A STUDY ON PEER TO PEER ENCRYPTED FILE SHARING IN A ADHOC NETWORK

Sharan*, S.Palaniappan

UG student, Department of Information Technology, Saveetha School of Engineering, Chennai, India.
Associate Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Chennai, India.

Email: sharanragesh@hotmail.com

Received on 10-08-2016
Accepted on 06-09-2016

Abstract:

Today there are a lot of social networking services are available on the internet. Many more peer-to-peer (P2P) social networks are coming into existence in these networks the user’s data is often stored in semi-trusted and untrusted locations hence there is a need of very efficient encrypting algorithm and technique. This paper discusses various encryption techniques available for peer-to-peer file transfer.

Keywords: Peer to peer, Networks, Encrypting.

I. Introduction:

In a traditional computer network few services are used to provide multiple services in the network. In a peer to peer network the process of providing the various services available in the network is handled by each of the peer or nodes in that network. Hence each node in the network acts as both the client and server. Technically a peer-to-peer is a self-organised network with a symmetric communication and a distributed control system. These networks don’t have a central storage system. Peer to peer networks pools the resource of all the peers in its network. Since there is no central resource or storage location in a peer to peer network they are open to attacks like denial of service, contamination of the network and the personal information of the peers in the network being compromised.

The concept of peer to peer networks was first established in 1969. It was then known as host to host connection. The first implementation of peer to peer network was Usenet in 1979 the client can access the resources through servers which is connected to other servers in manner similar to that of a peer to peer network these servers send messages to other servers on demand without any central authority.

Peer to peer networks has gained popularity since the 1990s they were used in file sharing applications to send multimedia files. Free net, Napster, Direct Connect, Gnutella, eDonkey2000, Bit Torrent are some popular high
profile file sharing protocol. Since peer to peer networks rely on other peers major security threats arise as the trust between the peers is exploited and all the internal data in these peers are exposed in the pretext of distribution of workload. Encryption is essential to provide security and privacy to each of the peers in the network.

Privacy and identity of the peers in the network is sometimes compromised by the fellow peers who help in the transmission of data. Even though the data to be sent is encrypted. The peer carrying the data packet in the network now has direct access to the encrypted data packet so there is always a need for a very efficient algorithm and technique for the encryption of the data being sent through these networks. One more issue faced in these networks is the lack of anonymity, in some file sharing systems that rely on peer to peer networks the IP address of the each peer is exposed to peers downloading the same file. This makes that particular peer to be vulnerable to more attacks.

Encryption of the data being transmitted in a peer to peer network is important not just to keep the data safe but to also encrypt the data stream making it difficult to detect the traffic in the network which helps reduce the chance of being attacked, blocked or throttled.

Anonymizing peers in a peer to peer network helps in protecting the identity of nodes and the users on the network. this is something that cannot be achieved using only encryption. This can be done by making all the peers universal senders and receivers making it difficult to identify if the is peer is sending, receiving or just passing the data.

Network that is encrypting and anonymous peer to peer network will result in one of the most secure peer to peer experience available today.

II. Literature Survey:

Encryption for Peer-to-Peer Social Networks

Oleksandr Bodriagov[1] and Sonja Buchegger[1] discuss the need for encryption in a peer to peer network and the need for the encryption to efficient in terms of space and time it requires. They propose to use BE schemes with high performance encryption and decryption techniques to have an efficient encryption based access control environment in a peer to peer network

A Survey of Peer-to-Peer Network Security Issues

James li[2] discusses the basics of a peer to peer network and some attacks and issues faced by it. Most of these issues and attacks faced by these networks is due to the lack of a central administration. Encrypted and anonymous peer to peer network can protect the network from certain attacks and resolve almost all privacy and usage issues faced by these peer to peer networks. Protection against direct attacks in a peer to peer network can only be
implemented only by careful design and protocols.

Applying XML Signature and XML encryption in Peer to Peer Platform Security

Takeshi kato[3], Hiromitsu sumino[3], and Norihiro Isikawa[3], talk about the several general purpose peer to peer platforms and it is importance to provide appropriate security services for the application. For this we have to choose appropriate security mechanism and protocols depending on the characteristics and performance of the peer to peer network. In this paper they propose to use XML signatures and XML encryption to the security architecture

A Novel Stochastic-Encryption-Based P2P Digital Rights Management Scheme

Majing Su[4], Hongli Zhang[4] discusses about the protecting of the rights of each peer in the network using stochastic encryption. They propose that using this method they will encrypt the files in such way that only the end user can view the file and they use the random characteristics of the peer to peer networks to increase the key space to prevent collusion attacks and also has a piece validation policy to prevent poisoning attacks.

III. Requirements for Peer to Peer Encryption

The absence of trusted parties in a peer to peer network has imposed many security limitations on the encryption-based access control system. For a positive user experience it is essential that all actions are executed at a very fast rate. This part of the paper discusses the security constrains and the requirements for encryption systems.

