Information Technology Concepts

Module 3

Module Objectives

1. **Discuss the purpose and function of a computer**
2. Explain the components of a computer
3. **Discuss the various types of computers or computing devices**
4. **Discuss the notion of a virtual computer**
5. Discuss the concept and purpose of operating systems
6. **Discuss the lineage of popular operating system families**
7. **Discuss the concepts of "client" operating system and a "server" operating system and compare them**
8. **Discuss the common interaction mechanisms for OS use and administration**
9. Discuss the concept and purpose of applications
10. Discuss the concept of a standalone application and a client-server application and compare them
11. **Discuss the purpose and function of networking**
12. **Discuss the concept of connectivity in terms of wired and wireless networking**
13. **Discuss the concept and purpose of Personal Area, Local Area and Wide Area networking**
14. **Discuss the concept secure and non-secure networks**
15. **Discuss the history, structure and challenges of the Internet**
16. Discuss the concept and purpose of networking protocols
17. Discuss the concept and purpose of network services
18. Discuss the concept of data representation and abstraction
19. Discuss the purpose of the following data representations: binary, ASCII/Unicode, ASN.1, XML and file formats
20. **Discuss the purpose of cyber security**
21. Explain the concepts of: confidentiality, integrity, availability, trust, least privilege, need to know
22. **Explain the concepts and purpose of policy as an administrative control and as in context of technical controls (.e.g, device or domain policy)**
23. **Explore the concept and purpose of risk management**
24. ~~Explain the concept and purpose of control and the types (e.g. administrative, technical)~~

Revision:YYYYMMDD

25. **Explain the concepts and purpose of identity and authentication**.
26. Explore the concept, threats and purpose of password security
27. Explore the concept and basic function of multi-factor authentication techniques.
28. **Explore the concept and purpose of authorization**
29. **Explore the concept and purpose of accountability**
30. **Explore the states of information (i.e. "at rest", "in transit", "in process") and security considerations for these states**
31. Explore how complexity as opposed to simplicity affects security
32. Explore the basic functional elements of cryptography like: hashes, encryption, digital signatures and certificates
33. **Explore the information security management paradigm of "Prevent, Detect, Respond"**

Note: Objectives listed as bold are topics covered in video content and activities. The topics not in bold will be presented in supplemental materials.

Module Guidance

1. Video	Introduces the module and addresses module objectives 1, 3 and 4.	Duration: 5 minutes
2. Activity 1		Duration: 5 minutes - 2 Minutes for completion - 3 minutes for review
3. Video	Addresses module objectives 6, 7 and 8.	Duration: 5 minutes
4. Activity 2		Duration: 5 minutes - 2 Minutes for completion - 3 minutes for review
5. Video	Addresses module objectives 11, 12, 13, 14 and 15.	Duration: 5 minutes
6. Activity 3		Duration: 5 minutes
7. Class Review or Video Review	Reviewing the results of Activity 3	Duration: 5 – 10 minutes
8. Video	Addresses module objectives 20, 22 and 23. **Assumption**: Handouts 1, 2, 3, 5, 7 were read	Duration: 5 minutes

9. Activity 4		Duration: 5 minutes - 2 Minutes for completion - 3 minutes for review
10. Video	Addresses module objectives 25, 28 and 29. **Assumption**: Handouts 8, 9 and 10 were read	Duration: 5 minutes
11. Activity 5		Duration: 5 minutes - 2 Minutes for completion - 3 minutes for review
12. Video	Addresses module objectives 30, 33 **Assumption**: Handouts 11 and 12 were read	Duration: (5 – 10) minutes
13. Activity 6		Duration: 5 minutes
14. Class Review or Video Review	Reviewing the results of Activity 6	Duration: 5 – 10 minutes

Total time: ?? minutes

There is much more content in this module than can be accommodated in one IT-Club session. The first session is planned to end after item 7, Class Review or Video Review. This plan is only provided as a suggestion.

