E-Collaboration Enhanced Host Security

Zoltán Czirkos
Budapest University of Technology and Economics, Hungary

Gábor Hosszú
Budapest University of Technology and Economics, Hungary

Ferenc Kovács
Budapest University of Technology and Economics, Hungary

INTRODUCTION

The importance of the host security problems come into prominence by the growth of the Internet, since the network means a breaking point to the intruders (Wang, Jha, McDaniel, & Livny, 2004). The article presents the e-collaboration related security questions, the main concepts of the ***intrusion detection*** and the different classes of the system protection methods.

As an example of the application for non-conventional purposes, a security system is presented in the article that utilizes just the network for protecting the operating system of the computers. The software maintains a database about the experienced intruding attempts. Its entities working on each computer share their experiments among each other on the *peer-to-peer* (P2P) overlay network created by self organizing on the Internet. In such a way the security of the participants is increased, and then they can take the necessary steps.

BACKGROUND

Currently the *application-level networking* (ALN) has increasing importance. In this communication technology the applications running on host directly create connections among them and they use these connections in order to exchange information and packets. Their communication way is different from the more traditional networking model, where the communicating software entities create connections among them for solving certain task (e.g., downloading a file). In case of the ALN the applications produce more stable virtual network, called *overlay*, which can be used complex file-management and application level routing functionalities (e.g., making *application-layer multicast*; ALM). The ALN overlays use typically the P2P communicating model oppositely to the more traditional *Client/Server* model (Hosszú, 2005).

A special kind of the P2P networking is the Grid-computing (shortly Grid), where the registered participants actively collaborate to produce new results (Uppuluri, Jabisetti, Joshi, & Lee, 2005). The notion of a Grid has gained popularity as a metaphor and guiding principle for system architectures designed to permit large-scale resource sharing across widespread heterogeneous collections of systems (Foster, Kesselman, & Tuecke, 2001). An important feature is the notion of a dynamic Virtual Organization (VO) in which a collection of individuals or organizations share resources in an ad hoc way for a period of time, with minimal effort required to set up or finalize the organization (Martin & Cook, 2004).

It has been clear that careful consideration of security issues is central to the successful deployment of Grids. Potential resource providers will be reluctant to participate if the possibility of misuse of their resource is too great; potential customers will not use Grid services if they cannot achieve an adequate guarantee of quality of service (QoS)—including integrity, confidentiality, and availability (Martin & Cook, 2004).

Although Internet connections are now almost ubiquitous, and of very low cost, different applications and organizations find good reasons to employ leased private networks. They may use the Internet protocol (IP) for their implementation, in such a way virtual private network (VPN) can be realized. VPNs can also be used to link separate sites, by use of private leased lines, so that network traffic may travel over a long distance as if it were within a single site. Multinational corporations implement internal networks in this way; the long-distance links may be well-protected, but the

attached nodes are necessarily more accessible (Martin & Cook, 2004).

To the end user, VPNs are something of a marvel. They allow a roaming device—a laptop or a personal digital assistant (PDA)—using any Internet connection to behave as if it were part of their home corporate network, apparently on the inside of any firewall protection, and with potentially full access to sensitive network data and resources. Moreover, this solution is completely sanctioned and even supported by their system and network administrators. Those administrators are also able to use a VPN to connect remote sites using the Internet. Although the traffic travels over the public IP network, the encryption prevents clear-text eavesdropping or tampering (Martin & Cook, 2004).

In order to use a VPN over each connection between a user and a resource node, a potentially enormous number of VPNs will be needed, with associated key management challenges for each. This will almost certainly render the enterprise unmanageable. Even a model in which only the Grid nodes (compute, data, broker, and other resource) participate, VPNs will exhibit an exponentially rising set-up cost for adding new nodes (Martin & Cook, 2004).

The VPN itself cannot provide perfect security. Whilst VPNs support strong encryption of data over a shared medium, they do not provide complete undetectability of activity. It must be noted that VPNs do not attempt to shield the presence of users within the network, or hide identity of endpoints and hosts, the types of data, and the frequency of data exchanges. If the primary uptake of VPNs within Grid infrastructures is to provide security, the designers of such Grids must be aware of the above vulnerabilities.

To address the problem of traffic snooping within VPNs, an accepted form of defense is the use of a single IPSec channel between VOs, as described in Herscovitz (1999). This provides a degree of secrecy and a degree of immunity to traffic analysis, but as illustrated in Cohen (2003), single IPSec channels between endpoints are sometimes not possible.

Based on the reviewed properties of the networking technologies of the e-collaboration it can be stated that a single solution has not solved the problem. The host-based and the network-based intrusion detections are equally important. In the followings the various intrusion detection methods will be analyzed.

THE INTRUSION DETECTION

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. Stored data can not only be stolen, but changed. Information modified on a host is extremely useful to cause economic damage to a company.

Resources are also to be protected. Resource is not only hardware. 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.

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.

With attempts of downloading data, or disturbing the functionality of a host, the network address of the target is known by the attacker. He 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, 2006).

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.

Next generation intrusion detection systems utilized monitoring log files, mainly with Unix type operating systems. Of course this is not enough to protect a system, because many types of intrusions can only be