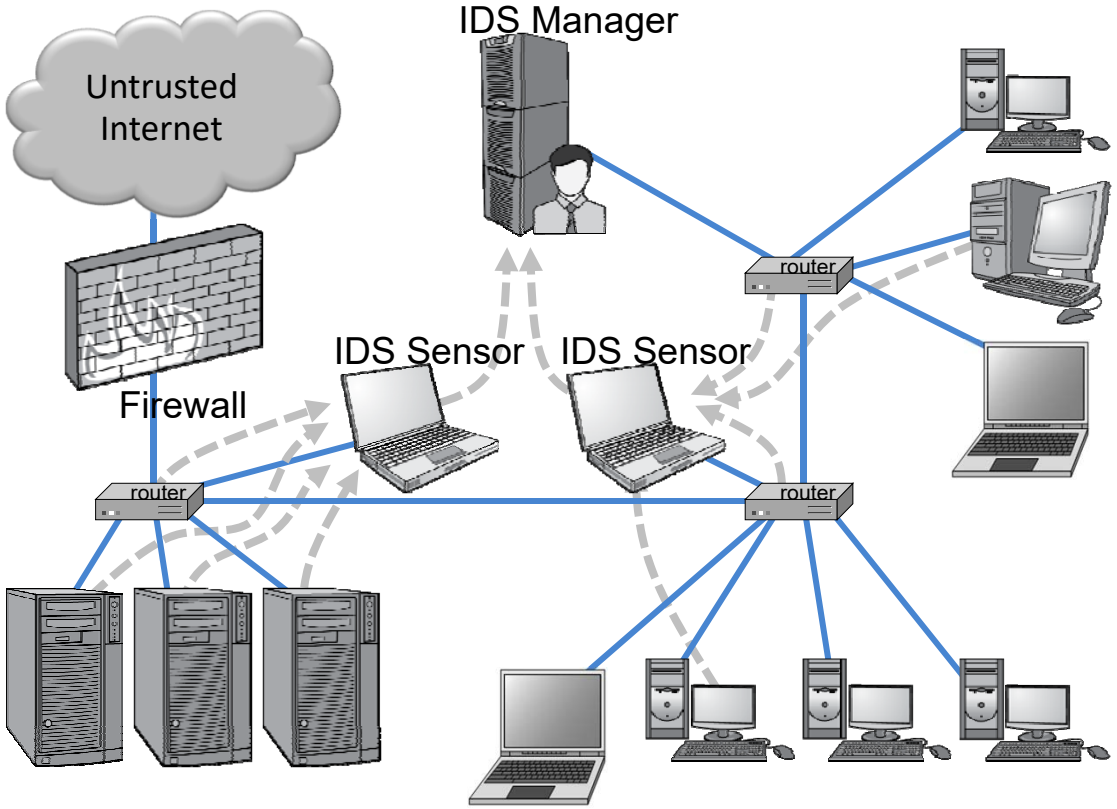
Network Intrusion Detection

Intrusion Detection Systems

- **Intrusion**
  - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing/networking resources)
- **Intrusion detection**
  - The identification through intrusion signatures and report of intrusion activities
- **Intrusion prevention**
  - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

IDS Components

- The **IDS manager** compiles data from the IDS sensors to determine if an intrusion has occurred.
- This determination is based on a set of **site policies,** which are rules and conditions that define probable intrusions.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.

