Chapter 8.13
A Novel Application of the P2P Technology for Intrusion Detection

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 come into prominence by the growth of the Internet. This article presents a new kind of software that uses the network itself to protect the hosts and increase their security. The hosts running this software create an application level network (ALN) over the Internet (Hosszú, 2005). Nodes connected to this ALN check their operating systems' log files to detect intrusion attempts. Information collected this way is then shared over the ALN to increase the security of all peers, which can then make the necessary protection steps, for example, blocking network traffic by their own *firewall*.

Different kinds of security software utilizing the network were also written previously (Snort, 2006). The novelty of Komondor is that its client software entities running in each host create a *peer-to-peer* (P2P) *overlay network* (Czirkos, 2006). Organization is automatic; it requires no user interaction. This network model ensures stability, which is important for quick and reliable communication between nodes. By this build-up, the system remains useful over the unstable network.

THE IMPORTANCE OF THE P2P COMMUNICATIONS

The Internet-based communication technology enabled people to share information with anybody in seconds. This has brought benefits to people spanning many spheres from social services to education (Frasz, 2005). Probably the best example of such extended network of content sharing is the P2P that allows users to download media files off other computers free of charge. Once content enters the Internet, it can be downloaded by an unlimited number of people.

One of the latest steps in the steady advances in P2P technologies is the release of new P2P technologies in 2005 that enable a user community to filter out mislabeled or corrupt files (Goth, 2005). One approach to build a more trustworthy P2P overlay is the application credence (Sirer & Walsh, 2005). It rates a certain network object instead of a given peer node for trustworthiness. The reason is that nodes can be inhabited by various people over time, but the data in the object itself does not change. This system uses a secure and anonymous voting mechanism. Over time, users with similar votes or the legitimacy of a file will dynamically form a kind of community enabling enough correlation of trust. Similarly, a user that systematically answers contrarily will get an equally significant negative weighting; however, an inconsistent voter will have less statistical weight. In such a way, the more users who join credence overlay, the more accurate an overall rating each file will receive.

The trend of the P2P systems is building more resilient services. Centralized solutions are fragile, since a single link breakage in the network can cut access to the whole service. P2P enables higher ability to construct overlays that self-organizes and recovers from failures.

Another interesting and important feature of the development process of the P2P technology is that the most successful projects are open sources such as LimeWire, which is a Gnutella client with rapidly growing popularity (Bildson, 2005). Its business model has two sides. One version is free, however, advertising-supported, and the other is ad-free, but the users must pay for it. LimeWire guarantees no bundled software with downloads. The open source property of the LimeWire encourages its users to monitor its development. The largest competitor of LimeWire is BitTorrent, which is very efficient in sharing large files (BitTorrent, 2006). Its users upload portions of required documents to a requester instead of forcing one client to upload the whole file many times.

THE PROBLEM OF THE INTRUSION

Computers connected to networks are to be protected by different means (Kemmerer & Vigna, 2002). Information stored on a computer can be personal or business character, private or confidential. An unauthorized can person can therefore steal it; its possible cases are shown in Table 1.

We have to protect not only our data, but also our resources. Resources are not necessarily hardware only. Typical types of attack are to gain access to a computer to initiate other attacks from 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 the previous one as its attacker.

Stored data can not only be stolen, but changed. Information modified on a host is extremely useful to cause economic damage to a company. The attacker can alter or obstruct its functioning properly and cause damage.

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

Table 1. The types of the information stealth

- An unauthorized person gains access to a host.
- Monitoring or intercepting network traffic by someone.
- An authorized but abusive user.

Related Content