Network Security: Terminology, Mechanisms and Tools Overview

Network Management
Prof. Dr.-Ing. Alexandru Soceanu

Motivation

- Number of Computer Networks are constantly increasing

- ca. 400 new types of viruses, warms, back doors programs, blended threats are discovered every week!!!

- Companies, public institutions, private people are more and more networked than ever: i.e. They all need protection

Security Goals for transferred information:

- Confidentiality: hidden from unauthorized access
- Integrity: protect from unauthorized change
- Availability: available to an authorized entity when is needed

Taxonomy of attacks in relation to security goals:

a) Threat to confidentiality (passive attack):
- Snooping
- Traffic Analysis

b) Threat to Integrity (active attack):

- Modification
- Masquerading (attacker impersonates somebody else)
- Replaying (attacker gets a copy of the original message and later on replay it; ex.: bank payments
- Repudiation (sender or receiver denies that they received a message; ex.: buy a product, pays it electronically and later the seller denies that a payment occurs)

b) Denial of Service (active attack)

Security Services (according to specifications X.800 from ITU-T)

- Data Confidentiality

- Data integrity:
  - anti-change
  - anti-rplay

- Authentication
  - per entity
  - data orogin

- Nonrepudiation
  - proof of origin
  - proof of delivery

- Access control

Security Mechanisms(according to specifications X.800 from ITU-T)

- Encipherment
  hiding or covering data using cryptography or steganogrphy

- Data integrity

- Digital signature
  sender can electrically sign the data and the receiver
  checks the signature

- Authentication exchange

- Traffic padding
  insert some special data into the traffic to mess up the
  traffic analysis done by an attacker

- Routing control
  permanently change the route between sender and receiver
  in order to avoid eavesdropping on a particular route

- Notarization
  select a third trusted party to control the communication
  between two entities

- Access control
  prove that a user has access rights to the data or resources
  ex.: proof passwords and PINs

Security Services relations to Security mechanisms

Security Service	Security Mechanisms
Confidentiality	Encipherment, Routing control
Integrity	Encipherment, Digital signature, Data integrity
Authentication	Encipherment, Digital signature, Authentication exchanges
Nonrepudiation	Digital signature, Data integrity, Notorization
Acces control	Access control mechanisms

Techniques to implement security

A) **Cryptography** (Greek origins: secret writing)

Definition: Using three distinct mechanisms in order to transform the message so that it is immune to the attacks

Cryptography mechanisms:

a) Symmetric-Key Encipherment (secret-key encipherment)
   - sender and receiver encrypt/decrypt the message using an encrypt/decrypt algorithm
   - encpryption and decryption takes place using a single ***secret key***

b) Asymmetric-Key Encipherment (public-key cryptography)
   - encpryption and decryption takes place using two keys:
     - ***public key***
     - ***private key***
   - sender encrypts the message using the public key
   - receiver decrypts the message using its private key

c) Hashing
   - used to provide check values which are necessary for verifying the integrity of the messages
   - a fixed length message ***digest*** is generated out of a variable-length message. The digest is much smaller than the message
   - sender sends the message and the digest to the receiver

B) Steganogrphy (Greek origin: “cover writing”)

- conceiling the message itself by covering it with something else
- cover of the secret dta can be a text;
  ex.:- insert single space between words to represent a binary0
  - insert double space between words to represent a binary1
- cover the secret data under a color image
  ex.: digitized images are represented using pixels:
  - 1 Pixel= 24 bits/3 Bytes;
  - each Byte represent : red, green, blue
  - one can have 2^8 different shades of each color
  - one can use the least significant bit out of each byte in order to hide the secret information.

Network Security Methods and Tools

The previous methods defined above are combined in order to build different layers of defense used to protect the networks using Internet model

Comparison of different network security methods and tools

File Level	→	**Steganography, Steganalysis** *Examine files inside application traffic*
Application Level	→	**Intrusion Detection Prevention IDS/ IPS** (*Examine application fields within the traffic)*
Session + Transport Level	→	**- Firewall statefull inspection** *Examine packet header and control fields; usage of state behavior* **- SSL** *(Secure Sockets Layer)* **- TSL** *(Transport Layer Security)*
Network Level	→	**- Packet Filtering** (Access Control Lists: ACL-CISCO or IPChains-Linux) *Examine few fields within the packet header* - **IPSec** (IP Security) Modes of operation: - Transport Mode - Tunnel Mode
Data Link Level	→	- **VLAN Security** (Security policies based on different type of VLANs: - Port based-VLAN - MAC based VLAN - IP Based VLAN - Application based VLAN
Physical Level		-----

