Peer-to-Peer Methods for Operating System Security

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 with the growth of the Internet. This article presents a special approach to the *intrusion detection* (ID) problem, which relies on the collaboration of the protection programs running on different hosts. Computers connected to networks are to be protected by various means (Kemmerer & Vigna, 2002). The collaboration of the elements of the proposed intrusion detection system uses the so-called *peer-to-peer* (P2P) communication model. The article first presents the usage of the P2P paradigm for improving the protection of the operating systems (Bauer, 2005).

In the following sections the most important intrusion types and the developed intrusion detection methods are introduced. Intrusion attempts, based on their purpose, can be of different methods, but these techniques share things in common, for example, scanning networks ports or subnetworks for services, and making several attempts in a short time. This property can be used to detect these attempts and to prepare for protection.

An attacker may be looking for sensitive data as well as resources. One common scenario for an attack is scanning many "neighboring" hosts, a network address range in a local area network for some security flaw or bad configuration. This is known as a *portscan*.

One of the most important properties of these intrusion attempts is that many hosts are usually under attack by a single attacker. In particular, this fact can also be used to create defense. If a host, whose protection was strong enough to defend its own operating system, could send an alert to the other hosts, those could prepare themselves for the attack in advance, and could improve their protection, for example, by installing the necessary software. The novel application of P2P theory is easy to use; the nodes organize the P2P overlay automatically, and do not need any user interaction. The developed system is named *Komondor*, which is a very reliable Hungarian guard dog.

The article demonstrates the effectiveness of the novel system and shows the roadmap for further development, too.

THE PEER-TO-PEER COMMUNICATION

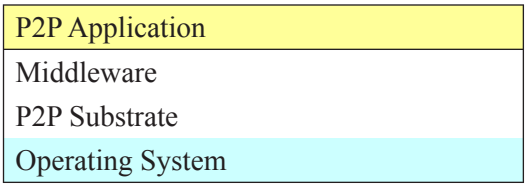
In order to demonstrate the P2P overlay network used in the proposed intrusion detection method the theory and the latest results of P2P networks are reviewed in this section.

The P2P communication model is old in computing, its first example was the Usenet system. The Usenet has no central control. It is similar to a mailing list to some extent. It is mainly used by software developers and beginners to share their knowledge. This system relies on newsgroup servers, which are connected virtually to each other and exchange messages at specific time intervals. The difference between the Usenet and the current P2P systems is that the Usenet applies dedicated servers in each organization, whereas the current P2P applications use the hosts as servers to share their resources.

Theory of P2P and grid networks has gone through a great development since the most recent years. Both of them consist of peer nodes; however, usually registered and reliable nodes connect to a grid, while P2P networks can tolerate unreliability of nodes and quick change of their numbers (Uppuluri et al., 2005). The important parts of an application implementing a P2P overlay network can be seen on *Figure 1* (Hosszú, 2005).

In *Figure 1*, the layer "P2P Substrate" is responsible for the creation and the maintenance for the overlay network, while the task of the "P2P Application" layer is communication. The optional middleware layer has

Figure 1. The protocol stack of a peer-to-peer application



auxiliary functions, for example, the selection of reliable peers in order to enhance connectivity and the quality of the application. Tasks of P2P substrates can usually be divided into four groups:

- **Routing:** Sending data to a particular node
- **Lookup:** Finding a node containing some particular data
- **Replication:** Controlling how data should be stored redundantly
- **Overlay management:** Maintaining the overlay network

P2P computing has many advantageous properties, such as load-balancing, availability, fault tolerance and self-organization (Li & Vuong, 2004). The majority of the current overlays are loosely controlled; they have a decentralized organization. Nodes can be easily missing, the network can flexibly manage network failures and peers are constantly entering and leaving the overlay. The usual lookup is also done by the peers, by forwarding search queries to each other.

Overlay networks of this type are Gnutella (Gnutella, 2006), Freenet (Freenet Project, 2006) and FastTrack (FastTrack, 2006). Systems like Gnutella and FastTrack are constructed for the heterogeneous Internet environment, where the availability of the nodes is not guaranteed. The main properties of such systems are simplicity, robustness, and low requirement for network topology. Usually a file exchange program is also built in the application, together with the P2P substrate. KaZaA and Morpheus are one of these (Morpheus, 2006).

In order to improve the performance of P2P overlay systems, the theory of scale-free networks (Albert & Barabási, 2002) is used. A network is scale-free if there is no single characteristic scale as measured by node degree—number of links per node (Silvey & Hurwitz, 2004). Opposite of the scale-free networks is the category of random networks, which have degree distributions with a central tendency. In the case of scale-free networks most of the nodes have few links, whereas a few nodes have a lot of links. The scale-free network can develop if the network grows in a bottom-up fashion, where the joining new nodes exhibit a preferential attachment bias in selecting their neighbors. Such networks are usually the P2P overlays. However, real world P2P networks have partly scale-free and partly random graph properties.

The more scale-free a P2P overlay is, the more efficient is its lookup functionality (Albert & Barabási, 1999). Scale-free networks usually show the "small-world phenomenon," which means that any two nodes in a scale-free network are interconnected with a very few number of links, typically five or six, even in the largest P2P networks in practice. This means that any two nodes are likely to be relatively close to each other via some path in the overlay. The scale-free property is usually a desired one for a P2P overlay, also for the proposed intrusion detection system, Komondor.

THE INTRUSION DETECTION

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

We have to protect not only our data, but also our resources. Resource is not necessarily hardware. A typical type of attack is to gain access to a computer to initiate other attacks through it. This is to make the identification of the attacker more difficult, because this way the next intruded host in this chain sees the IP address of previous one as its attacker.

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. *Data integrity* must therefore be always monitored.

The *integrity of a computer system* means that the host behaves and works as its administrator intended it to do so. The attacker can alter or obstruct its functioning properly, likewise to cause damage.

The attacker is able to find resources through the security holes. With this type of action whole ranges of network addresses are scanned for a particular service