Network Security

Summary

Author: Thomas Pettinger

2017–03–02

Network Security
Technische Universität München

Table of Contents

1 Introduction

1.1 Attacks and Attack Detection

Attacks can have different impacts on the target. Disruptive attacks try to fully deny the service (DoS) of the victim whereas degrading ones only occupy parts of the resources. A DoS attack can also executed distributed, a so called DDoS Attackers might also try to gain confidential data or control the target system. Port scans can be used to gain information about the network topology, operating systems and applications or application versions.

To be able to tell if a system is under attack, different measures can be taken at different points in the system.

Host intrusion detection systems (HIDS) are located on the host system. This enables easy detection using information available on the potential victim system but it has to be present on every system (expensive deployment) and the attack actually reaches the victim and is not detected in advance. Network intrusion detection systems (NIDS) lay on the network layer which enables the detection of attacks before they reach the host.

One of the detection methods available is knowledge-based detection. Known signatures of attacks are compared to the actual traffic and if the patterns match an alarm is raised. This only detects known attacks though. To improve this shortcoming, anomaly detection in traffic, protocol or applciaiton behavior can be used. Anomalies can be detected with different metrics in mind. A very simple one might be the number of request, but this does not take legitimate change in traffic into account. A better approach is using cumulative sums which are low if the average is small or whenever only small amounts of values are large but grows if the amount of large values grows in a certain point in time. The disadvantage of anomaly detection though is that oftentimes the rate of false-positives is high.

Detecting attacks is not easy and network monitory often comes at a cost. It is important though especially in large systems when the attack surface grows. The challenge is to find a good compromise between security and performance.

1.2 Attacker Model and Locations

We generally assume the attacker to be (in) the network. They can perform any active or passive attack but cannot break cryptographic primitives. Active attacks are attacks where some influence is measurable e.g. a delay, modifications or replays whereas a passive attack simply stands for eavesdropping messages. This model is called the Dolev-Yao attacker model.

Attackers can be located on different parts of the network and depending on this location different attacks are possible. If the attacker is close to you they are able to perform active attacks like message modifications on you. This can be circumvented by communicating over a secure tunnel though. If the attacker is close to your servers, timing attacks are possible where attackers can measure how long certain operations take to break into the system. The last possibility is that the attacker is somewhere in the Internet. Since the end user has no control over how packets are routed, attackers can modify the path they take for example.

1.3 Security Goals

Data Integrity No improper or unauthorized change of data

Confidentiality Concealment of information

Availability Services should be available and function correctly

Authenticity Entity is who she claims to be

Accountability Identify the entity responsible for any communication event

Controlled Access Only authorized entities can access certain services or information

1.4 Threads

We define a thread in a communication as any possible event or sequence of actions that might lead to a violation of one or more security goals. The actual realization of a thread is then called attack.

Different threads are possible:

- **Masquerade**: An entity claims to be another entity (also called "impersonation")
- **Eavesdropping**: An entity reads information it is not intended to read
- **Loss or Modification of (transmitted) Information**: Data is being altered or destroyed
- **Denial of Communication Acts (Repudiation)**: An entity falsely denies its participation in a communication act
- **Forgery of Information**: An entity creates new information in the name of another entity
- **Sabotage/Denial of Service**: Any action that aims to reduce the availability and / or correct functioning of services or systems
- **Authorization Violation:**: An entity uses a service or resources it is not intended to use