First layer of defense

A) VLAN (Virtual LAN)

B) IPSec(IP Security)

C) Packet Filtering

Principle: Open two ports for each communication channel
- one Port for incoming traffic
- one Port for outgoing traffic

Problems: The ports are not associated with the content and relationship of the traffic flowing in and out

Result: Malicious packets can be appearing as being part of existing session. These packets can cause damage for protected resources

Second layer of defense

A) SSL (Secure Socket Layer)

B) TSL (Transport Layer Security)

C) Firewall Statefull Inspection

- Principle: Determine what traffic should be *allowed* and what traffic should be *denied* based on so called ***policy rules***

- Implementation: In order to support applications important to the organizations a Firewall has to allow traffic carried by typical Internet protocols like i.e.: HTTP, FTP, SMTP

- Result: ***Firewall keeps out traffic that it considers as may representing a threat for the organizational network These allowed traffic may contain different type of hidden attacks***

- Solution: Extend the security protection with a so called ***second layer of defense***

Third layer of defense

The methods known for implementing this layer are based on a thoroughly real time *analyses of the applications as well as of the content* of the transferred files.

A) IDS- Intrusion Detection System

- Real-Time analyses of applications within the traffic
- ***Detect so called "bad traffic" based on signatures and protocol anomaly detection***
- Generate "positive alarms" in case detecting bad traffic

B) IPS- Intrusion Detection and Prevention System

- Real-Time analyses of applications within the traffic
- Detect so called "bad traffic" based on signatures and protocol anomaly detection
- ***Drop and Block the connection transporting real bad traffic***
- Generate "positive alarms" in case detecting bad traffic

C) Steganography

Method for transporting information invisible (hidden).
The hidden message can be any digital data, and it can be hidden in almost any type of digital data

Principle: - the existence of the real message is unknown
- the main goal is to hide the real message along to other information.

Result: is achieved if no suspicion about the transportation of hidden data is raised.

***Security solution: Steganalysis*:**
Methods for investigating the transported data.
It has two main goals:

1) discovering /proving the existence of hidden messages
2) destruction of these messages

State of the Art in Steganography
The recent research and development activities concentrate on:
creating new steganography tools and algorithms mainly for hiding text or images inside text, images or audio data.

IDS-System Limitations

1) False Alarms:

Inaccurate results due to poorly implemented detection mechanism

***Result*: Large number of alarms which overwhelm the system administrator**

Most ID-systems can be tuned to reduce false alarms. Tuning requires very long time periods, and irritate the administrators

2) Low Manageability and High Maintenance

- It requires large efforts to keep the sensors and Security Policy updated

- For this reason many companies are forced to outsource the maintenance of their ID-Systems

3) No Prevention of Attacks

IDS are merely detection tools and not able to ***prevent*** attacks
This is why the IDS are vulnerable to so called "evasion"

Evasion = fools the ID mechanism into seeing different data than the victim host. This allows attacks without being detected

The most significant drawback to a ***"Passive IDS"*** is that it is passive and can not control whether the attack is allowed to reach the target; i.e. ***no Prevention***

IP-System advantages vs. ID-System

1) *Able to Deny traffic based on*:

a) IP-Address
b) protocol/service
c) "Application Level" analysis and verification

2) *Support a wide range of protocols and applications*

Operation steps:

a) receives traffic from network
b) reassembly the traffic streams
c) analysis at the application level the primitives and the commands in order to detect suspicious fields

Limitations of the IP-Systems

Application and protocol protection does not do a detailed analysis at the File Level

Solution: for File Level protection usually are used so called : ***Gateway Antivirus*** Systems (GAS)

Operation of the GAS

a. extract files from the traffic
b. inspect files based on signatures
c. detect malware, i.e.: Viruses, Warms, Trojans
d. remove the detected infected file from the traffic
e. update constantly the virus pattern data in order to reach an effective protection

f. typically scanned files are:
   - e-mail from server to clients
   - web traffic from server to clients

Detection Techniques

The common used mechanisms are:

