

Software Assurance Additions to the Core Knowledge Areas

General Model (Framework)

Knowledge Area	Tier1	Tier2	Core	Core
AL- Algorithms and Complexity	19	9	31	31
AR- Architecture and Organization	0	16	36	36
CN- Computational Science	1	0	0	0
DS-Discrete Structures	37	4	43	43
GV-Graphics and Visual Computing	2	1	3	3
HC-Human-Computer Interaction	4	4	8	8
IAS-Security and Information Assurance	2	6	--	--
IM- Information Management	1	9	11	10
IS-Intelligent Systems	0	10	10	10
NC- Networking and Communication	3	7	15	15
OS-Operating Systems	4	11	18	18
PBD- Platform-based Development	0	0	--	--
PD-Parallel	5	10	--	--

and Distributed Computing PL- Programming Languages	8	20	21	21
SDF- Software Development Fundamentals	42	0	47	38
SE-Software Engineering SF-Systems Fundamentals	6	21	31	31
SP-Social and Professional Issues	18	9	--	--
SP-Social and Professional Issues	11	5	16	16
Total Core Hours	163	142	290	280
All Tier1 + All Tier2 Total			305	
All Tier1 + 90% of Tier2 Total			290.8	
All Tier1 + 80% of Tier2 Total			276.6	

Area - Human-Computer Interaction (HC) 1

Human-computer interaction (HCI) is concerned with designing the interaction between people 2 and computers and the construction of interfaces to afford this interaction. 3 Interaction between users and computational artifacts occurs at an interface which includes both 4 software and hardware. Interface design impacts the software life-cycle in that it should occur 5 early; the design and implementation of core functionality can influence the user interface – for 6 better or worse. 7 Because it deals with people as well as computers, as a knowledge area HCI draws on a variety 8 of disciplinary traditions including psychology, computer science, product design, anthropology 9 and engineering.

Course - HC/Human factors and security 185

[Elective] 186

Motivation: Effective interface design requires basic knowledge of security psychology. Many 187 attacks do not have a technological basis, but exploit human propensities and vulnerabilities. 188 “Only amateurs attack machines; professionals target people” (Bruce Schneier) 189 **Topics:** 190

- Applied psychology and security policies 191
- Security economics 192
- Regulatory environments – responsibility, liability and self-determination 193
- Organizational vulnerabilities and threats 194
- Usability design and security 195
- Pretext, impersonation and fraud. Phishing and spear phishing (cross reference IAS/Fundamentals) 196
- Trust, privacy and deception 197
- Biometric authentication (camera, voice) 198

- Identity management 199

200 **Learning Outcomes:** 201 Students should be able to apply the principles of HCI foundations to: 202

1. Explain the concepts of phishing and spear phishing, and how to recognize them (knowledge) 203
2. Explain the concept of identity management and its importance (knowledge) 204
3. Describe the issues of trust in interface design with an example of a high and low trust system (knowledge) 205
4. Design a user interface for a security mechanism (application) 206
5. Analyze a security policy and/or procedures to show where they consider, or fail to consider, human factors 207 (comprehension) 208

Area - Information Assurance and Security (IAS) 1

In CS2013, the Information Assurance and Security KA is added to the Body of Knowledge in 2 recognition of the world's reliance on information technology and its critical role in computer 3 science education. Information assurance and security as a domain is the set of controls and 4 processes both technical and policy intended to protect and defend information and information 5 systems by ensuring their availability, integrity, authentication, and confidentiality and providing 6 for non-repudiation. The concept of assurance also carries an attestation that current and past 7 processes and data are valid. Both assurance and security concepts are needed to ensure a 8 complete perspective. Information assurance and security education, then, includes all efforts to 9 prepare a workforce with the needed knowledge, skills, and abilities to protect our information 10 systems and attest to the assurance of the past and current state of processes and data. The 11 Information Assurance and Security KA is unique among the set of KA's presented here given 12 the manner in which the topics are pervasive throughout other Knowledge Areas. The topics 13 germane to only IAS are presented in depth in the IAS section; other topics are noted and cross 14 referenced in the IAS KA, with the details presented in the KA in which they are tightly 15 integrated. 16 The aim of this KA is two-fold. First, the KA defines the core (tier1and tier2) and the elective 17 components that depict topics that are part of an undergraduate computer science curriculum. 18 Secondly (and almost more importantly), we document the pervasive presence of IAS within a 19 computer science undergraduate curriculum. 20 The IAS KA is shown in two groups; (1) concepts that are, at the first order, germane to 21 Information Assurance and Security and (2) IAS topics that are integrated into other KA's. For 22 completeness, the total distribution of hours is summarized in the table below.

