CSC229 Course Walk-Through
Cybersecurity for Non-IT Majors

Sandra Gorka, Alicia McNett, **Jacob Miller**, Brad Webb

Pennsylvania College of Technology

This material is based upon work supported by the National Science Foundation under Grant No. 1623525. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

History

- In fall 2016 received NSF Cybercorps grant
- Improving the Pipeline: After-School Model for Preparing Cyber Defense and Information Assurance Professionals
  - Extend the IA/CS pipeline to the high school environment
  - After-school for college-credit program (4 credits)
- Award number: 1623525

Improving the Pipeline: Goals

- Raise awareness about cybersecurity careers
- Generate interest in those careers
- Prepare students to pursue the education required to succeed in cybersecurity fields

Evolution to Cybersecurity for Non-IT Majors

- Recognized the need for more security conscience workforce
- Incorporated assignments to meet Penn College's technological literacy requirements
- Reduced from 4 credits to 3 credits
- Materials developed for the grant are still in use for the course

Evolution to Cybersecurity for Non-IT Majors

- What we learned from the grant class
  - When students understand the rationale, they can better understand how their actions can impact themselves and the organization
- Cybersecurity for Non-IT Majors was designed to
  - Equip students to more effectively protect themselves and their employer
  - Enables them to continue to adapt and evolve with the ever-changing IT security environment

Cybersecurity for Non-IT Majors: Description

Introduction for non-IT professionals to the concepts of information security. Topics include many of the various hazards to data and information as well as a variety of current practices employed to keep data safe. Course work provides the skills necessary to secure one's own information assets or participate in an organization-wide security program.

Cybersecurity for Non-IT Majors: Outcomes

1. Identify information assets, the role of stakeholders, and the need for cybersecurity practices.
2. Identify and analyze the impact of ignoring the need for cybersecurity.
3. Recognize breaches, attacks, threats, and vulnerabilities, and respond appropriately.
4. Respond to threats accordingly within the scope of your role and responsibilities.
5. Select and use controls as needed to protect information assets.

Cybersecurity for Non-IT Majors: Outcomes

6. Locate and use tools and techniques that demonstrate cybersecurity vulnerabilities.
7. Examine the legal, ethical and professional issues involved with cybersecurity including policy and compliance.
8. Identify and apply the principle factors and tasks in risk management.
9. Identify and explain elementary software development concepts and how they relate to cybersecurity.
10. Identify and explain elementary computing and networking concepts and how they relate to cybersecurity.

Course Modules

0. Introduction to Security
1. Basics of Computing
2. Programming Basics
3. Security by Design
4. Basics of Networking
5. Networking Security
6. Wireless Security
7. Protecting Confidentiality: Encryption
8. Protecting Integrity: Hashing
9. Protecting Availability
10. Social Engineering
11. Risk
12. Policy, Legal Issues & Professionalism
13. Contingency Planning

Module Format:
Security Decision-Making Considerations

- Risk
- Controls
- Who cares
- Who implements
- What is protected

- When it must be protected
- Where it can be protected
- How it can be protected
- Why it is important to protect

Modules

- All modules have the same basic format
- Most modules only have one prerequisite: Module 0 Intro to Security
  - Confidentiality
  - Integrity
  - Availability

Sample Module: Protecting Confidentiality Objectives:

- Define cryptography, encryption and decryption
- Identify important data to protect
- Describe/identify when/where data needs to be protected
- Demonstrate how data can be protected using simple ciphers
- Demonstrate the ability to encrypt and decrypt files

Sample Module: Protecting Confidentiality Outline of Class Discussion

- Discuss the security decision-making considerations
- Define cryptography and discuss history
- Consider simple classical ciphers (substitution and transposition)
- Discuss modern ciphers and VeraCrypt

Sample Module: Protecting Confidentiality Activities/Homework

- Encrypt and decrypt simple substitution ciphers
- Encrypt and decrypt simple transposition ciphers
- Use VeraCrypt to create a container and store content within it

Cybersecurity for Non-IT Majors: Conclusion

- Designed to develop a more security conscience workforce
- Satisfies Penn College's technological literacy requirements
- Equips students to more effectively protect themselves and their employer
- Enables them to continue to adapt and evolve with the ever-changing IT security environment

Questions?

