Peer-To-Peer Security

MOHD ASRI BIN MOHAMAD STAMBUL
UNIVERSITI KEBANGSAAN MALAYSIA
Bangi , Selangor
Email: mdasri.stambul@yahoo.com

Abstract

The abstract goes here.

1. Introduction

Peer-to-peer systems (P2P) have grown in importance over the last 5 years as an attractive way to mobilize the resources of Internet users. As more and more users have powerful processors, large storage spaces and fast network connections, more actors seek to coordinate these resources for common goals. Because of their unique decentralized nature, security in these systems is both critical and an interesting problem. How do you secure a dynamic system without central coordination? Good security on P2P systems must reflect the design goals of the system itself. In this chapter, we introduce some basic concepts for P2P systems and their security demands, and then discuss several case studies to highlight issues of robustness, privacy, and trust. We analyze systems that offer secure distributed routing, privacy-enhancing and censorship-resistance publishing, shared storage and decentralized collaborative work spaces. We conclude by examining how accountability and trust mechanisms must be built into a secure system.

mds
January 11, 2007

1.1. ABOUT PEER-TO-PEER SYSTEMS What is P2P

Peer-to-peer systems have two dominant features that distinguish them from a more standard client-server model of information distribution: they are overlay networks that have unique namespaces. P2P systems link different, possibly heterogeneous systems as peers, and allow them to interact on top of existing network configurations. It does this by defining relationships unique to that system, usually in the form of a topology by which systems are linked. Occasionally a system will piggyback atop an existing namespace, such as the IP/port labeling, but still treats these separately from the Internet-layer protocols. The combined effect of independent systems interacting through a unique namespace is decentralization. Not every system generally considered a P2P system is strictly decentralized in managementhe infamous Napster actually ran through a centralized serverbut the matter of decentralization brings out important concerns for system security. Although they have won the most attention for their roles as (often illicit) file-swapping networks, peer-to-peer systems can serve many functions, and design considerations must reflect these. One proposed use of a P2P system was that of shared expertise. A Gnutella pioneer has suggested that the system could be used to propagate queries of any sort through a network until a peer felt that it could respond to the query, anything from a lexical look-up to a specialized calculation (Kan, 2000). In a network with varied resource availability, P2P systems have been used to distribute those resources to those who need or want them the most. The shared resources in question are usually computation or storage. This can create efficient resource usage, given a low marginal cost of using a resource not otherwise needed. Beyond sharing computation power for enormous tasks, P2P networks have been proposed as an escrow system for digital rights management, or for distributing searches across a wide range of other peers. A new class of business software systems known as groupware uses many P2P principles. Groupware networks are closed networks that support collaborative work, such as the Groove network discussed below. Finally, the decentralized nature of peer systems offers many positive features for publishing and distribution systems, not least of which is their resilience to legal and physical attacks and censorship. P2P architectures have many different functions, and different functions lead to different design conclusions, with respect to overall system structure, and specifically to security issues.

1.1.1. Subsubsection Heading Here. Subsubsection text here.

2. Conclusion

The conclusion goes here. this is more of the conclusion

Acknowledgment

The authors would like to thank... more thanks here

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.