CRIM 2130 Introduction to Critical Infrastructure Protection
Spring 2016

Chapter 8 – Information Technology

School of Criminology and Justice Studies
University of Massachusetts Lowell
Some Key Terms

- Enterprise systems
- Cybersecurity (used interchangeably with IT security)
- DMZ (demilitarized zone) in cybersecurity
- VPN (virtual private network)
- Asymmetric encryption
- Cipher
- AES (advanced encryption standard)
- CA (certificate of authority)
- TCB (trusted computer base)
- TCP (trusted computer path)
Principles of IT Security

- **Authentication**
  - Verify authenticity of users and data

- **Integrity**
  - Guarantee message or document has not been altered

- **Confidentiality**
  - Ability to conceal content of messages and documents

- **Nonrepudiation**
  - Inability to deny authenticity; non-concealment of ownership
Basic Principle of IT; secure Computing
Privacy is another issue
Trusted base and communication path to user
“Encapsulation” is inviolate; sometimes called a DMZ

Figure 8.1 in Text
Demilitarized Zone (DMZ)

- Encapsulated through layers
  - User level via authentication
  - Network via encryption
  - Hardware via firewalls and intrusion detection systems

Figure 8.2 in Text - Encapsulation of IT assets inside of a hardened DMZ
Encryption

- Symmetric encryption is used to secure information between trusted parties
  - Same key that is shared by both parties
- Asymmetric encryption is used to secure information between anonymous parties.
  - Two keys; one to send, other to receive information
  - Sender uses a public key; receiver uses a private key
  - Requires a key broker in between, however
Standard Symmetric Encryption

- Digital Encryption Standard (DES) and triple-DES (applies cipher algorithm three times to each data block)
  - Older codes evolved from Lucifer (IBM) in 1960s and 1970s
  - Adequate for short bursts of messages with short-lived keys
  - Commonly used by cell phones and web sites
- Advanced Encryption Standard (AES) by the U.S. National Institute of Standards and Technology (NIST) in 2002
  - Strong encryption (256-bit keys); suitable for small computers such as those used in SCADA systems.
- 3DES and AES are Federal Information Processing Standards (FIPS) compliant
  - Required by Federal Government.
Asymmetric Encryption

- Diffie-Hellman (D-H) cipher; Asymmetric ciphers rediscovered by Diffie and Hellman in 1976
  - Public key to encode
  - Private key to decode.
- Rivest, Shamir, and Adleman (RSA) invented a practical method of performing the D-H algorithm
- RSA algorithm
  - Makes it possible to authenticate users (digital signatures) and protect the security of sender and receiver
RSA Encryption

- RSA encryption looks random
- Public Key Infrastructure (PKI) makes security possible

Figure 8.3 in Text
Example of RSA encryption: private, public keys and plaintext/cyphertext

Figure 8.4 in Text
PKI authenticates the identity of users by assuring that the sender is who he or she claims

- Guarantees integrity and security of the message by assuring that it has not been modified by an intermediary
- Assures privacy by ensuring message is decodable only by intended recipient
- Guarantees authentication, security and privacy by assuring the message is signed by the verified parties
- Guarantees non-repudiation by assuring that both parties cannot disavow or deny involvement with the transaction.
Public Key Infrastructure (PKI) (Cont.)
IEEE X509

- Four fundamental principles of IT sector security as defined by the IEEE X509 Standard
  - Authentication
  - Information integrity
  - Information confidentiality
  - Non-repudiation of ownership

https://www.ieee.org/index.html
Alice Sends Message to Bob

- PKI example using a certificate

1. Alice gets Bob’s Public Key from CA.
2. Alice signs Msg_to_Bob using her Private key.
3. Alice encrypts her signed Msg_to_Bob using his Public key.

Bob Receives Msg_to_Bob

1. Bob gets Alice’s Public Key from CA.
2. Bob decodes Msg_to_Bob using his Private Key.
3. Bob authenticates Alice’s identity using her Public Key

Figure 8.5 in Text
Countermeasures

- Sample countermeasures to vulnerabilities typically found in enterprise systems
  - Power failure and backup power supply
  - Open modem and VPN
  - Desktop and patches and anti-virus software
  - No firewall and install firewalls and filter ports
  - Browser session open and time-out inactive screens

Table 8.2 in Text

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Counter-Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Failure</td>
<td>Buy Backup Power Supply</td>
</tr>
<tr>
<td>Telecom Failure</td>
<td>Buy redundant Telecom Service</td>
</tr>
<tr>
<td>SYN Attack</td>
<td>Install IDS</td>
</tr>
<tr>
<td>No IDS</td>
<td>Install Firewall: Filter Ports</td>
</tr>
<tr>
<td>Break-in</td>
<td>Install IDS</td>
</tr>
<tr>
<td>Clear Password file</td>
<td>Encrypt password files</td>
</tr>
<tr>
<td>No Backup</td>
<td>Do Periodic Backups</td>
</tr>
<tr>
<td>No Firewall Filter</td>
<td>Install Firewall: Filter Ports</td>
</tr>
<tr>
<td>No Anti-viral SW on desktop</td>
<td>Install Firewall: Filter Ports</td>
</tr>
<tr>
<td>Clear XML/HTML</td>
<td>Install HTTPS/SSL</td>
</tr>
<tr>
<td>Clear Browser use</td>
<td>Install PKI/VPN</td>
</tr>
<tr>
<td>Password not changed</td>
<td>Time-Out Inactive Sessions</td>
</tr>
<tr>
<td>War dialing</td>
<td>Change password periodically</td>
</tr>
<tr>
<td>No HTTPS/SSL</td>
<td>Close modem ports</td>
</tr>
<tr>
<td>Browser Session Open</td>
<td>Install HTTPS/SSL</td>
</tr>
<tr>
<td>Weak Encryption</td>
<td>Time-out Inactive sessions</td>
</tr>
<tr>
<td>Weak LDAP in applications</td>
<td>Install 3DES or AES</td>
</tr>
<tr>
<td>Buffer overflow</td>
<td>Install PKI</td>
</tr>
<tr>
<td>Weak OS Patches</td>
<td>Modify Applications</td>
</tr>
<tr>
<td>Open Wi-Fi ports</td>
<td>Install firewalls: Filter ports</td>
</tr>
<tr>
<td></td>
<td>Encrypt Wi-Fi Sessions</td>
</tr>
<tr>
<td>Open FTP ports</td>
<td>Install firewalls: Filter ports</td>
</tr>
<tr>
<td></td>
<td>Authenticate Wi-Fi users</td>
</tr>
<tr>
<td>Open modem</td>
<td>Close dialup modes or use VPN</td>
</tr>
<tr>
<td>Server Filter off</td>
<td>Install firewall: Filter ports</td>
</tr>
<tr>
<td></td>
<td>Encrypt Wi-Fi Sessions</td>
</tr>
<tr>
<td></td>
<td>Install IDS</td>
</tr>
<tr>
<td></td>
<td>Install firewall: Filter ports</td>
</tr>
<tr>
<td></td>
<td>Encrypt Wi-Fi Sessions</td>
</tr>
<tr>
<td></td>
<td>Close FTP or Filter Ports</td>
</tr>
<tr>
<td></td>
<td>Turn on Firewall Filtering</td>
</tr>
</tbody>
</table>