest and list 4 common algorithms? [Knowledge]
18. What is a digital signature and how is one created? [Knowledge]
19. What the three components of a PKI? [Knowledge]
20. List the ways a PKI infrastructure can be attacked. [Knowledge]

IAS/Risk Management

[Elective]

Topics:

- Risk Analysis involves identifying the assets, probable threats, vulnerabilities and control measures to discern risk levels and likelihoods. It can be applied to a program, organization, sector, etc. Knowledge in this area includes knowing different risk analysis models and methods, their strengths and benefits and the apropriateness of the different methods and models given the situation. This includes periodic reassessment.
- Cost/Benefit Analysis is used to weigh private and/or public costs versus benefits and can be applied to security policies, investments, programs, tools, deployments, etc.
- Continuity Planning will help organizations deliver critical services and ensure survival.
- Disaster Recovery will help an organization continue normal operations in a minimum amount of time with a minimum amount of disruption and cost.
- Security Auditing: a systematic assessment of an organization's system measuring the conformity vis-àvis a set of pre-established criteria.
- Asset Management minimizes the life cost of assets and includes critical factors such as risk or business continuity.
- Risk communication Enforcement of risk management policies is critical for an organization.

Learning outcomes:

1. How is risk determined? [Knowledge]
2. What does it mean to manage risk? [Knowledge]
3. What is the primary purpose of risk management? [Knowledge]
4. Who can accept Risk? [Knowledge]
5. What is the objective of Security Controls in security management? [Knowledge]
6. With respect to a risk program, what is an Asset? [Knowledge]
7. With respect to a risk program, what is a Threat? [Knowledge]
8. With respect to a risk program, what is a Vulnerability? [Knowledge]
9. With respect to a risk program, what is a Safeguard? [Knowledge]

10. With respect to a risk program, what is the Exposure Factor (EF)? [Knowledge]
11. What is the difference between Quantitative Risk Analysis and Qualitative Risk Analysis? [Knowledge]
12. How does an organization determine what safeguards or controls to implement? [Knowledge]
13. Given the value of an asset and the cost of the security controls to mitigate loss/damage/destruction, is the security plan appropriate? [Evaluation]
14. What is Risk Analysis (RA)? [Knowledge]
15. Describe how data is classified in either (government or commercial)? [Knowledge]
16. When are the factors used when determining the classification of a piece of information? [Knowledge]
17. What are three ways to deal with Risk? [Knowledge]

IAS/Security Policy and Governance

[Elective]

Topics:

- Strategies and Plans for creating security policies.
- Policies, Guidelines, Standards and Best Practices for individuals or organizations, including national security policies.
- Procedures for creating policies, guidelines, standards, specifications, regulations and laws.
- Privacy Policies to help protect personal and other sensitive information.
- Compliance and Enforcement of policies, standards, regulations, and laws.
- Formal Policy Models such as Bell-LaPadula, Biba and Clark-Wilson, which provide precise specifications of security objectives.
- Relation of national security policies, regulations, organizational security policies, formal policy models, and policy languages.
- Policy as related to Risk Aversion.

Learning outcomes:

1. What is a security policy and why does an organization need a security policy? [Knowledge]
2. Come up with an example of your own, which would be caused by missing security policies.[Application]
3. What are the basic things that need to be explained to every employee about a security policy? At what point in their employment? Why? [Application]
4. Say you have an e-mail server that processes sensitive emails from important people. What kind of things should be put into the security policy for the email server? [Evaluation]
5. Read your institution's security plan and critique the plan. [Evaluation]
6. Update your institution's security plan. [Evaluation]

IAS/ Digital Forensics

[Elective]

Topics:

- Basic Principles and methodologies for digital forensics.
- Rules of Evidence – general concepts and differences between jurisdictions and Chain of Custody.
- Search and Seizure of evidence, e.g., computers, including search warrant issues.
- Digital Evidence methods and standards.
- Techniques and standards for Preservation of Data.
- Data analysis and validation.
- Legal and Reporting Issues including working as an expert witness.

- OS/File System Forensics
- Application Forensics
- Network Forensics
- Mobile Device Forensics
- Computer/network/system attacks.