Interested in seeing the materials?

Email: cyber.pct@gmail.com

Email: Jake at jmiller3@pct.edu or Sandra at sgorka@pct.edu

Access the modules: https://forms.gle/p7JWbTn8iNBJZnR68

Sample Module

NOTE 1: Left out a few slides

NOTE 2: Condensed a few slides to just show topics

Protecting Confidentiality: Using Cryptography

Module 7

This material is based upon work supported by the National Science Foundation under Grant No. 1623525. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Objectives

- Define cryptography, encryption and decryption
- Identify important data to protect
- Describe/identify when/where data needs to be protected
- Demonstrate how data can be protected using simple ciphers
- Demonstrate the ability to encrypt and decrypt files
- (? Can we easily do this without servers set-up) Demonstrate the ability to encrypt and decrypt emails (see https://support.google.com/mail/answer/6330403?hl=en – requires G suite access - $5/month/user)

Security Decision-Making Considerations

- Risk
- Controls
- Who cares
- Who implements
- What is protected

- When it must be protected
- Where it can be protected
- How it can be protected
- Why it is import to protect

Course discussions include

- Definition of cryptography and a bit of the history
- Discussion of codes and ciphers
  - Navajo Code Talkers
- Simple ciphers including shift cipher, substitution ciphers, pigpen cipher

Activity One - Objectives

1. Use an online tool to decrypt a message
   http://www.xarg.org/tools/caesar-cipher
2. Use the crypt.exe program on the readonly drive to “Break” or decrypt a given message using a frequency analysis of letters.
   - The program is located at R:\sgorka\csc229\encryption\
   - There are more encrypted practice files at R:\jmiller3\CIT335\CRYPT – note you must rename the practice files to “crypt.txt”

Activity One, Task 1

- Use http://www.xarg.org/tools/caesar-cipher/ to decrypt the following messages:
  - Wklv lv d vdpsoh ri d Fdhvdu Vkliw flskhu
  - Kl, L’p Ulfn Kduulvrq, dqg wklv lv pb sdzq vkrs
  - JXU SYQ CETUB QTTHUIIUI JXU SEDVYTUDJYQBYJO, YDJUWHYJO QDT QLQYBQRYBYJO EV YDVEHCQJYED

