Chapter 2.28
Potential Security Issues in a Peer-to-Peer Network from a Database Perspective

Sridhar Asvathanarayanan
Quinnipiac University, USA

ABSTRACT

Computing strategies have constantly undergone changes, from being completely centralized to client-servers and now to peer-to-peer networks. Databases on peer-to-peer networks offer significant advantages in terms of providing autonomy to data owners, to store and manage the data that they work with and, at the same time, allow access to others. The issue of database security becomes a lot more complicated and the vulnerabilities associated with databases are far more pronounced when considering databases on a peer-to-peer network. Issues associated with database security in a peer-to-peer environment could be due to file sharing, distributed denial of service, and so forth, and trust plays a vital role in ensuring security. The components of trust in terms of authentication, authorization, and encryption offer methods to ensure security.

INTRODUCTION

Over the last few years, the world has witnessed the explosion of Internet technology and the rapid growth in the use of peer-to-peer-based applications. The open nature of peer-to-peer networks and the decentralized administration and management of resources make it flexible for servents to operate in complete autonomy, thereby allowing them to freely participate or withdraw from the network without disclosing their true identity. While this can be considered as one of the salient features of a peer-to-peer network, the same can also be viewed as an inherent vulnerability

built into these networks as they open up issues related to servent trust and security. The threat to database security, due to inherent vulnerabilities in the product and network, is further amplified when considering database implementations on a peer-to-peer network. While it is essential to discuss the security issues pertaining to peer-to-peer networks in general, it is equally vital to discuss the security issues pertaining to databases in a peer-to-peer network. This paper focuses specifically on database-related security issues in a peer-to-peer environment. The examples discussed are centered on Windows and UNIX environments, but the concepts can be applied to other environments as well.

There has been a growing trend towards using peer-to-peer networks for serious business purposes and for enterprise computing, and hence the need to analyze these security issues receives greater importance. The concept of enterprise peer-to-peer technology is evolving and, over time, it is predicted by observers that distributed data spread across peer-to-peer networks and stored on desktops and other computing devices in various locations where an enterprise operates are likely to replace centralized databases. There are also predictions on the rise of companies thinking in terms of corporate infrastructures that share the characteristics of peer-to-peer and client-server networks (Zeiger, 2001). It is not uncommon for companies that do not have a strong information security policy to have databases residing on departmental servers spread across the organization in various departments rather than being managed centrally by a data center. Most medium-sized companies find the decentralized approach more flexible as each department can be made responsible for its own operational applications, data, and security. The departments, too, enjoy this autonomy. The concept of enterprise peer-to-peer networks are built around this basic premise and the databases being stored and accessed in such peer-to-peer networks are subject to greater security concerns. Database systems, no matter how carefully designed and implemented, are constantly being exposed to security threats in various forms, such as denial of service and worm attacks. Peer-to-peer networks in general are prone to worm and denial of service attacks and with some of the existing vulnerabilities associated with databases, these networks, when they host corporate databases are likely to be an easy target for hackers. Due to the frequent discovery of new vulnerabilities associated with either the networks or with the security architecture of the database management systems, the whole activity of security administration and data management is turning to be a challenge rather than a routine function.

As the placement of data transitions from centralized servers to a distributed peer-to-peer network, the challenge of securing data is only likely to get even tougher. The administration and control of security was centralized when mainframe systems were used to store and manage all corporate data for an enterprise. All data needs of the organization were satisfied by the centrally stored database and there was neither the need to connect outside the corporate network to access data nor the necessity for interaction between host nodes in a distributed network to exchange data. With the emergence of client-server computing, the approach went a little more decentralized allowing users to connect to any data sources available on the corporate network (Zeiger, 2001). As the business processes got more demanding and the need to access and process data outside of the company started becoming more critical to the success of the enterprise, network access started to reach beyond the organization's domain, thus exposing the corporate network to higher risks of security. With the slow but certain evolution of enterprise peer-to-peer technology, organizations have started looking more outward for their data needs and eventually there is a compelling need for security administrators to better understand the associated issues with data security.