CS 493
Secure Software Systems

Ch 3 The Network Environment

Dr. Williams
Central Connecticut State University

Introduction

- Information that is communicated across computers immediately becomes a high risk for attack.
- Communication is the transmission of system information within or outside of the system boundary.

Objectives

- Terminology in network communications
- The process of communicating on a network
- The possible compromises of network traffic
- The proper application of cryptography to the network environment
- The Open Systems Interconnection (OSI) model of network communication
- Best practices in deciding which security measures to implement on a network

Goals

- Identify threats to network communication.
- Identify proper applications of cryptosystems to the protection of network traffic.
- Identify the risks associated with different layers of connectivity.
- Assess the needs of a message in transit.

Risk of networking

- Networking could potentially be considered the root of all cybercrime.
- **Networking**, is allowing one machine to communicate with another.
- The safest system in the world is one that is turned off, poured in concrete, and buried in a vault, but how useful would that be?

The cast of characters

- Alice and Bob
  - These are the personifications of A and B, respectively, two nodes that are sending information back and forth
  - The “good” parties, or more generally the systems we are trying to protect
- Eve (the Eavesdropper)
- Trudy (the intruder) – *note difference in capabilities with Eve will be important*

CIA in network

- **Confidentiality** - you do not want to unintentionally allow anyone other than the intended party to be able to read message
- **Integrity** means you do not want what you say to be twisted or misinterpreted in any way.
- **Authentication,** as it relates to communication, means you know you are “talking” to the person or entity to whom you wish to speak.

CIA

- **Nonrepudiation** means the person or entity to whom you are speaking cannot deny speaking to you and is therefore held accountable for what was said.
- Confidentiality can mostly be provided by the use of **cryptography**.

The Science of Secrecy

- Cryptography dates back more than 2,000 years; science of encoding a message so that it cannot be read when the message itself is compromised.
- Greeks - **transposition** by winding a leather strap around a stick and writing the message; when unwrapped for transfer, it would appear as a jumble of letters until it was wound around a stick of similar size at its destination.

The Science of Secrecy

- **A Substitution** cipher
  - Each letter of the alphabet is substituted by another symbol or letter
- The **Vigenére cipher**
  - Multiple substitution alphabets were used in a repeating pattern such that neighboring symbols were encrypted differently.

Cryptography in the Wartime Era

- **World War II -** German **Enigma cipher**
  - It had a number of encryption rotors, which could be changed and rotated to a new origin; the key for an Enigma machine was the set of rotors used and the starting position of each rotor
  - The **Enigma** was an incredibly strong encryption system and it was only broken by a concerted use of cryptanalysis and human misuse of the cipher by the German military.

Enigma cont.

- Enigma cipher - quantitatively too difficult to solve by brute force or short cuts by human personnel
- Defeated the combined use of mathematical attack, *cribs* in the intercepted text, and the first use of a computer to attack a cryptosystem.
  - A **crib** is a piece of known text in plaintext that corresponds to a section of known ciphertext
- Estimated allies breaking Enigma shortening the war by an estimated two to three years

The National Standard

- 1970s
  - national standard for encryption
  - introduction of public key cryptography

  Theoretical analysis of cryptographic properties
  - **Confusion** is the property of making the relationship between the key and the ciphertext as complex as possible.
  - **Diffusion** means that the ciphertext output should relate to the plaintext input in a very complex way.
  - **Symmetric Encryption** means that a single key, which has to be kept secret, is used to encrypt the plaintext and the same key was used to decrypt the ciphertext.

The National Standard

- IBM **Lucifer cipher –** Commercially available **block cipher**
  - fixed-size set of plaintext bits
  - Fixed-size set of ciphertext bits
  - Applied symmetric key.

- Became basis for Data Encryption Standard (DES) – became National Standard 1977
  - 56 bit key
- Replaced by Advanced Encryption Standard (AES) in 2001
  - 128, 192, or 256 bit key

Public Key Cryptography

- **Asymmetric encryption**
  - Uses two separate keys.
  - The encryption key is called a public key.
  - The decryption key is called a private key.
  - Introduced the ability to provide **non-repudiation**

The Quest for Perfect Secrecy

- Goal remains to develop an algorithm that will provide perfect secrecy in communication.
- **One-time pad**
  - Only algorithm found that establishes perfect secrecy
  - uses simple substitution with a key length equal to the length of the message so that each letter is substituted by a different alphabet without repetition.
  - immune to brute force because a brute force attack will yield every possible result of equal length to the message without any way to determine which one is the actual message.

