Cybersecurity Principles

Domain Scope [40 hours]

1. Identification of policies, mechanisms, services, and countermeasures related to cybersecurity
2. Cyber-attacks, cyber-detection, services and operational issues, security mechanisms and detection
3. Vulnerabilities, threats, concealment, cyphers and deciphers, encryption, and decryption
4. Malware operations, mitigation, and recovery
5. Data and information security, security breaches, and reporting requirements

Cybersecurity Principles Subdomains

01 History and overview
Minimum instructional hours: 1 hour
Competencies:

a. Identify significant continuing trends in the history of cybersecurity.
b. Identify two significant cybersecurity events since 1980.
c. Discuss the historical context for today's cybersecurity problems.

d. Discuss the role of mediation and the principle of complete mediation.
e. Discuss the concept of defense in depth, i.e. having multiple layers of defenses.
f. Identify a risk management framework that is in use today.

g. Discuss security issues that arise at boundaries between multiple components.
h. Define the roles of prevention, deterrence, and detection mechanisms.
i. Discuss the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
j. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
k. Describe commercial approaches to delivering high-assurance services, including SE Linux, Security Enhanced Hypervisors, role-based access systems, and digital signatures applied to code and data.
l. Summarize the principle of fail-safe and deny-by-default.
m. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
n. Discuss the role of Trusted Platform Modules (TPMs) in creating high assurance software and systems.
o. Discuss the role of Trusted Platform Modules (TPMs) in creating high assurance systems.

02 Policy goals and mechanisms
Minimum instructional hours: 2 hours
Competencies:

a. Identify governance structures through which cybersecurity policy goals are created and promulgated.
b. Provide three multiple definitions for the word “policy” within a cybersecurity context.
c. Identify current cybersecurity policy objectives and goals.
d. Discuss vulnerability notification and repair policies, important policy issues to consider in computer security, including issues 3051 associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities.
e. Discuss the implications of relying on open design or the secrecy of design for security.
f. Discuss why cybersecurity is a societal imperative.

g. Discuss the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability).
h. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security).
i. Define the concept of “countermeasures” and provide examples for specific threats.
j. Define the concept of “continuous monitoring” and provide examples.
k. Explain the concept of identity management and its importance.
l. Explain the concepts of authentication, authorization, and access control.
m. Explain the benefit of two-factor authentication, including the use of biometrics.

03 Security services, mechanisms and countermeasures
Minimum instructional hours: 4 hours
Competencies:

a. Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability).
b. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security).
c. Define the concept of “countermeasures” and provide examples for specific threats.
d. Define the concept of “continuous monitoring” and provide examples.
e. Explain the concept of identity management and its importance.
f. Explain the concepts of authentication, authorization, and access control.
g. Explain the benefit of two-factor authentication, including the use of biometrics.
h. Define application ’whitelisting’.
i. Identify the costs and tradeoffs associated with security that a company implements into a product.

04 Cyber-attacks and detection
Minimum instructional hours: 4 hours
Competencies:

a. Define the roles of prevention, deterrence, and detection mechanisms.
b. Identify password guessing, port scanning, SQL injection probes, and other cyberattacks in log files.
c. Discuss the role and limitations of signature-based and behavioral-based anti-virus technology.
d. Explain two differences between host-based and network-based intrusion detection systems.
e. Create three rules for a network-based intrusion detection system that will protect against specific known attacks.
f. Discuss the use of deception by malware to evade security mechanisms.

g. Demonstrate a cross-site scripting attack against a server that reads an unbounded data into a fixed-size data structure.
h. Demonstrate a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure.
i. Demonstrate a cross-site scripting attack against a server that does not properly sanitize user input prior to displaying the results in a browser.

05 High assurance systems
Minimum instructional hours: 4 hours
Competencies:

a. Explain the concept of trust and trustworthiness.
b. Describe the principle of least privilege and isolation as applied to system design.
c. Summarize the principle of fail-safe and deny-by-default.
d. Describe the concept of mediation and the principle of complete mediation.
e. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
f. Describe commercial approaches to delivering high-assurance services, including SE Linux, Security Enhanced Hypervisors, role-based access systems, and digital signatures applied to code and data.
g. Discuss the role of formal methods in creating high assurance software and systems.
h. Discuss the role of Trusted Platform Modules (TPMs) in creating high assurance systems.