Learning outcomes:

1. What is a Digital Investigation? [Knowledge]
2. What systems in an IT infrastructure might have forensically recoverable data? [Knowledge]
3. Who in an organization is authorized to permit the conduct of a forensics investigation? [Knowledge]
4. What is the Rule of Evidence? [Knowledge]
5. What is a Chain of Custody? [Knowledge]
6. Conduct a data collection on a hard drive. [Application]
7. Validate the integrity of a digital forensics data set. [Application]
8. Determine if a digital investigation is sound. [Evaluation]
9. Describe the file system structure for a given device (NTFA, MFS, iNode, HFS…) [Knowledge]
10. Determine if a certain string of data exists on a hard drive. [Application]
11. Describe the capture of live data for a forensics investigation. [Knowledge]
12. Capture and interpret network traffic. [Application]
13. Discuss identity management and its role in access control systems. [Knowledge]
14. Determine what user was logged onto a given system at a given time. [Application]
15. Determine the submissability (from a legal perspective) of data. [Evaluation]
16. Evaluate a system for the presence of malware. [Evaluation]

IAS/Security Architecture and Systems Administration

[Elective]

Topics:

- How to secure Hardware, including how to make hardware tokens and chip cards tamper-proof and tamper-resistance.
- Configuring systems to operate securely as an IT system.
- Access Control
- Basic Principles of an access control system prevent unauthorized access.
- Physical Access Control determines who is allowed to enter or exit, where the user is allowed to enter or exit, and when the user is allowed to enter or exit.
- Technical/System Access Control is the process of preventing unauthorized users or services to utilize information systems.
- Usability includes the difficulty for humans to deal with security (e.g., remembering PINs), social engineering, phishing, and other similar attacks.
- Analyzing and identifying System Threats and Vulnerabilities
- Investigating Operating Systems Security for various systems.
- Multi-level/Multi-lateral Security
- Design and Testing for architectures and systems of different scale
- Penetration testing in the system setting
- Products available in the marketplace
- Supervisory Control and Data Acquisition (SCADA)
- SCADA system uses. Communications protocols supporting data acquisition
- Communications protocols supporting distributed control.
- Data Integrity
- Data Confidentiality

Learning outcomes:

1. Explain the need for software security and how software security is different from security features like access control or cryptography. [Knowledge]
2. Understand common threats to web applications and common vulnerabilities written by developers. [Knowledge]
3. Define least privilege. [Knowledge]
4. Define “Defense in Depth”. [Knowledge]
5. Define service isolation in the context of enterprise systems. [Knowledge]
6. Architect an enterprise system using the concept of service isolation. [Application]
7. Describe the methods to provide for access control and what enterprise services must exist. [Knowledge]
8. Discuss how user systems integrate into an enterprise environment. [Knowledge]
9. Discuss the risks client systems pose to an enterprise environment. [Knowledge]
10. Describe various methods to manage client systems. [Knowledge]
11. Create a risk model of a web application, ranking and detailing the risks to the system’s assets. [Application]
12. Construct, document, and analyze security requirements with abuse cases and constraints. [Application]
13. Apply secure design principles, such as least privilege, to the design of a web application. [Application]
14. Validate both the input and output of a web application. [Application]
15. Use cryptography appropriately, including SSL and certificate management. [Application]
16. Create a test plan and conduct thorough testing of web applications with appropriate software assistance. [Application]

IAS/Secure Software Design and Engineering

[Elective]

Fundamentals of secure coding practices covered in other knowledge areas, including SDF/SE/PL.

Topics:

- Building security into the Software Development Lifecycle
- Secure Design Principles and Patterns (Saltzer and Schroeder, etc)
- Secure Software Specification and Requirements deals with specifying what the program should and should not do, which can be done either using a requirements document or using a more formal mathematical specification.
- Secure Coding involves applying the correct balance of theory and practice to minimize vulnerabilities in code.
- Data validation
- Memory handling
- Crypto implementation
- Secure Testing is the process of testing that security requirements are met (including Static and Dynamic analysis).
- Program Verification and Simulation is the process of ensuring that a certain version of a certain implementation meets the required security goals, either by a mathematical proof or by simulation.

Learning outcomes:

1. Describe the Design Principles for Protection Mechanisms (Saltzer and Schroeder) [Knowledge]
2. Describe the Principles for Software Security (Viega and McGraw) [Knowledge]
3. Define Principles for a Secure Design (Morrie Gasser) [Knowledge]
4. Compare the principles for software and systems in the context of a software development effort. [Application]
5. Discuss the benefits and drawbacks of open-source vs proprietary software and security [Knowledge]
6. Integrate trustworthy development practices into an existing software development lifecycle [Application]
7. Integrate authenticating libraries, DLL, run-time [Application]
8. Identify a buffer overflow in a code sample [Knowledge]
9. Describe the difference between static and dynamic analysis. [Knowledge]
10. Conduct static analysis to determine the security posture of a given application. [Application]
11. Monitor the execution of a software (dynamic analysis) and discuss the observed process flows. [Application]
12. How is quality assurance conducted for software development? [Knowledge]
13. Participate in a code review focused on finding security bugs using static analysis tools. [Application]
14. Where does patch management fit in a software development project? [Knowledge]