The Quest for Perfect Secrecy

- One-time pad not used in network communications
  - Symmetric key, infinite length, key distribution problem
  - The big problem with a onetime pad is that the key size has to be equivalent to the message length and cannot be used more than once.

Eve Unleashed

- The simplest scenario is where Alice sends Bob a message (M) in the clear, or without any encryption. Eve can intercept this message, often without the detection of either party.
- Without any encryption, Eve can read the message and store the information for use at her leisure.

Eve Unleashed

- Eve can take the message offline and start working to break the encryption scheme
  - No security by obscurity
    - means you rely on an attacker not knowing how the internal mechanism of your security operates as a means of securing the system.
  - Strength of your security should be
    - you assume that an attacker knows how the message is encrypted and how your security schema works even if this is not the case
    - **Only thing they don’t know is the key**

Eve Unleashed

- Breaking cryptography
  - choice of the cryptosystem robust
  - Brute force
  - Password length/choice
  - Short cuts
    - D**ictionary attack** use of common words and password formats to form possible keys or passwords; generally effective and **much** faster than brute force

Introduction of Trudy

- Eavesdropping is generally a passive activity and the participants are unaware of the extra presence.
- Trudy more generally is an ***active*** attacker
  - Malicious modifications and insidious insertions
- **A cryptographic hash algorithm** is a one-way algorithm that converts the original message into a fixed size by a cryptographically complex process.

Malicious Modifications and Insidious Insertions

- Symmetric key crypto
  - **Integrity** - in conjunction with crypto-hashes between two parties with key
- Public key - **<u>signatures</u>**
  - Integrity and **nonrepudiation**.
  - message sent is guaranteed to be from the identified sender and the sender cannot later deny sending it.

Non-non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice computes **MAC** using symmetric key
- Stock drops, Alice claims she did ***not*** order
- Can Bob prove that Alice placed the order?
- **No!** Since Bob also knows the symmetric key, he could have forged message
- **Problem:** Bob knows Alice placed the order, but he can't prove it

