What is computer security?

Security requirements of different system are different.

University:
- Papers, discoveries and work are available to the public.
- Protects the integrity and confidentiality of grades and other data.
- Its shared resources must be open via the internet.

Military research organization:
- All the work within the organization must remain secret.
- Emphasizes confidentiality over integrity.
- None of its resources must be available over the internet.
Security Components

- **Requirements**: “What do you want security to do for you?”

- **Policy**: “What steps do you take to reach the goal set out above?”

- **Mechanisms**: “What tools and procedures do you use to ensure the above steps are followed?”

---

Firewalls

The role of a firewall is to deny or permit access to a network based on the enforced policy.

- **Packet Filtering Firewalls**. Applies packet filters based on protocol type, on source and destination address and on source and destination ports.

- **Application Gateway Firewalls**. Every connection to a host outside of the internal network is made through an application program called a proxy.

- **Stateful Inspection Firewalls**. Track the state of communication sessions and dynamically open and close ports based on access policies.

Therefore a firewall can implement policies that concern the perimeter of the protected network.
The Role of an Intrusion Detection System (IDS).

- “With so much advancement in hacking, if attackers try hard enough, they will eventually succeed in infiltrating the system. This makes it important to monitor what is taking place on a system and look for suspicious behavior. Intrusion detection systems do just that.”

- A false positive occurs when the IDS reports an event of legitimate network activity as an intrusion.
  Likewise a false negative occurs when the IDS fails to detect malicious network activity.

- As we employ heavier rules in the IDS we can detect more variances of intrusion attempts but more false positives are probable.
  If we employ lighter rules, we have less false positives but the system is easier to penetrate.

- The security policy for the specific system must specify how the IDS would perform.

Definition of IDS

- An Intrusion detection system is a system that is used to detect inappropriate, incorrect or anomalous activity.

- Can be host based or network based.

- Malicious activity can be classified as misuse if it originates from the internal network or intrusion if it originates from the external network.

- Most common approaches are pattern matching detection and statistical anomaly detection.
Pattern Matching Detection

- Looks for a fixed sequence of bytes within each packet. To filter traffic inspection the pattern is also usually associated with a particular service and source or destination port.

- For example it looks for IPv4 packets that use TCP protocol, have destination port of 27015 and contain the string “abc” in the payload.

- Is straightforward and easy to deploy but…
  - Many attacks and protocols don’t always use well known ports.
  - If the matching pattern isn’t so unique a large number of false positives can occur.

Stateful Pattern Matching

- Stateful packet matching adds to pattern matching by searching for unique sequences that might be distributed across several packets within a stream.

- Is more specific that pattern matching but…
  - Is still vulnerable to false positives if the pattern isn’t unique enough.
  - Slight modification of an attack can avoid detection.
Statistical Anomaly Detection

Statistical anomaly detection detects activity that deviates from “normal” activity. It depends on the statistical definition of normal and because of that is usually prone to a large number of false positives.

Intrusion detection based on Hidden Markov Model

The Hidden Markov Model is a finite set of states each of which is associated with a probability distribution. Transitions among the states are governed by a set of probabilities called transition probabilities.

In a particular state, an outcome or observation can be generated according to the associated probability distribution.

It is the outcome, not the state visible to an external observer and therefore the states are “hidden” to the outside.
Building a Hidden Markov Model

- The biggest challenge is to select the states that best characterize the system’s activity.
- Usual observable outcomes are login events and system calls.

![Transition Matrix Diagram](image)

<table>
<thead>
<tr>
<th></th>
<th>a11</th>
<th>a12</th>
<th>a13</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>a11</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>a21</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>a22</td>
<td>1</td>
<td>a33</td>
<td>a34</td>
<td>a35</td>
</tr>
<tr>
<td>a41</td>
<td>0</td>
<td>0</td>
<td>a44</td>
<td>a45</td>
<td></td>
</tr>
<tr>
<td>a51</td>
<td>0</td>
<td>0</td>
<td>a54</td>
<td>a55</td>
<td></td>
</tr>
</tbody>
</table>

The IDS knows the initial state of the system. Then it calculates the possible transitions and observable outcomes for a series of steps.