IAS. Information Assurance and Security (2 Core-Tier1 hours, 6 Core-Tier2 hours) 26	Core-Tier2 hours	Includes Electives
Core-Tier1 hours		
IAS/Fundamental Concepts	1	2
IAS/Network Security	1	4
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
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	1	3
Translation And Execution		
PD/Parallelism	1*	Y
Fundamentals		
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	
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	

4. Discuss the role of a certificate authority in public-key cryptography. [Knowledge] 99
5. Discuss non-repudiation [Knowledge] 100
6. Describe a digital signature [Knowledge] 101
7. Describe how public key encryption is used to encrypt email traffic. [Knowledge] 102
8. Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message. 103 [Application] 104
9. Describe how public key encryption is used to secure HTTP traffic. [Knowledge] 105
10. Describe the security risks present in networking. [Knowledge] 106
11. Discuss the differences in Network Intrusion Detection and Network Intrusion Prevention. [Knowledge] 107
12. Describe how the basic security implications of a hub and a switch. [Knowledge] 108
13. Describe how a system can intercept traffic in a local subnet. [Knowledge] 109
14. Describe different implementations for intrusion detection. [Knowledge] 110
15. Identify a buffer overflow vulnerability in code [Evaluation] 111
16. Correct a buffer overflow error in code [Application] 112
17. Describe the methods that can be used to alert that a system has a backdoor installed. [Knowledge] 113
18. Describe the methods that can be used to identify a system is running processes not desired by the system owner. [Knowledge] 115
19. Analyze a port listing for unwanted TCP/UDP listeners. [Application] 116
20. Describe the difference between non-routable and routable IP addresses. [Knowledge] 117
21. List the class A, B, and C non-routable IP ranges. [Knowledge] 118
22. Describe the difference between stateful and non-stateful firewalls. [Knowledge] 119
23. Implement firewalls to prevent specific IP's or ports from traversing the firewall. [Application] 120
24. Describe the different actions a firewall can take with a packet. [Knowledge] 121
25. Summarize common authentication protocols. [Knowledge] 122
26. Describe and discuss recent successful security attacks. [Knowledge] 123
27. Summarize the strengths and weaknesses associated with different approaches to security. [Knowledge] 124
28. Describe what a message digest is and how it is commonly used. [Knowledge] 125

Course - IAS/ Cryptography 127

[Elective] 128

Topics: 129

- The Basic Cryptography Terminology covers notions pertaining to the different (communication) partners, 130 secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their 131 characteristics, signatures, etc. 132
- Cipher types:, Caesar cipher, affine cipher, etc. together with typical attack methods such as frequency 133 analysis, etc. 134
- Mathematical Preliminaries; include topics in linear algebra, number theory, probability theory, and 135 statistics. (Discrete Structures) 136
- Cryptographic Primitives include encryption (stream ciphers, block ciphers public key encryption), digital 137 signatures, message authentication codes, and hash functions. 138
- Cryptanalysis covers the state-of-the-art methods including differential cryptanalysis, linear cryptanalysis, 139 factoring, solving discrete logarithm problem, lattice based methods, etc. 140

- Cryptographic Algorithm Design covers principles that govern the design of the various cryptographic 141 primitives, especially block ciphers and hash functions. (Algorithms and Complexity - Hash functions) 142
- The treatment of Common Protocols includes (but should not be limited to) current protocols such as RSA, 143 DES, DSA, AES, ElGamal, MD5, SHA-1, Diffie-Hellman Key exchange, identification and authentication 144 protocols, secret sharing, multi-party computation, etc. 145
- Public Key Infrastructure deals with challenges, opportunities, local infrastructures, and national 146 infrastructure. 147