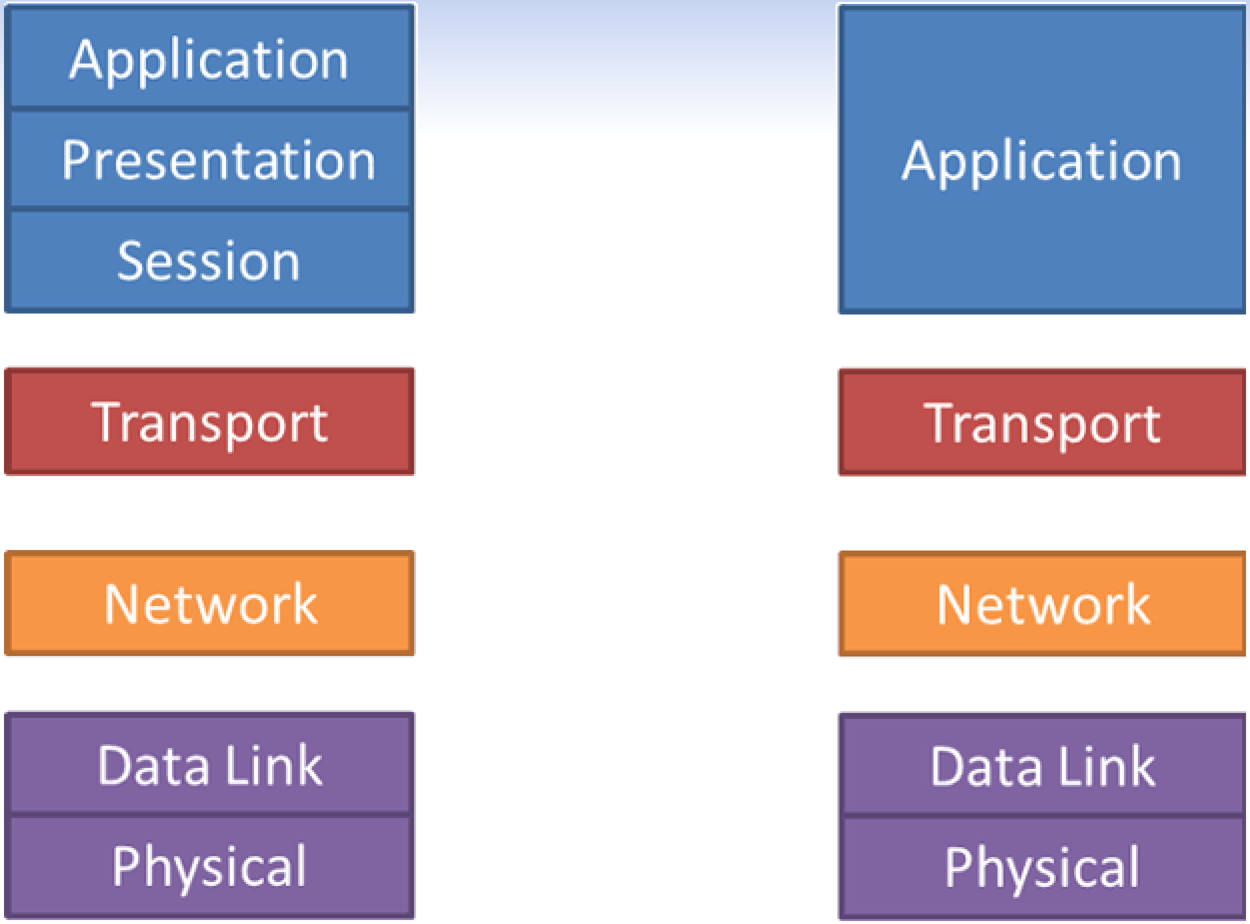
Non-repudiation

- Alice orders 100 shares of stock from Bob
- Alice **signs** order with her private key
- Stock drops, Alice claims she did not order
- Can Bob prove that Alice placed the order?
- **Yes!** Only someone with Alice’s private key could have signed the order
- This assumes Alice’s private key is not stolen (revocation problem)

Making the Connection

- Network communications follow a structure
- A **protocol** is a set structure for an exchange of messages that allows computers to determine what information is being sent and what to expect
- limited by the characteristics of the network on which it will travel
- 1978, the International Organization for Standardization (ISO) began defining what has evolved into the **Open Systems Interconnection (OSI) model.**

OSI vs TCP/IP model



Application
Presentation
Session
Transport
Network
Data Link
Physical

OSI model

Application
Transport
Network
Data Link
Physical

TCP/IP model

OSI Model

- Physical layer (layer 1)
  - connecting the machine to the medium of transmission.
- Data link layer (layer 2)
  - identifying characteristics to each machine on the network such as a physical address of a device, which is a Media Access Control (MAC) address, and the ability to detect errors in the physical layer.

OSI Model

- Network layer (layer 3)
  - Routing between machines
- Transport layer (layer 4)
  - Transmission protocols. This layer is responsible for providing end-to-end transfer of data, detecting errors in transmission, and retransmitting data if necessary.

OSI Model

- Session layer (layer 5)
  - tasked with organizing connections between a network node and a remote entity or service.
- Presentation layer (layer 6)
  - translates between application and network formats; this layer is primarily concerned with the representation of data and any possible structure of the data for use in the application layer.

OSI Model

- Application layer (layer 7)
  - Software is directly involved in directing network communications.

Roll Up the Welcome Mat

- One of the highest risks to a system that is connected to a network is uninvited traffic.
- The more complex a system becomes, the more likely it is that there is a proverbial backdoor that is not locked.
- A good housekeeping rule in development is to make sure that the module or object that opens a session also closes it.

Summary

- Communication is a vital component of any modern software system.
- There are techniques available to secure communications through confidentiality, integrity, nonrepudiation, authentication, and message freshness.
- Mitigation techniques need to be used for communication of any sensitive information housed within the system.

In class exercises

Bob’s Pizza Shack

In groups consider this scenario and draw a rough system diagram and identify the network concerns in the diagram and list your concerns

- Bob is a small business owner of Bob’s Pizza Shack and wants to create a website to allow online credit card delivery orders
- What are Bob’s security concerns from a network perspective?
  - Consider ones in own environment
  - Consider ones associated with the public facing web site
  - Consider data concerns

Alice’s Online Bank

In groups consider this scenario and draw a rough system diagram and identify the network concerns in the diagram and list your concerns

- Alice opens Alice’s Online Bank (AOB)
- What are Alice’s security concerns from a network perspective?
  - Consider ones in own environment
  - Consider ones interoperating with another bank
  - Consider ones interacting with customer
    - Web
    - Mobile app

Location based social media app

In groups consider this scenario and draw a rough system diagram and identify the network concerns in the diagram and list your concerns

- Open source group wants to create a mobile app to allow groups to communicate/find each other in public demonstrations/protests
  - Communication internet, as well as, P2P (WiFi/Bluetooth) in case internet cut off – so if person you want to contact is on other side of crowd and no internet as long as P2P network can be established with app can reach somebody outside your immediate vicinity via the P2P network
  - Should be able to communicate securely messages and images to people you identify within your group (group as whole or direct)
  - Should be able to share GPS location with people in group (group as whole or direct)
- Broader scope – Who are potential threats and associated ways could attack/weaken system?