Activity One, Task 2 – Encrypted Message

TQJQ IJEHUT YD SECFKJUHI HUFHUIUDJI Q BEJ EV YDVEHCQJYED QREKJ UQSX EV KI UW WHQTUI CUTYSQB XYIJEHO RQDA QSSEKDJI SHYCYDQB HUSEHTI UJS YV JXU MHEDW FUEFBU XQLU QSSUII JE JXQJ YDVEHCQJYED YV JXU YDVEHCQJYED YI YDSEHHUSJ EH YV JXU YDVEHCQJYED KDQLQYBQRBU MXUD DUUTUT JXYI SQD SQKIU Q LQHYUJO EV FHERBUCI VEH KI QDT SEKBT SQKIU YHHUFQHQRBU TQCQWU JE EKH HUFKJQJYED EH ULUD RUSECU BYVU JXHUQJUDYDW YV JXU MHEDW FUEFBU XQLU QSSUII JE EKH YDVEHCQJYED JXUD JXU SEDVYTUDJYQBYJO EV JXU YDVEHCQJYED YI SECFHECYIUT JXU SEDVYTUDJYQBYJO EV YDVEHCQJYED HUVUHI JE DEJ TYISBEIYDW JXU YDVEHCQJYED JE YDTYLYTKQBI MXE QHU DEJ UDJYJBUT EH QBBEMUT JE IUU JXU YDVEHCQJYED SEDVYTUDJYQBYJO FHEJUSJI EJXUHI VHEC BUQHDYDW YDVEHCQJYED QREKJ KI BYAU EKH WHQTUI EH CUTYSQB XYIJEHO KDBUII JXUO XQLU Q HUQIED JE ADEM JXU YDVEHCQJYED YV JXU YDVEHCQJYED YI YDSEHHUSJ JXUD JXU YDJUWHYJO EV JXU YDVEHCQJYED XQI RUUD SECFHECYIUT JXU YDJUWHYJO EV YDVEHCQJYED XQI RUUD SECFHECYIUT YV JXU YDVEHCQJYED XQI RUUD CETYVYUT EH TUBUJUT YD QD KDQKJXEHYPUT CQDDUH JXU YDJUWHYJO EV EKH WHQTUI EH CUTYSQB YDVEHCQJYED UDIKHUI JXQJ JXU YDVEHCQJYED XQI DEJ RUUD CETYVYUT JXHEKWX YDQFFHEFHYQJU CUQDI YV JXU YDVEHCQJYED YI DEJ QLQYBQRBU MXUD YJ YI DUUTUT JXUD JXU QLQYBQRYBYJO EV JXU YDVEHCQJYED XQI RUUD SECFHECYIUT QLQYBQRYBYJO CUQDI JXQJ JXU YDVEHCQJYED SQD RU QSSUIIUT MXUD Q FUHIED HUGKYHUI JXU YDVEHCQJYED

Transposition Cipher

- Rearranges the letters in a message using a key-based rule
- Similar to an anagram
- Example: “box” could become “obx”, “xbo” “xob”, etc.
- The key is the rearrangement (or permutation) order

Course discussions continue

- Transposition ciphers including scytale cipher

Activity 2:

1. Given a key, encrypt a short message using a shift cipher.
2. Given a key, encrypt a short message using a transposition cipher.
3. Given a key, decrypt a short message using a shift cipher.
4. Given a key, decrypt a short message using a transposition cipher.

Activity Two, Task One and Two

1. Encrypt the message: `Confidentiality can be protected using cryptography.`
   - Use a shift cipher with a key of 5 – that is, shift 5 characters forward.
2. Encrypt the message: `Confidentiality can be protected using cryptography.`
   - Use a transposition cipher using a block of 4 characters and switch the first and third characters.

Activity Two, Task Three and Four

1. Decrypt the message: `mlc uyw rm npmrcar glrcepgrw gq rm sqc y fyqfgle yjempgrfk`
   - The encryption key is 24 characters
2. Encrypt the message: `ahtn gski nivg asil yaws nnio mevb er`
   - Use a transposition cipher using a block of 4 characters and switch the first and third characters.

Course discussions transition to the ‘modern’

- Jefferson wheel cipher
- Enigma (rotor ciphers)
- Modern ciphers
  - Discuss how they combine multiple instances of substitution/transposition of bits
  - DES, AES, etc.
- VeraCrypt

Activity 3: Using VeraCrypt

Obtain from Course Management System

Activity 3: Using VeraCrypt

Overview

The purpose of this activity is to use VeraCrypt to create an encrypted container. A VeraCrypt Container is basically an encrypted file on your hard drive that can be used to store other files. You can use the VeraCrypt application to mount a VeraCrypt Container much like you mount a USB thumb drive. In order to mount the VeraCrypt Container, you must provide the password that will decrypt the container for use.

Note:

Using this application will encrypt files on your hard drive. Depending on how you use the application, you may accidentally encrypt your entire hard drive. If you do this and you forget the password you used, you will NOT be able to get your system back to a working order. Until you better understand this application, do not use it for anything other than creating VeraCrypt Containers.

Instructions:

1. Install VeraCrypt using the default settings.
    a. Download the VeraCrypt from the readonly drive or download it from https://sourceforge.net/projects/veracrypt/.
    b. Install VeraCrypt.
2. Create a VeraCrypt Volume.