1) Signature Detection

Look for known attack patterns within the traffic. This is implemented using a so called “Sniffer” which is a packet monitor
The system looks into the information contained in the packet stream and compare it to a data base of known attack signatures

Disadvantage of this approach:

- ***Performance slow*** down because the entire flow needs to be searched
- ***False Positive*** are most likely to occur, because if more data are searched, the more likely is to find a match with a signature to irrelevant data

Limitation: Attacks for which a signature is not written can not be detected

2) Protocol Anomaly Detection (Protocol Analysis)

- analyze the packet flow and the identify deviation of internet rules of communication (deviation from RFCs)
- attacks which can be detected are:
  a) unknown and new attacks only because the traffic contains deviation from protocol specifications
  b) attacks that treys to bypass the system
  c) slightly modified attacks that change the format of known attack patterns

Example:
Protocol Anomaly detection: ***FTP Bounce Attack***

Operation steps of FTP Application for downloading or uploading files:

1) user starts to connect to FTP-Server

2) Server requires from the client:
    - IP-Address
    - Port Number where the file should be sent

   This is so called "Port Command".
   Port Command specification does not limit the IP-Address to the user's address

3) Attacker tells the FTP-Server to open a connection to an IP-Address different from the user's address

4) Attacker uses the open port to transfer files containing a Trojan through FTP-Server onto the victim

5) Attacker is now able (because of Trojans) to access the victim host and transfer files from the victim to the attacker's computer

An Intrusion Detection System should be able to detect the above described attack by doing following :

- compare the request in the "Port Command" with the IP-Address of the client

- in case no match, then IDS sends an alarm.

Conclusion: ***Protocol Anomaly Analysis*** can detect attacks even though the signatures for these attacks are not known.

3) Stateful Signature Detection (SSD)

SSD identifies attacks pattern by using:

- stateful inspection and
- protocol analysis performed as part of "Protocol Anomaly Detection "

Result: a) Statetful Signature (SSD) understands

- the context of each data byte and
- the state of the client and server at transmission time

b) SSD looks for an attack in the state of the communication where the attack can cause damage

c) SSD procedure improve performance and reduce the number of "False Positive" messages

Extension of the SSD Procedure

- pattern search is not done just on fixed pattern
- the search supports so called "Regular Expression (RE)"
  RE provides wildcards and complex pattern matching
  Example:
  Look-up within an e-mail with an executable attachment
  name = "< Any-Name>.exe
  RE analysis procedure allows that:
  the sign "=" is
  preceded or followed *by any number of spaces and tabs*

4) Backdoor Detection (BKD)

Detect attacks that are unknown and do not violate a protocol

ex.: ***Trojans*** and ***Warms***

These attacks install and open up a “back door” on a station connected to a network.
Attacker can to a later time ***activate this “back door” and take control*** over the victim.

Solution:

- detect the unique characteristics of this interactive traffic
- check all interactive traffics and detect which is unauthorized based on what the administrator defined as “allowed” in the rule base
- this procedure ***detects any “back door”*** attack even in case ***the traffic is encrypted and the protocol is unknown***

5) Traffic Anomaly Detection (TAD)

Identify the attacks consisting out of

- “scanning” all the ports of the resource
- “scanning” a specific port within the entire network

Attacker discovers ***vulnerabilities*** for the responding services on those open ports

Solution:
Identify pattern within the overall traffic flow based on:
frequency and threshold triggers

ID- and IP-System Manageability

In order to benefit from the detection mechanisms of the

Intrusion Detection and Intrusion Protection Systems

they have to be for the administrator ***easy to manage***.

Solution:
Most of the IDS and IPS manufacturer provides management approaches for their systems similar to the ones known from the Firewalls:

- ***granular control of the system capabilities***

- ***rule based management scheme***
  i.e.: one can control all devices under management with a ***single logical security policy*** which is made up of individual rules.
  Rule => basic format of matching criteria and
  associated action specification

- ***centralized security policy***
  this approach enables to determine how the administrator would like to be applied each rule;
  ex: one rule is applied to one sensor or to all sensors

- ***automatic updating***
  updating is carried out via Central Security Policy which once updated it will apply automatically to all corresponding sensors

- ***closed loop investigation***
  move freely from summary reports to the individual logs and to rules that triggered as well as to the packets data of the logs