Supplemental Materials

1. Handout – Components of a computer
2. Handout – Operating Systems
3. Handout – Applications
4. Handout – Networking Protocols
5. Handout – Network Services
6. Handout – Data Representation
7. Handout – Security Concepts
8. Handout – Password Security – Threats and Protection Ideas
9. Handout – Multi-Factor Authentication Techniques
10. Handout – Complexity and its Effect on Security
11. Handout – Functional elements of cryptography

Module 3 – Objectives and Key Instruction Points

Objectives:
Teaching students to think like administrators instead of users. Their user experiences make for important context in which to ground administration lessons, but the goal is not treat them as end-users. There is only so much time to share the underpinnings of IT administration, so some things will have to left as a black box.

Video Segment 1 – Computers

1. Purpose and function of a computer
    a. History
    b. Why are computers necessary?
    c. What do computers do?
2. Computer components – Primarily a handout
    a. Minimal explanation of computer components
3. Computing devices – primary focus is on common IT devices
    a. Minimal reference to embedded and specialized computing devices
    b. Computer Catalog – PCs (portable, stationary), Servers, Clusters, Mainframes
        i. Storage – local, remote; fault tolerance
    c. Computing devices – Tablets, entertainment devices, smartphones
4. Virtual computer
    a. Why have virtual computers?
    b. What are virtual computers?
    c. How does virtual computing work?

Video Segment 2 – Operating System

5. Operating Systems: Concept and purpose – Primarily a handout
    a. Very basics of the role of an OS
    b. Very basics of the role of an application
    c. Reinforce the idea that “technology stacks” or “functionality stacks” are very common in IT.
6. History and Lineage of popular operating system families
    a. Windows
    b. Mac OSX
    c. Unix/Linux
    d. The value of understanding their history
7. Client vs Server Operating Systems
    a. Client-server model
    b. Objectives of each
    c. Typical similarities and differences in functionality and performance
8. Interaction mechanisms for OS users and administrators
    a. Physical interactivity
    b. Proximity of interaction
        i. “console”
        ii. remote session
            1. generic full featured

2. specialized interfaces
3. centralized management.

c. GUI vs command line
d. Interactive/transactional vs batch

Video Segment 3 – Networking

11. Purpose and function of networking
    a) Why is networking necessary?
    b) What does networking do?
    c) Basic introduction to components
12. Wired and Wireless Connectivity
    a) Wired
        i) Common types
        ii) Advantages of wired networking
        iii) Disadvantages of wired networking
    b) Wireless
        i) Common types
        ii) Advantages of wireless networking
        iii) Disadvantages of wireless networking
13. Concept and Purpose of common network arrangements
    a) Personal Area Networking
    b) Local Area Networking
    c) Wide Area Networking
14. Secure and non-secure networks
    a) Importance of the distinction
    b) What makes a secure network
    c) What makes a non-secure network
15. History, Structure and Challenges of the Internet
    a) History
    b) Structure
        i) Operational control
        ii) Logical layout of the Internet
    c) Challenges
        i) Functional
        ii) Security

Activities

Name	Objectives	Content ideas
Activity1	Reflect on the potential of computing; the nature of an actual computer and the gap between the starting point (just hardware) and what is being achieved. Reflect on	Questions or activities that explore: 1. The most common uses of a computer by a student 2. The major components of a computer 3. Terminology and concepts of

	what a virtual computer is	virtual computing
Activity 2	Reflect on the role of an Operating System Reflect on the role of applications Reflect on client-server model Reflect on transaction and batch computation	Questions or activities that explore: - The role of computers, operating systems and applications - Explore examples of the client-server model - Explore examples of transaction and batch processing that students may experience
Activity 3	Reflect on the elements of networking Reflect on the wired and wireless connectivity approaches Reflect on spatial scope and how it affects networking uses. Reflect on secure and non-secure networks	Questions or activities that explore: - Envision how the elements would work together possibly through role playing - Use case matching – align use cases to the three spatial options - Evaluate secure and non-secure network examples considering the issue of trust and control

Video Segment 4 – Cyber Security

20. Purpose of Cyber Security
    a. Origins of Cyber Security
    b. What is Cyber Security?
    c. Why is Cyber Security necessary?
22. Security Policy
    a. What is Security Policy?
    b. Why is Security Policy necessary?
    c. How is Security Policy developed?
    d. Security policy at device level
23. Risk management
    a. What is risk management?
    b. Avoiding vs Managing Risk
    c. Purpose of risk management
    d. Risk management terminology
    e. Basic steps of risk management