- If a series of observable outcomes matches the predicted behavior of the model, then the behavior is considered as normal, else it is considered abnormal.
Weaknesses of an IDS implementation

- The IDS does not know the full range of behavior allowed by a particular protocol.
- The IDS does not know the exact expected behavior of each host.
- The IDS does not know the topology of the internal network.

These ambiguities can be exploited by an attacker to trick the IDS into assuming different activity that the actual.

By manipulating the TTL field in the IP header the IDS does not know which packet actually arrives at the end host.
The IDS does not know how the end host would deal with the reception of overlapping packets

“The passive network intrusion detection systems can only effectively identify malicious flows when used in conjunction with an interposed active mechanism”.

Traffic Normalization / Protocol Scrubbing

Active Networks
Traffic Normalization

The normalizer’s job is to sit directly in the path of traffic into a site and patch up or normalize the packet stream to remove potential ambiguities so that the traffic seen by the intrusion detection system is guaranteed unambiguous.

How a normalizer treats some ambiguities of the IP Protocol

IPv4 Header

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Header Len</td>
<td>TOS/Diffserv/ECN</td>
<td>Total Length</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP Identifier</td>
<td>0</td>
<td>DF</td>
<td>Fragment Offset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time to Live</td>
<td>Protocol</td>
<td>Header Checksum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source Address</td>
<td>Destination Address</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Options</td>
<td>Padding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Version:** A normalizer should only pass packets with IP version fields which the NIDS understands.

**Header Length:** It may be possible to send a packet with an incorrect header length field that arrives at the end system and is accepted. However, other operating systems or internal routers may drop the packet. If the header length is less than 20 bytes or exceeds the packet length it should be discarded.

**Don’t Fragment Flag:** If DF is set and the Maximum Transmission Unit (MTU) anywhere in the internal network is smaller than the MTU on the access link to the site, an attacker can deterministically cause some packets to fail behind the link. The normalizer clears the DF flag.

**Time To Live:** The normalizer sets the TTL value greater than the largest path across the internal site.

**More Fragments / Fragment Offset:** An ambiguity arises if two incoming fragments overlap each other and differ in their contents. Internal hosts may resolve the ambiguity differently. The normalizer reassembles incoming fragments before forwarding them. If needed fragments them again.
Stealth port Scans: The normalizer transmits an ACK packet behind every RST packet it forwards out of the site.

Attacks On the Normalizer:

Stateholding attacks: The attacker tries to consume the normalizer's memory by causing it to instantiate too many states. Common stateholding attacks are:

- **SYN flooding**: The attacker floods SYN packets so that the normalizer instantiates states for each connection.
- **ACK flooding**: If the normalizer restarted recently by receiving an ACK packet it instantiates state because the packet might be part of a connection that initiated before the restart.
- **Initial window flooding**: The attacker sends a SYN to an internal host, receives a SYN-ACK and then floods data without sending ACK. The normalizer would buffer that information to prevent inconsistent retransmissions.
**CPU overload attacks:** An attacker attempts to overload the CPU on the normalizer. Such attacks can cause the normalizer to forward packets at a slower rate than it normally would, but cannot cause an ambiguity to pass.

**Usual policy of the normalizer to withstand such attacks:**

The normalizer knows whether or not it’s under attack by monitoring the amount of memory it is consuming. If it’s not under attack it can instantiate whatever state it needs to normalize correctly. If it believes it is under attack, it takes a more conservative strategy that is designed to allow it to survive, although some legitimate traffic will see degraded performance.

---

**Active Network-Based Intrusion Detection and Response systems**

- Active networks carry executable code within packets which is executed at network nodes such as hubs, bridges, switches, routers, gateways.

- Communication is achieved using the Active Network Encapsulation Protocol (ANEP)
Active Network-Based Intrusion Detection System Design

References


Intrusion Detection Based On Hidden Markov Model. Qing-Bo Yin, Li-Ran Shen, Ru-Bo Zhang, Xue-Yao Li, Hui-Qiang Wang.


An Active Network-Based Intrusion Detection And Response Systems. Han-Pang Huang, Chia-Ming Chang.