3. Discuss the fundamental ideas of public-key cryptography. [Knowledge] 98
4. Discuss the role of a certificate authority in public-key cryptography. [Knowledge] 99
5. Discuss non-repudiation [Knowledge] 100
6. Describe a digital signature [Knowledge] 101
7. Describe how public key encryption is used to encrypt email traffic. [Knowledge] 102
8. Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message. 103 [Application] 104
9. Describe how public key encryption is used to secure HTTP traffic. [Knowledge] 105
10. Describe the security risks present in networking. [Knowledge] 106
11. Discuss the differences in Network Intrusion Detection and Network Intrusion Prevention. [Knowledge] 107
12. Describe how the basic security implications of a hub and a switch. [Knowledge] 108
13. Describe how a system can intercept traffic in a local subnet. [Knowledge] 109
14. Describe different implementations for intrusion detection. [Knowledge] 110
15. Identify a buffer overflow vulnerability in code [Evaluation] 111
16. Correct a buffer overflow error in code [Application] 112
17. Describe the methods that can be used to alert that a system has a backdoor installed. [Knowledge] 113
18. Describe the methods that can be used to identify a system is running processes not desired by the system 114 owner. [Knowledge] 115
19. Analyze a port listing for unwanted TCP/UDP listeners. [Application] 116
20. Describe the difference between non-routable and routable IP addresses. [Knowledge] 117
21. List the class A, B, and C non-routable IP ranges. [Knowledge] 118
22. Describe the difference between stateful and non-stateful firewalls. [Knowledge] 119
23. Implement firewalls to prevent specific IP's or ports from traversing the firewall. [Application] 120
24. Describe the different actions a firewall can take with a packet. [Knowledge] 121
25. Summarize common authentication protocols. [Knowledge] 122
26. Describe and discuss recent successful security attacks. [Knowledge] 123
27. Summarize the strengths and weaknesses associated with different approaches to security. [Knowledge] 124
28. Describe what a message digest is and how it is commonly used. [Knowledge] 125

2. What is plain text? [Knowledge] 151
3. What is cipher text? [Knowledge] 152
4. What are the two basic methods (ciphers) for transforming plain text in cipher text? [Knowledge] 153
5. Describe attacks against a specified cypher. [Knowledge] 154
6. Define the following terms: Cipher, Cryptanalysis, Cryptographic Algorithm, Cryptology. [Knowledge] 155
7. What is the Work Function of a given cryptographic algorithm? [Knowledge] 156

8. What is a One Time Pad (Verna Cipher)? [Knowledge] 157
9. What is a Symmetric Key operation? [Knowledge] 158
10. What is an Asymmetric Key operation? [Knowledge] 159
11. For a given problem and environment weigh the tradeoffs between a Symmetric and Asymmetric key 160 operation. [Evaluation] 161
12. What are common Symmetric Key algorithms? [Knowledge] 162
13. Explain in general how a public key algorithm works. [Knowledge] 163
14. How does "key recovery" work? [Knowledge] 164
15. List 5 public key algorithms. [Knowledge] 165
16. Describe the process in the Diffie-Hellman key exchange. [Knowledge] 166
17. What is a message digest and list 4 common algorithms? [Knowledge] 167
18. What is a digital signature and how is one created? [Knowledge] 168
19. What the three components of a PKI? [Knowledge] 169
20. List the ways a PKI infrastructure can be attacked. [Knowledge] 170

Course - IAS/Risk Management 172

[Elective] 173

Topics: 174

- Risk Analysis involves identifying the assets, probable threats, vulnerabilities and control measures to 175 discern risk levels and likelihoods. It can be applied to a program, organization, sector, etc. Knowledge in 176 this area includes knowing different risk analysis models and methods, their strengths and benefits and the 177 appropriateness of the different methods and models given the situation. This includes periodic 178 reassessment. 179
- Cost/Benefit Analysis is used to weigh private and/or public costs versus benefits and can be applied to 180 security policies, investments, programs, tools, deployments, etc. 181
- Continuity Planning will help organizations deliver critical services and ensure survival. 182
- Disaster Recovery will help an organization continue normal operations in a minimum amount of time with 183 a minimum amount of disruption and cost. 184
- Security Auditing: a systematic assessment of an organization's system measuring the conformity vis-à-vis a 185 set of pre-established criteria. 186
- Asset Management minimizes the life cost of assets and includes critical factors such as risk or business 187 continuity. 188
- Risk communication Enforcement of risk management policies is critical for an organization. 189

