Evaluating Security Mechanisms in Peer-to-Peer Applications

Manish Parashar Manish Agarwal Steele Arbeeny Viraj Bhat Rangini Chowdhury
Department of Electrical and Computer Engineering
Rutgers University
94 Brett Road
Piscataway, NJ 08854-8058 USA
{parashar, manishag, arbeeny, virajb, rangini}@caip.rutgers.edu

Abstract

Many different kinds of peer-to-peer applications are in use today. Some allow inter-person communication, such as video and text messaging, while others provide data sharing capabilities. Some also function as large virtual computers, providing distributed compute services to a central source. One major difficulty in developing these systems is the selection of an appropriate security mechanism from the wide array of available technologies. In this paper we discuss three common peer-to-peer application areas, and evaluate several different security enabling technologies with the aim of assisting the application developer in selecting a suitable one that satisfies the requirements. Data on these security technologies, and their performance in different application scenarios, is gathered using real-world applications, simulation, and results of related research. Results are presented in a simple table that allows developers to easily match up an application related security requirement with the most suitable enabling technology.

1. Introduction

Peer-to-peer applications have been gaining in popularity ever since Napster caught the recording industry by surprise, and allowed individuals to trade in the precious commodity of music – a right previously reserved for the privileged few. The empowerment felt by users of this program helped fuel the development of many other projects that have similar goals. [1] One important area that must be evaluated when developing peer-to-peer applications is that of security. In decentralized applications, security is much more than simple user authentication. It must provide source verification and data integrity services, as well as intellectual property rights management. All this is in addition to more mundane authentication services. Of course, all of these operations must be implemented with an eye towards conserving network bandwidth and other resources. A major difficulty in designing security for peer-to-peer applications is to decide which security enabling technologies are best suited for the application.

In this paper we study three peer-to-peer application categories that will have elements in common with most popular peer-to-peer applications, both existing and under development. These categories are: distributed file sharing, real-time communications and distributed computing. The general security requirements of each application type are then discussed. The properties of several common security enabling technologies such as public key cryptography, smart cards and steganography are measured based on real-world applications, simulation, and results of related research. This information is then related back to the original applications, with the goal of determining the pros and cons of using a given enabling technology in a particular application scenario. Finally, a simple matrix that can aid application developers in selecting the most appropriate security technology, or combination of technologies, is presented.

2. Application Categories

After an analysis of the security requirements of peer-to-peer applications, one will determine that a few representative categories cover enough of the requirement space so that a large set of applications can be characterized by this smaller set.

2.1. Distributed File Sharing

A distributed file sharing application, like the popular LimeWire or Morpheus, allows users to search for and retrieve files based on a wide array of criteria. Some of these files might be copyrighted material, or available only to subscribing members. For these reasons, the security framework in a file sharing application must provide some method for digital rights management. Watermarking would be desirable, so that unauthorized duplication could be detected, but it is not a strict requirement that the source of the file be verified if these previous requirements are satisfied. Further, the security information must be processed at interactive, or nearly

interactive rates. A moderate increase in the size of the data is acceptable, as is a moderate increase in bandwidth usage since it is assumed that these applications will run on the desktop. Enabling technologies that require special purpose hardware should be avoided in this type of application.

2.2 Real-Time Communications

This application category covers chatting and instant messaging applications, as well as video and telephony based communications. They require strong encryption with source verification so the sender of a message can be verified along with the message integrity. Messages need not be encrypted uniquely for each receiver, and should be able to be decoded at interactive rates. Special purpose hardware is acceptable as long as the cost is very low.

2.3 Distributed Computing

A distributed computing application sends out segments of a large data set for processing on remote systems. These applications generally require source and message integrity verification. However, since they will be processing a significant data set, the decoding need not be in real-time. Generally, watermarking is not required since the data will not be distributed.

3. Security Enabling Technologies

Each of the popular security technologies being evaluated in this paper, namely public key cryptography, smart cards and steganography, each are specially suited to securing data in certain ways. Some of these technologies rely on encryption, and others rely on hiding security information directly in the data.

3.1. Cryptography

Cryptography is used to encrypt messages sent between two communicating parties so that an eavesdropper will not be able to decode them. There are several accepted methods for implementing cryptography, and popular ones, such as public key cryptography, rely on the difficulty in factoring the product of large prime numbers. They are very useful in peer-to-peer systems because they can uniquely protect a message for an individual recipient, and verify its integrity. It can also be used to set-up secure, virtual communications channels between peers using a third-party network such as the Internet. A major drawback is the processor resources required to perform arithmetic on huge numbers. This can be addressed with special purpose hardware, but the expense is significant. We will use public key cryptography to satisfy many security requirements such as message security and integrity, and digital rights management.

3.2. Smart Cards

Smart cards are plastic cards, similar to credit cards, that contain an integrated circuit chip resulting in information storage capacity, and processing power that is not available in magnetic stripe cards. Coupling the microprocessor with a reader provides the card with the power to serve different applications. They are useful as access-control devices, incorporating encryption and authentication, making data available only to authorized users. For peer-to-peer networking, smart cards allow safer and easier management of diverse networks minus the significant costs for access control. Along with data portability and security they are also convenient. A single card be used for personal identification and also have other functionalities integrated into it.

3.3. Steganography

Steganography is the process of hiding security information within the data as opposed to encryption, which aims to make the data unreadable to unauthorized viewers. It is very useful because it can provide data with a unique identity embedded directly in the information. This process is known as watermarking, and can be used to track duplications and carry intellectual property information along with the protected data. This technology will be evaluated for its usefulness in peer-to-peer applications, and compared to the other enabling technologies.

4. Evaluation Process

Security enabling technologies will be evaluated in several ways. Different cryptography and steganography algorithms will be used to implement application specific security services in a simulated peer-to-peer network. The complexity, performance and strength of each of these algorithms, along with the results of related research, will be used to determine their success at satisfying the requirements. Smart cards will be evaluated through the use of case studies and literature surveys to determine the security requirements they can satisfy.

5. Bibliography

[1] Udell, J., Asthagiri, N., Tuvell, W., “Security”, *Peer-To-Peer: Harnessing the Power of Disruptive Technologies*, Oram, A. – Editor, O’Reilly & Associates, 2001