Rationale

Why is this lesson important? Why does the student need this lesson? How does this lesson fit in the larger module?

It is important to know mitigation techniques for threats. Mitigation techniques using cryptography are common. The student needs this lesson to be able to choose appropriate cryptographic techniques to mitigate threats. This lesson provides the student with an overview of cryptographic techniques including symmetric-key cryptography, asymmetric-key cryptography, hash functions, message authentication codes, digital signatures, and authentication protocols.

Objective(s)

What will the student know, be able to do, and value at the end of this lesson? This is smaller amounts of information than the module objectives.

The student will be able to list symmetric- and asymmetric-key encryption algorithms, describe the difference between symmetric- and asymmetric-key cryptography, and modify an existing authentication protocol to make it more secure.

Exploration

Explicit concepts related to the Module goal are explored. It is at this point that the student will be provided basic information about the topic and the chance to explore some basic concepts about the topic. This is where the instructor imparts information.

- Cryptography – Cryptography is the study of encryption and decryption schemes.
  - Used to uphold the security principles of confidentiality and integrity
- Symmetric-key cryptography
  - Also known as secret-key or single-key cryptography
  - Plaintext – It is the original message or data
  - Encryption algorithm – It scrambles the message by performing substitutions and transformations on the plaintext based upon a key. The output of the encryption algorithm is called ciphertext.
  - Ciphertext – It is the scrambled version of the plaintext that the encryption algorithm produces.
  - Key – It determines the particular type of transformations and substitutions performed by the encryption algorithm. A different key produces a different ciphertext. The key must be kept secret. The key is usually a bit string representing a number. If the algorithm is secure/good, the bigger the length of the key the more secure the data is.
o Decryption algorithm – It is the algorithm that unscrambles the ciphertext to the original plaintext given the correct key.

o Exclusive-OR encryption and decryption

o Block cipher – It is an encryption/decryption algorithm in which data is processed in blocks. A block of plaintext produces an equal-length block of ciphertext.

o Stream cipher – It is an encryption/decryption algorithm in which the data is processed one bit or byte at a time.

o Block cipher examples

  ▪ Data encryption standard (DES)
    • 1977
    • NIST
    • 64-bit blocks
    • 56-bit key
    • Too small for many applications today
  
  ▪ Triple DES (3DES)
    • Apply DES three times
    • Two-key version (2x56 = 112-bit key)
    • Three-key version (3x56 = 168-bit key)

  ▪ Advanced encryption standard (AES)
    • NIST Standard in 2001 after contest
    • 128-bit block size
    • Key sizes: 128-, 192-, or 256-bit key
    • Larger block size more efficient and secure
    • High throughput (fast)
    • Efficient

o Stream cipher examples

  ▪ Exclusive-OR
  
  ▪ RC4
• Variable key: 1-256 bytes
• Secure sockets layer (SSL)
• Transport layer security (TLS)
• Wired equivalent privacy (WEP)
• WiFi protected access (WPA)

• Asymmetric-key cryptography
  • Also called public-key cryptography
  • Encryption and decryption performed with two different keys. The two keys are generated as a pair called a public key and private key and have special mathematical properties. The public key is distributed publicly and is used for encryption. The private key is kept secret and used for decryption.
  • Using two different keys has significant advantages.
  • Asymmetric-key cryptography is based on functions that are easy to calculate one way but computationally difficult to calculate the other way.
  • Two problems are solved using asymmetric-key cryptography
    • Key distribution
    • Digital signatures
  • Asymmetric-key algorithms
    • RSA
      • 1024-, and 2048-bit keys are common
      • Cannot compare length of keys directly to symmetric cryptography key lengths
    • Elliptic curve cryptography (ECC)
      • For the same key length, ECC is more secure than RSA

• Hash function
  • Hash function – It accepts a variable-length message and outputs a hash value (hash code, message digest)
    • One-way function
    • Hard or near impossible to reverse
Hash value is a function of all bits in a message and provides error detection. If one or more bits in the message change, the hash value should change with high probability.