190 **Learning outcomes:** 191

1. How is risk determined? [Knowledge] 192
 2. What does it mean to manage risk? [Knowledge] 193
 3. What is the primary purpose of risk management? [Knowledge] 194
 4. Who can accept Risk? [Knowledge] 195
 5. What is the objective of Security Controls in security management? [Knowledge] 196
 6. With respect to a risk program, what is an Asset? [Knowledge] 197
 7. With respect to a risk program, what is a Threat? [Knowledge]
- Data analysis and validation. 245
 - Legal and Reporting Issues including working as an expert witness. 246
 - OS/File System Forensics 247
 - Application Forensics 248

- Network Forensics 249
- Mobile Device Forensics 250
- Computer/network/system attacks. 251

252 **Learning outcomes:** 253

1. What is a Digital Investigation? [Knowledge] 254
2. What systems in an IT infrastructure might have forensically recoverable data? [Knowledge] 255
3. Who in an organization is authorized to permit the conduct of a forensics investigation? [Knowledge] 256
4. What is the Rule of Evidence? [Knowledge] 257
5. What is a Chain of Custody? [Knowledge] 258
6. Conduct a data collection on a hard drive. [Application] 259
7. Validate the integrity of a digital forensics data set. [Application] 260
8. Determine if a digital investigation is sound. [Evaluation] 261
9. Describe the file system structure for a given device (NTFA, MFS, anode, HFS...) [Knowledge] 262
10. Determine if a certain string of data exists on a hard drive. [Application] 263
11. Describe the capture of live data for a forensics investigation. [Knowledge] 264
12. Capture and interpret network traffic. [Application] 265
13. Discuss identity management and its role in access control systems. [Knowledge] 266
14. Determine what user was logged onto a given system at a given time. [Application] 267
15. Determine the submissability (from a legal perspective) of data. [Evaluation] 268
16. Evaluate a system for the presence of malware. [Evaluation]

Course - IAS/Security Architecture and Systems Administration 272
[Elective] 273

Topics: 274

- How to secure Hardware, including how to make hardware tokens and chip cards tamper-proof and tamper-275 resistance. 276
- Configuring systems to operate securely as an IT system. 277
- Access Control 278
- Basic Principles of an access control system prevent unauthorized access. 279
- Physical Access Control determines who is allowed to enter or exit, where the user is allowed to enter or 280 exit, and when the user is allowed to enter or exit. 281
- Technical/System Access Control is the process of preventing unauthorized users or services to utilize 282 information systems. 283
- Usability includes the difficulty for humans to deal with security (e.g., remembering PINs), social 284 engineering, phishing, and other similar attacks. 285
- Analyzing and identifying System Threats and Vulnerabilities 286
- Investigating Operating Systems Security for various systems. 287
- Multi-level/Multi-lateral Security 288
- Design and Testing for architectures and systems of different scale 289
- Penetration testing in the system setting 290
- Products available in the marketplace 291
- Supervisory Control and Data Acquisition (SCADA) 292
- SCADA system uses. Communications protocols supporting data acquisition 293
- Communications protocols supporting distributed control. 294
- Data Integrity 295

- Data Confidentiality 296

1. Explain the need for software security and how software security is different from security features like 299 access control or cryptography. [Knowledge] 300
2. Understand common threats to web applications and common vulnerabilities written by developers. 301 [Knowledge] 302
3. Define least privilege. [Knowledge] 303
4. Define “Defense in Depth”. [Knowledge] 304
5. Define service isolation in the context of enterprise systems. [Knowledge] 305
6. Architect an enterprise system using the concept of service isolation. [Application] 306
7. Describe the methods to provide for access control and what enterprise services must exist. [Knowledge] 307
8. Discuss how user systems integrate into an enterprise environment. [Knowledge] 308
9. Discuss the risks client systems pose to an enterprise environment. [Knowledge] 309
10. Describe various methods to manage client systems. [Knowledge] 310
11. Create a risk model of a web application, ranking and detailing the risks to the system’s assets. 311 [Application] 312
12. Construct, document, and analyze security requirements with abuse cases and constraints. [Application] 313
13. Apply secure design principles, such as least privilege, to the design of a web application. [Application] 314
14. Validate both the input and output of a web application. [Application] 315
15. Use cryptography appropriately, including SSL and certificate management. [Application] 316
16. Create a test plan and conduct thorough testing of web applications with appropriate software assistance. 317 [Application]