06 Vulnerabilities, threats and risk
Minimum instructional hours: 5 hours
Competencies:

a. Explain the relationship between vulnerabilities, threats and risk.
b. Give two examples of how security mechanisms can contain vulnerabilities.
c. Identify a risk management framework that is in use today.
d. Identify the role of penetration testing; use penetration-testing tools to identify a vulnerability.
e. Discuss three benefits of defense in depth, i.e. having multiple layers of defenses.
f. Describe security issues that arise at boundaries between multiple components.
g. Determine if software installed on a server or network component is listed in the National Vulnerability Database.
h. Distinguish vulnerabilities, threats and risks that are distinct to network infrastructure, cloud computing servers, desktop computers, and mobile devices.
i. Demonstrate a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure.

07 Cybersecurity policy
Minimum instructional hours: 6 hours
Competencies:

a. Explain the concept of cybersecurity policy goals are created and promulgated.
b. Describe the principle of least privilege and isolation as applied to system design.
c. Summarize the principle of fail-safe and deny-by-default.
d. Describe the concept of mediation and the principle of complete mediation.
e. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
f. Describe commercial approaches to delivering high-assurance services, including SE Linux, Security Enhanced Hypervisors, role-based access systems, and digital signatures applied to code and data.
g. Discuss the role of formal methods in creating high assurance software and systems.
h. Discuss the role of Trusted Platform Modules (TPMs) in creating high assurance systems.

08 Cyber-attacks and detection
Minimum instructional hours: 4 hours
Competencies:

a. Define the roles of prevention, deterrence, and detection mechanisms.
b. Identify password guessing, port scanning, SQL injection probes, and other cyberattacks in log files.
c. Discuss the role and limitations of signature-based and behavioral-based anti-virus technology.
d. Explain two differences between host-based and network-based intrusion detection systems.
e. Create three rules for a network-based intrusion detection system that will protect against specific known attacks.
f. Discuss the use of deception by malware to evade security mechanisms.

g. Demonstrate a cross-site scripting attack against a server that reads an unbounded data into a fixed-size data structure.
h. Demonstrate a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure.
i. Demonstrate a cross-site scripting attack against a server that does not properly sanitize user input prior to displaying the results in a browser.
07 Anonymity systems
Minimum instructional hours: 2 hours
Competencies:
  a. Explain the relationship between vulnerabilities, threats and risk.
  b. Give two examples of how security mechanisms can contain vulnerabilities.
  c. Identify a risk management framework that is in use today.
  d. Identify the role of penetration testing; use penetration-testing tools to identify a vulnerability.
  e. Discuss three benefits of defense in depth, i.e. having multiple layers of defenses.
  f. Describe security issues that arise at boundaries between multiple components.
  g. Determine if software installed on a server or network component is listed in the National Vulnerability Database.
  h. Distinguish vulnerabilities, threats and risks that are distinct to network infrastructure, cloud computing servers, desktop computers, and mobile devices.
  i. Demonstrate a buffer-overflow attack against a server that reads an unbounded data into a fixed-size data structure.
  j. Demonstrate a cross-site scripting attack against a server that does not properly sanitize user input prior to displaying the results in a browser.

08 Usable security
Minimum instructional hours: 3 hours
Competencies:
  a. Discuss the concept of “psychological acceptability” and the importance of usability in security mechanism design.
  b. Describe the issues of trust in interface design with an example of a high and low trust system.
  c. Design a user interface for a security mechanism.
  d. Analyze a security policy and/or procedures to show where it considers, or fails to consider, human factors.
  e. Critique the ability of complex password policies to achieve the desired goal of preventing unauthorized access to sensitive systems.
  f. Discuss three difference between erasing pointers to information and overwriting the data contents, with application to file systems, databases, and cloud storage.
  g. Evaluate the effectiveness of an authentication mechanism from the perspective of a person who is visually impaired.

