Application of the P2P Model for Adaptive Host Protection

Zoltán Czirkos
Budapest University of Technology and Economics, Hungary

Gábor Hosszú
Budapest University of Technology and Economics, Hungary

INTRODUCTION

The importance of the network security problems comes into prominence by the growth of the Internet. This article introduces the basics of the host security problem, reviews the most important intrusion detection methods, and finally proposes a novel solution.

Different kinds of security software utilizing the network have been described (Snort, 2006). The novelty of the proposed method is that its clients running in each host create a peer-to-peer (P2P) overlay network. Organization is automatic; it requires no user interaction. This network model ensures stability, which is important for quick and reliable communication between nodes. Its main idea is that the network that is the easiest way to attack the networked computers is utilized in the novel approach in order to improve the efficiency of the protection. By this build-up the system remains useful over the unstable network. The first implementation of the proposed method has proved its ability to protect operating systems of networked hosts.

THE PROBLEM OF HOST SECURITY

This section describes basic security concepts, dangers threatening user data and resources. We describe different means of attacks and their common features one by one, and show the common protection methods against them.

Information stored on a computer can be personal or business character, private or confidential. An unauthorized person can therefore steal it; its possible cases are shown in Table 1. Stored data can not only be stolen, but also changed. Information modified on a host is extremely useful to cause economic damage to a company.

Table 1. The types of the information stealth

• An unauthorized person gains access to a host. • Abuse of an authorized user. • Monitoring or intercepting network traffic by someone.

Not only data, but also resources are to be protected. Resource is not only hardware. A typical type of attack is to gain access to a computer to initiate other attacks from it. This is to make the identification of the original attacker more difficult, as the next intruded host in this chain sees the IP address of previous one as its attacker.

Intrusion attempts, based on their purpose, can be of different methods. But these methods share things in common, scanning networks ports or subnetworks for services, and making several attempts in a short time. This can be used to detect these attempts and to prepare for protection.

With attempts of downloading data, or disturbing the functionality of a host, the network address of the target is known by the attacker. He or she scans the host for open network ports, in order to find buggy service programs. This is the well-known port scan. The whole range of services is probed one by one. The object of this is to find some security hole, which can be used to gain access to the system (Teo, 2000). The most widely known software application for this purpose is Nmap (Nmap Free Security Scanner, Tools, & Hacking Resources, 2006). It is important to notice that this is not written for bad intention, but (as everything) it can also be used in an unlawful way.

Modern intrusion methods exert software and hardware weaknesses simultaneously. A well-known example is ARP poisoning. An attacker, already having

gained access to a host of a subnetwork, sends many address resolution protocol (ARP) packets through its interface. This causes network switches to enter hub mode, resulting in every host on the subnetwork being able to see all traffic, also packets addressed to other hosts. The traffic can then be analyzed by the attacker, to gain passwords or other data. Therefore, to detect modern, multi-level intrusions, a single probe is not enough (Symantec Internet Security Threat Report, Volume III, 2005).

THE INTRUSION DETECTION

Computer intrusion detection has three following main types:

- Traffic signatures (data samples) implying an intrusion,
- Understanding and examining application level network protocols, and
- Recognizing signs of anomalies (non-usual functioning).

Unfortunately, not every attack is along with easily automatically detectable signs. For example the abusing of a system by an assigned user is hard to notice.

The oldest way of intrusion detection was the observation of user behavior (Kemmerer & Vigna, 2002). With this some unusual behavior could be detected, for example, somebody on holiday still logged in the computer. This type of intrusion detection has the disadvantage of being casual and non-scalable for complex systems.

The next generation of intrusion detection systems utilized monitoring operating system log files, mainly with Unix type operating systems. Many security utilities realize this method, the well-known *Swatch* (*S*imple *WATCH*er for logfiles) (2006), are one of these. Finding a sign of intrusion in a log file, Swatch can take a predefined step: starting a program, sending an e-mail alert to the administrator, and so forth. Of course this is not enough to protect a system, because many types of intrusions can only be detected too late.

To understand modern intrusion detection, it must be concluded that the detection system does not observe intrusions, but the signs of it. This is the attack's manifestation (Vigna, Kemmerer, & Blix, 2001). If an attack has no, or only partial, manifestation, the system cannot detect the intrusion. One good example to help understanding this is a camera with a tainted lens, which cannot detect the intruder even if he or she is in its field of vision.

Data Acquisition

For accurate intrusion detection, authorative and complete information about the system in question is needed. Authorative data acquisition is a complex task on its own. Most of the operating systems provide records of different users' actions for review and verification. These records can be limited to certain security events, or can provide a list of all system calls of every process. Similarly, gateways and firewalls have event logs of network traffic. These logs may contain simple information like opening and closing network sockets, or may be the contents of every network packets recorded, which appeared on the wire.

The quantity of information collected has to be a trade-off between expense and efficiency. Collecting information is expensive, but collecting the right information is important, so the question is which types of data should be recorded.

Detection Methods

Supervising a system is only worth this expense if the intrusion detection system also analyzes the collected information. This technology has two main types: anomaly detection and misuse detection.

Anomaly detection has a model of a properly functioning system and well behaving users. Any deviation it finds is considered a problem. The main benefit of anomaly detection is that it can detect attacks in advance. By defining what is normal, every break of the rules can be identified whether it is part of the threat model or not.

The disadvantages of this method are frequent false alerts and difficult adaptability to fast-changing systems.

Misuse detection systems define what is wrong. They contain intrusion definitions, alias signatures, which are compared with the collected supervisory information, searching for the signs of the known threats.

An advantage of these systems is that investigation of already known patterns rarely leads to false alerts. At the same time, these can only detect known attack methods, which have a defined signature. If a new kind