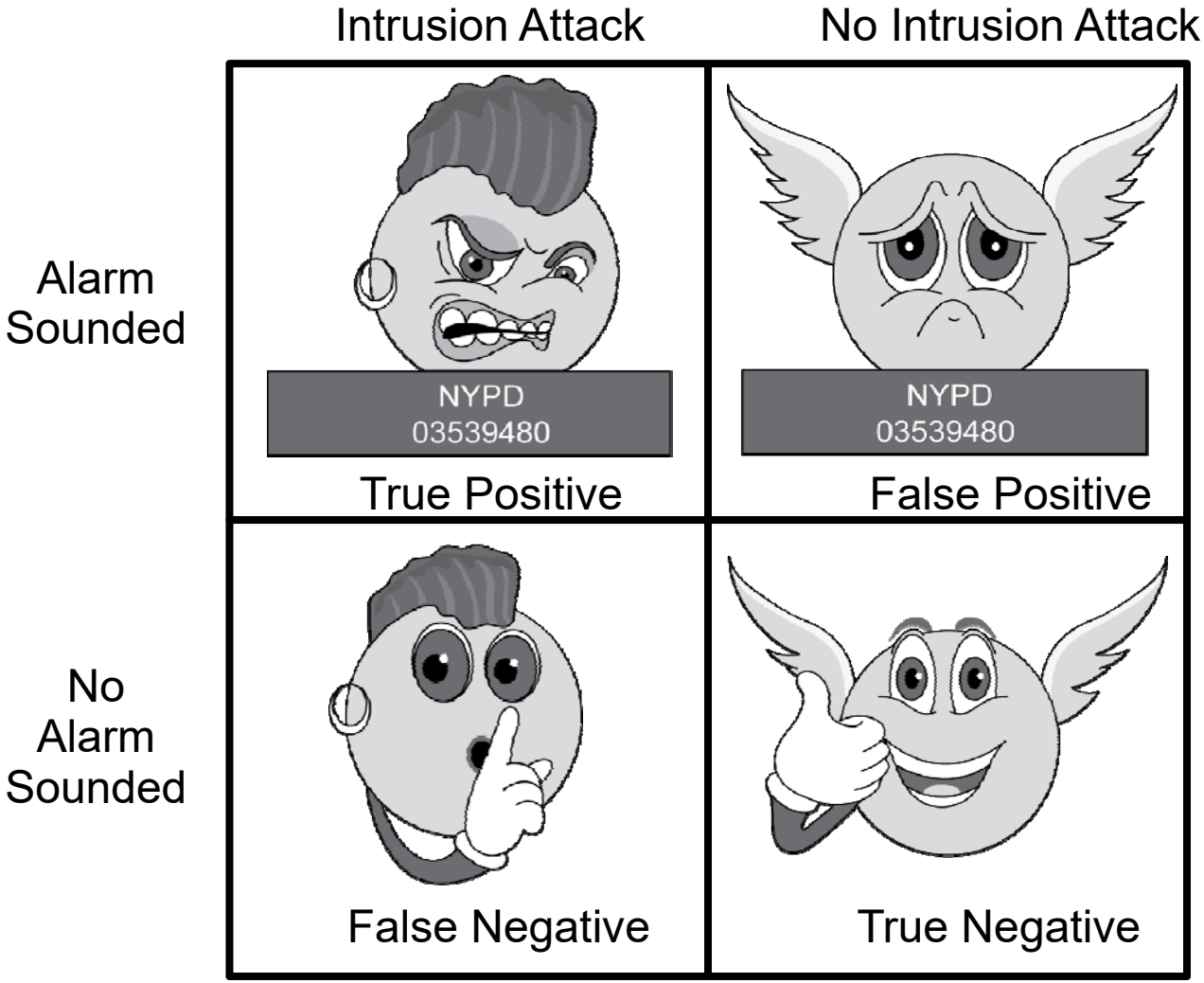


Intrusions

- An IDS is designed to detect a number of threats, including the following:
  - **masquerader:** an attacker who is falsely using the identity and/or credentials of a legitimate user to gain access to a computer system or network
  - **Misfeasor:** a legitimate user who performs actions he is not authorized to do
  - **Clandestine user:** a user who tries to block or cover up his actions by deleting audit files and/or system logs
- In addition, an IDS is designed to detect automated attacks and threats, including the following:
  - **port scans:** information gathering intended to determine which ports on a host are open for TCP connections
  - **Denial-of-service attacks:** network attacks meant to overwhelm a host and shut out legitimate accesses
  - **Malware attacks:** replicating malicious software attacks, such as Trojan horses, computer worms, viruses, etc.
  - **ARP spoofing:** an attempt to redirect IP traffic in a local-area network
  - **DNS cache poisoning:** a pharming attack directed at changing a host's DNS cache to create a falsified domain-name/IP-address association

Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative)



IDS Data

- In an influential 1987 paper, Dorothy Denning identified several fields that should be included in IDS event records:
  - **Subject:** the initiator of an action on the target
  - **Object**: the resource being targeted, such as a file, command, device, or network protocol
  - **Action:** the operation being performed by the subject towards the object
  - **Exception-condition:** any error message or exception condition that was raised by this action
  - **Resource-usage:** quantitative items that were expended by the system performing or responding to this action
  - **Time-stamp:** a unique identifier for the moment in time when this action was initiated

Types of Intrusion Detection Systems

- **Rule-Based Intrusion Detection**
  - Rules identify the types of actions that match certain known profiles for an intrusion attack, in which case the rule would encode a **signature** for such an attack. Thus, if the IDS manager sees an event that matches the signature for such a rule, it would immediately sound an alarm, possibly even indicating the particular type of attack that is suspected.
- **Statistical Intrusion Detection**
  - A **profile** is built, which is a statistical representation of the typical ways that a user acts or a host is used; hence, it can be used to determine when a user or host is acting in highly unusual, anomalous ways.
  - Once a user profile is in place, the IDS manager can determine thresholds for anomalous behaviors and then sound an alarm any time a user or host deviates significantly from the stored profile for that person or machine.

The Base-Rate Fallacy

- It is difficult to create an intrusion detection system with the desirable properties of having both a high true-positive rate and a low false-negative rate.
- If the number of actual intrusions is relatively small compared to the amount of data being analyzed, then the effectiveness of an intrusion detection system can be reduced.
- In particular, the effectiveness of some IDSs can be misinterpreted due to a statistical error known as the **base-rate fallacy.**
- This type of error occurs when the probability of some conditional event is assessed without considering the “base rate” of that event.

Base-Rate Fallacy Example

- Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives. Suppose further…
- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative.**
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That is, roughly 99% of our alarms are false alarms.