09 Cryptography overview
Minimum instructional hours: 3 hours
Competencies:
  a. Define the terms encryption, decryption, key, public key cryptography, symmetric cryptography, algorithm, key length, key escrow, key recover, key splitting, random number generator, nonce, initialization vector, cryptographic mode, plaintext, cipher text, S/MIME, PGP, 3151 IPsec, TLS.
  b. Identify the algorithms DES, 3DES, AES, MD5, SHA-1, SHA-2, SHA-3.
  c. Distinguish encryption, digital signatures, and hash functions.
  d. Compare encryption for data at rest and data in motion.
  e. Distinguish between block-level encryption, file-level encryption, and application-level encryption for encrypted storage.
  f. Describe why it is preferred to use validated, proven algorithms and implementations rather than developing new ones.

10 Malware fundamentals
Minimum instructional hours: 2 hours
Competencies:
  a. Define “malware” and distinguish the categories and uses of malware.
  b. Identify malware infection mechanisms, malware countermeasures (e.g., signature-based detection, behavioral detection).
  c. Identify appropriate locations within organizational information systems to provide protection from malware.
  d. Inspect a system (network, computer, or application) for the presence of malware.
  e. Identify two techniques for safely isolating malware samples from infected systems and classifying the sample.

11 Mitigation and recovery
Minimum instructional hours: 3 hours
Competencies:
  a. Discuss a risk mitigation and incident recovery plan.
  b. Identify the options for mitigating a malware infection on an enterprise client and an enterprise server.
  c. Describe the managerial and forensic steps for recovery after detecting a hostile insider.
  d. Contrast backup and recovery plans designed to protect against natural disasters from those designed to protect against hostile actors.
  e. List two examples of the steps taken after a credential is lost or compromised.
  f. Describe approaches for mitigating supply chain risks.

12 Personal information
Minimum instructional hours: 2 hours
Competencies:
  a. Define the terms Personal Information, Personally Identifiable Information, De-Identification, Anonymization, Pseudonym, Masking, Unmasking, Identifiable Information, De-Identification.
  b. Identify the Fair Information Practices.
  c. Classify two categories of personal information according to privacy and disclosure risk.
  d. Discuss two policies for collecting, processing, storing, sharing, and disposing of personal information.
  e. Discuss the role and limitations of encryption for protecting personal information.
  f. Discuss three policies and technologies for isolating personal data from enterprise data.
  g. Discuss two approaches for controlling access to personal information.
13 Operational issues
Minimum instructional hours: 4 hours
Competencies:
  a. Describe the steps for determining the exposure and planning recovery of a lost laptop and mobile device.
  b. Identify two standards that would apply to an organization’s information security posture.
  c. Evaluate potential vendors with respect to their security offerings.
  d. Track emerging threats, vulnerabilities and migrations.
  e. Develop a continuing education program.
  f. Discuss recruitment, retention and retaining of security personnel.

14 Reporting requirements
Minimum instructional hours: 1 hour
Competencies:
  a. Identify legal and regulatory requirements for sharing of threat and breach information.
  b. Contrast different vulnerability disclosure policies, including “full disclosure,” and “responsible disclosure.”
  c. Discuss the need and security advantages of security personnel sharing information about breaches with employees, and the need to balance employee notification with the need to maintain confidentiality during investigations.

BITM Outcomes for ITMS 448
Bachelor of Information Technology and Management graduates should be able to:
  (b) Analyze a problem and identify and define the computing requirements appropriate to its solution
  (c) Design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs
  (d) Function effectively on teams to accomplish a common goal
  (e) Recall and discuss professional, ethical, legal, security and social issues and responsibilities
  (f) Communicate effectively with a range of audiences
  (i) Use current techniques, skills, and tools necessary for computing practice
  (m) Describe and apply best practices and standards
  (n) Assist in the creation of an effective project plan

BITM Outcomes to be assessed in ITMS 448, Fall of 2016
Bachelor of Information Technology and Management graduates should be able to:
  (e) Recall and discuss professional, ethical, legal, security and social issues and responsibilities
  (f) Communicate effectively with a range of audiences
  (i) Use current techniques, skills, and tools necessary for computing practice