Efficiency

In the accustomed centralized access control the security subsystem authenticates the user and enforces behaviour accustomed by access control lists (ACLs) or capabilities. In contrast, in the peer to peer arrangement we cannot trust the un-trusted accumulator to authenticate and authorise the peers. We do not accept admission to the operating arrangement of a replica holder and appropriately use encryption and key administration to alter this functionality. Encryption based access control relies on authentication during the key setup phase, if a decryption key is given to the user after authentication. The key plays a similar role to the admission token in systems such as Kerberos, while the encryption arrangement in peer to peer amusing networks plays the role of the security subsystem in centralized systems in a manner that it takes a user's key and authorizes data access. Access tokens have a very small validity and are easy to be renewed. User keys have a longer validity and so have high probability of being stolen or lost. Due to the long span for which each user key is valid results in a leaving a large impact when the key is modified due to the fine-grained access control requirements. To maintain this highly fine-grained access control system each object is separately encrypted for each group of recipients, so that the user doesn’t have access to data other than the...
required data. Hence at the time of modifying the user key all the files which the user has access through this key is re-encrypted. This is one of the major reasons why a fast and efficient encryption technique needs to be in place. It is recommended that all files to the user’s key grants access to is renovated at the same time so that object needs to be encrypted only once, though this might be a slower process it is essential to maintain the fine grained access control system. The speed on of encryption/decryption depends on the speed of the cipher and also on the scalability of the scheme.

Another issue in encryption is the space it requires sometimes the encrypted data might be larger than the data to be encrypted this is sometimes caused due to the number of recipients, such encryptions are not suitable for peer to peer networks as storage is critical in peer to peer networks

**Functionality**

Encryption schemes differ on the basis of their properties some examples of some encryption schemes are symmetric and asymmetric encryption schemes. This scheme can be used by peer to peer networks to use different features available in each of these schemes. A peer to peer network should have a encryption system that should be able to encrypt objects for any number of subjects in a very efficient and cost effective manner. However this isn't supported by all encryption and decryption methods

**Privacy**

The flow of control in the traditional networks is controlled from a single point such a security system is very hard to be implemented in a peer to peer network as there are many untrusted storage location. It is important in such a network to protect

Information about which subjects have access too

**IV. Requirements for a good encryption and decryption technique**

In short for a encryption to be the best it should satisfy certain criteria like efficient addition and removal of users from a group; efficient user key revocation; efficient encryption and decryption; ability to encrypt for conjunction and disjunction of groups; ability to encrypt for a group that one is not a member of; ability to not reveal access structures in the header.

**Existing encryption techniques**

Fully homomorphic encryption is a cryptosystem that is capable of arbitrary computation on cipher texts. This uses a mathematical object known as ideal lattice. Fully homomorphic encryption is very powerful. Fully homomorphic
encryption scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the results.

Data encryption standard or DES is a symmetric key method of data encryption. In DES the sender and receiver use the same key to encrypt and decrypt the data. This technique was developed by IBM in 1970s. Advanced Encryption Standard is the successor to DES after it was cracked by a brute force attack. As the size of the key in DES was very small, the size of the key is directly linked to the strength of the encryption. Advance encryption standard came into existence in 1997 this is also a symmetric key encryption but it used a three block cipher and wasn’t prone to any brute force attacks.

Anonymous peer to peer networks

Some of the networks commonly referred to as "anonymous P2P" are truly anonymous, in the sense that network nodes carry no identifiers. Others are actually pseudonymous: instead of being identified by their IP addresses, nodes are identified by pseudonyms such as cryptographic keys. There are many reasons to use anonymous P2P technology; most of them are generic to all forms of online anonymity. P2P users who desire anonymity usually do so as they do not wish to be identified as a publisher (sender), or reader (receiver), of information. Common reasons include: 1) Censorship at the local, organizational, or national level.

2) Personal privacy preferences such as preventing tracking or data mining activities.

3) The material or its distribution is considered illegal or incriminating by possible eavesdroppers.

4) Materials is legal but socially deplored, embarrassing or problematic in the individual's social world.

Conclusion

The popularity of peer to peer networks has created many security risks for both individuals and for organizations. The current trend in the development of peer to peer networks is making it more secure by applying concepts of
encryption and providing anonymity to the users and hence protecting them from threats like identity and leakage of sensitive data from the peers, the cause for these problems are the absence of a centralized security subsystem and a not having a strong and efficient encryption technique in place.

Reference

1. Oleksandr Bodriagov, Sonja Buchegger Encryption for Peer-to-Peer Social Networks.


4. A Novel Stochastic-Encryption-Based P2P Digital Rights Management Scheme Majing Su, Hongli Zhang School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. Xiaojiang Du,Qiong Dai Dept. of Computer and Information Sciences, Temple University, Philadelphia, PA, USA.