Video Segment 5 – Control concepts

25. Identity and Authentication

28. Authorization
    a. What is authorization?
    b. Why is authorization necessary?
    c. What is needed for authorization to be effective?
    d. Types of authorization mechanisms
29. Accountability
    a. What is accountability?
    b. Why is accountability necessary?
    c. What is needed for accountability to be effective?
    d. Types of accountability
    e. Mechanisms that support accountability

Video Segment 6 – Ideas to consider

30. Information states and their security considerations
    a. Three states of information
    b. Why is it useful to make these distinctions?
    c. Security considerations for information:
        i. At rest
        ii. In transit
        iii. In process
33. Security management
    a. What is security management?
    b. Beyond security policy – standards, guidelines, procedure
    ~~c. Approaches to security management~~
    d. Paradigm: Prevent, detect, respond
        i. Prevention
        ii. Detection
        iii. Response

Activities

Name	Objectives	Content ideas
Activity 4	Reflect on what cyber security is and its importance. Reflect on what a security policy is and its importance. Reflect on risk analysis terminology. Reflect on risk philosophies.	Select two of the following: Explore examples of using computers for personal or family purposes where they would want service providers to practice cyber security. Review a sample policy and discuss its contents. Review risk analysis terms in context of practical uses of the terms. Compare the two philosophies by applying them to a scenario involving a mock organization.
Activity 5	Reflect on identity, authentication,	Assign the terms to scenarios that describe the use of one or more

	authorization and accountability	control. The goal is to identify how the scenarios address the control objectives
Activity 6	Reflect on the 3 states of information. Reflect on how prevent-detect-respond provides defense in depth and resilience	Given a set of scenarios identify the dominant information state. Identify the major threats to the information in each scenario.

Handouts
Title: Components of a computer
Objectives:

1. Identify and explain the purpose of the components or major subsystems of a computer
2. Provide some historical and engineering context that shaped the way a computer's functions have been distributed to these components and the initial limitations that have had a lasting influence in computer design.
3. Provide an explanation of how the components tie together to form a functional system.
4. Discuss how a computer boots
5. Set up a segue to the next handout on operating systems

Length: 10 pages

Title: Operating Systems
Objectives:

1. Explain the need for operating systems and their primary functional objectives
2. Identify and explain the purpose of common components of operating systems used in client and server contexts (i.e. realtime, embedded, HPC etc. contexts are not in scope)
3. Explain how the computer's CPU and system architecture influences operating system development.
4. Introduce the concept of application programming interfaces and their purpose.
5. Set up a segue to the next handout on applications

Length: 10 pages
Notes:

1. Security concepts have not been introduced yet, so go easy on them. Don't rely on security terminology, but functional aspects of security concepts can be introduced.

Title: Applications
Objectives:

1. Explain the need for applications.

2. Describe some of the common ways applications obtain and manage information
3. Describe and explain the purpose for common application architectures
    a. Standalone
    b. Client-server
    c. Peer to peer
4. Describe the common constraints or considerations programming languages introduce on application development
5. Describe what constraints or considerations the computer+operating system platform introduce on application development

Length: 10 pages

Notes:

1. Integrate the discussion of APIs from the OS handout into this handout.
2. Networking concepts have yet to be introduced, so networking terminology should be avoided. Functional descriptions of networking are acceptable.

Title: Networking Protocols

Objectives:

1. Introduce the core concepts needed to understand network protocols
2. Describe Ethernet, WiFi, IP, ICMP, TCP, UDP layers of the TCP/IP stack
3. Discuss MAC addresses, IP V4 addressing, TCP/UDP ports and how they interrelate functionally from a DHCP and URL perspective
4. Discuss how IP addresses, subnetting and packet forwarding are related
5. Identify and describe the common network device components and identify what layer in the stack they operate. (NIC, bridge, switch, router, gateway)
6. Set up a segue to the next handout on network services

Length: 10 – 15 pages

Notes:

1.

Title: Network services:

Objectives:

1. Describe how networks services relate to the TCP/IP stack
2. Describe the purpose and function of DNS, FTP, Telnet, SSH, HTTP, SMTP, IMAP, POP, RDP (remote desktop protocol)
3. Describe how DNS relates to SMTP and URLs.
4. Mention that the definition of network protocols used on the Internet are available and where to find them.