- **Hash function examples**
  - **MD5**
    - Produces 128-bit hash value
  - **Secure hash algorithm (SHA-1)**
    - 160-bit hash value
  - **SHA-256, SHA-384, SHA-512**
    - Created after AES

- An attacker can substitute file and recalculate the hash value of the new file.

- **Message authentication code (MAC)**
  - Also called a cryptographic checksum
  - The MAC is a function of the message and a secret key shared between the sender and receiver to authenticate the sender to the receiver
  - **MAC examples**
    - Use a block cipher
    - **HMAC**
      - Use standard hash function
      - Key
  - An attacker cannot create the correct MAC because he does not know the secret key.

- **Digital signature**
  - Requirements
    - Verify author, date, time of signature
    - Authenticate the message
    - Verifiable by a third party to resolve disputes
  - **Digital signature examples**
    - Any asymmetric-key cryptography like RSA or ECC
- Digital signature algorithm (DSA)

- Authentication protocols
  - Authentication – It is the process of determining if an entity, whether an individual or an object, is who/what they claim to be. Some evidence has to be provided to prove the claim such as what they know, what they have, or what they are. Passwords are the most common form of authentication and are an example of what a user knows.
  - Protocols – Protocols define the series of messages exchanged between two or more entities and their meaning.
  - Mutual authentication protocol – It permits parties to verify each other’s identity. This is important before exchanging keys or data.
  - Main threat
    - Replay attacks
  - Asymmetric-key cryptography to establish a session key

Reflection
Several questions are posed to the student to answer and then often discuss as a class. This is an attempt to determine whether the student “gets” the basic concepts delivered above. If they do get it, move on to engagement. If they do not get it, go back to exploration above. It could be as simple as asking a few probing questions or as complex as asking the student to write a paper.

- What two principles are enforced using cryptography?
- What is the different between symmetric-key and asymmetric-key cryptography?
- Why is a hash function alone not good for authentication?
- Can a MAC be used for a digital signature? Why or why not?
- What is authentication?

Engagement
Concepts learned in the Exploration are further developed by conducting experiments, designing and building solutions, and solving problems. This is an attempt to cause the student to apply the new knowledge. By applying the new knowledge, the student is much more likely to retain this information. This engagement could be accomplished through a debate, an experiment, a problem solving activity, or anything else that would cause the student to demonstrate understanding and competence.

- What do we add to the given simple authentication protocol to mitigate replay attacks?

Expansion
Provide opportunities for students to expand the concepts to more general or global situations including
connection to the Module goal. Expand back to the big ideas of the module and prepare for the next lesson.

- If you cannot have encryption algorithms on a passive tag, can you still perform authentication?

**Lesson Assessment**
Assess student understanding of the lesson content. This does not have to be a full-blown examination. It could be a graded homework assignment, a quiz, a performance examination, a graded problem solving activity, or something similar.

- Homework

**Equipment**
- None

**Software**
- None

**References**
Copyright Notice
This material is Copyright © 2008, 2009, 2011 by Dale R. Thompson. It may be freely redistributed in its entirety provided that this copyright notice is not removed. It may not be sold for profit or incorporated in commercial documents without the written permission of the copyright holder.

Acknowledgment
These materials were developed through a grant from the National Science Foundation at the University of Arkansas. Any opinions, findings, and recommendations or conclusions expressed in these materials are those of the author(s) and do not necessarily reflect those of the National Science Foundation or the University of Arkansas.

Liability Release
The curriculum activities and lessons have been designed to be safe and engaging learning experiences and have been field-tested with university students. However, due to the numerous variables that exist, the author(s) does not assume any liability for the use of this product. These curriculum activities and lessons are provided as is without any express or implied warranty. The user is responsible and liable for following all stated and generally accepted safety guidelines and practices.