Length: 10 – 15 pages

Title: Data Representation

Objectives:

1. Explain data abstraction and the need for data representations
2. Provide a brief historical context, functional description and purpose for: ASCII, Unicode, ASN.1, XML

3. Provide a brief historical context, functional description and purpose for file formats: JPG, WAV, MPEG, GIF, PDF, TXT

Length: 10 – 15 pages

Notes:

1. Relating data representations to network protocols and services would be helpful in better understanding how the protocols function
2. Assume the networking handouts were read before this one.

Title: Security Concepts

Objectives:

1. Provide an explanation and an example of how the concept can be applied in a practical context relevant to high school students for the following concepts: confidentiality, availability, integrity, trust, least privilege, need to know
   a. It may be worthwhile to add security concepts present in this module's presented materials.
2. This handout is meant to be a central resource for security terms and concepts used in the cyber defense program, so this handout may needed to be constructed iteratively as other modules are developed.
3. Some type of paper-based activity might be helpful for learning the terms. It should probably be at the end. An answer key should be provided either to the instructor or within the handout. A crossword puzzle might be good using the glossary's explanations as hints.

Length: 10 – 15 pages (hard to estimate given the security concept list is open ended)

Title: Password Security – Threats and Protection Ideas

Objectives:

1. Source may be part of a chapter written by Doug Jacobson and Joseph Idziorek in their book "Computer Security Literacy – Staying Safe in a Digital World."
2. Identify the threats to passwords throughout their lifecycle.
3. Identify best practice approaches to protect passwords from these threats.

Length: Depends on which pages are relevant and layout dimensions of the content.

Title: Multi-Factor Authentication Techniques

Objectives:

1. Identify multi-factor authentication techniques and discuss how they are used and how they function.
2. Biometrics may be a single factor, but it is worth at least discussing the notion of biometric authentication and how they work at a high level.
3. If data is available, explain the term "acceptability" and list the current social acceptability value for the various biometric authentication mechanisms. Acceptability relates to privacy concerns, invasiveness, and psychology and physical comfort with using a particular biometric technique.

Length: 10 pages

Notes: Be sure to provide device pictures and diagrams that explain function

Handout: Complexity and its Effect on Security
Objectives:

1. Complexity to be discussed is relevant to system design, application development and other common sources of complexity within IT environments. Explain how complexity manifests in these various contexts.
2. Explain what and how complexity introduces threats to security:
    a. More components as opposed to fewer components introduces greater opportunities for failure resulting from:
        i. Incorrectly designed, implemented or maintained interfaces necessary for the components to interoperate
        ii. Component diversity that results in the need for greater knowledge and skill diversity in order to operate and maintain them effectively. This in turn raises the possibility that personnel will not be available to address proper operations and maintenance.
    b. More components as opposed to fewer components introduces greater opportunities for integrity and confidentiality compromise:
        i. Component diversity increases the likelihood for vulnerabilities resulting both in their improper application from a design, implementation and maintenance perspective as well as in their construction from a design, implementation and maintenance perspective.
        ii. If more people as opposed to fewer are needed to sustain the system comprised of a complex arrangement of components, this greater number of people introduce a greater number of personal motivations that at one time or another may contradict security policy resulting in integrity and confidentiality problems.
3. Essentially the handout advocates the philosophy that less is more in many situations. If two security controls being considered are fairly equal in effectiveness, but one is more complex than the other than the simpler solution should be chosen.
4. Reality is that the drive for greater functionality and user convenience has resulted in complexity that must be managed securely.

Length: 5 – 10 pages

Handout: Functional Elements of Cryptography
Objectives:

1. Introduce the building blocks of encryption like keys, substitution and reordering.
2. Explain the significance of keys and their length. Additionally, explain the relationship between key length and their associated ciphers. Ex. Why is a DES key 56 bits?
3. Identify and explain the purpose for hashes, symmetric and asymmetric encryption, digital signatures and certificates. Avoiding the underlying math, provide an explanation for how these elements work.

4. Provide a systems explanation on how certificates are managed and their relationship with digital signatures

Length: 10 pages