International Journal of Research in Advent Technology, Vol.2, No.2, February 2014

E-ISSN: 2321-9637

Providing Security in Hybrid P2P Networks using Client Side Encryption

Nikhil Surkar[1], Harish Chincholkar[2]
BE (CSE)[1] M.Tech (CSE)[2]
Email: niksurkar@gmail.com[1] , harishchincholkar.7@gmail.com[2]

Abstract :In this paper, we demonstrate the application of Trusted Computing to securing Peer-to-Peer (P2P) networks. We identify a central challenge in providing many of the security services within these networks, namely the absence of stable verifiable peer identities. We employ the functionalities provided by Trusted Computing to establish an authentication scheme for peers and extend this scheme to build secure channels between peers for future communications. In this paper we demonstrate securing hybrid P2P network by using client side encryption with random key generation at middle tier.

Keywords:
P2P networks/computing, state-of-the-art in P2P networks, future trends in P2P domain, Encryption

1. INTRODUCTION

1.1 Peer to Peer Network

Peer-to-Peer (P2P) networks and the computations that they facilitate have received tremendous attention from the research community, simply because of the huge untapped potential of the P2P concept – extending the boundaries of scale and decentralization beyond the limits imposed by traditional distributed systems, besides enabling end users to interact, collaborate, share and utilize resources offered by one another in an autonomous manner. Moreover, P2P architectures are characterized by their ability to adapt to failures and dynamically changing network topology with a transient population of nodes/devices, while ensuring acceptable connectivity and performance. Thus, P2P systems exhibit a high degree of self-organization and fault tolerance.

The P2P concept represents a paradigm shift from the client-server or hub-spoke model to a more decentralized device to device model. The devices perform the role of either client or server depending on the application and the nature of interaction.

Since the interaction among peer devices is direct in nature it frees up the most basic of resources – network bandwidth, which was placed under tremendous strain due to millions of users accessing information over the internet, using the traditional client-server paradigm, where a few servers cater to the ever increasing demand for information from the end users. The peer model allows end users to directly connect to other peers on the internet, forming groups and collaborating, leading to the creation of virtual supercomputers, immense file systems offering potentially limitless storage, user created search engines and other novel applications.

A formal definition of P2P systems is as follows: "*Peer-to-peer systems are distributed systems consisting of interconnected nodes able to self-organize into network topologies with the purpose of sharing resources such as content, CPU cycles, storage and bandwidth, capable of adapting to failures and accommodating transient populations of nodes while maintaining acceptable connectivity and performance without requiring the intermediation or support of a global centralized server or authority.*"

1.2 Hybrid P2P Systems – in which peers rely partially on a central server to provide certain services, although the interaction between peers still takes place independently.

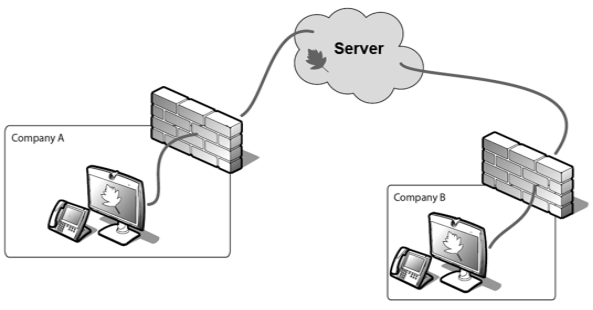

Figure 1: Hybrid P2P Network

1.3 Security in P2P networks

Whilst many aspects of P2P networks have been thoroughly researched, security within these networks still remains a challenge. It is not our intention to exhaustively review security issues for P2P networks here.
Rather, we focus on identifying some key security issues in P2P networks.
The security architecture associated with the ISO/ITU Open Systems Interconnection (OSI) reference model serves as a useful framework for assessing security issues in networks. According to, a secure system is governed by the set of security services it provides, and the mechanisms put in place to cater for these services. The set of potential security services in are divided into five main classes:

- Confidentiality
- Integrity
- Authentication
- Access Control
- Non-repudiation

1.4 Major Issues in Hybrid P2P Network

- Data may be seen by third person (Hacker) when the data passes from one client to another client.
- Encryption is done at middle server part in network systems which take heavy loads on server.
- Key is stored at particular place and same key is used which may get predicted or may get hacked.
- No trust at server part (Server Database cannot be trusted).

2. SYSTEM ARCHITECTURE:

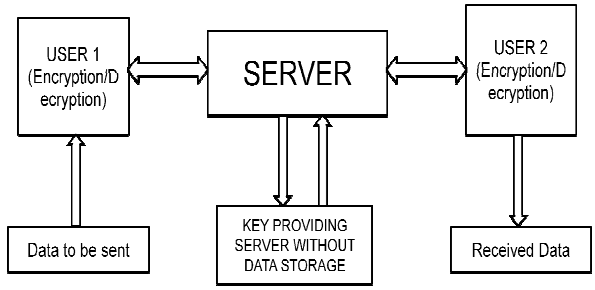

Figure 2: System Architecture

The system consists of following components:

- Server:
  The server basically performs two functions. One is to generate a random key every time a client wish to communicate with another client.
  Secondly server bypasses the data from one client to another without storing it at any location. In the approach presented in this paper the clients and server don't require any databases to store any key or the data that is been transferred from one client to another.
- Any symmetric algorithm can be used to encrypt data on client side. Whenever a client request to communicate with another client they receive a random generated key from server which they use to encrypt the data.
  Thus the communication lines (network path) consist of cipher data passing through network.
- Client: Client represents the users who need to communicate with other user on network. In normal scenario the encryption can be done on server side but it creates server as bottleneck and the other part is user send plain data through network which can be seen by third person (man in the Middle Attack).

2.1 Man in the Middle Attack

The M**an in the middle Attacks** (often abbreviated **MITM**, **MitM**, **MIM**, **MiM**, **MITMA**) in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones, which is straightforward in many circumstances (for example, an attacker within reception range of an unencrypted Wi-Fi wireless access point, can insert himself as a man-in-the-middle)

3. Preferred Encryption Algorithms

3.1 AES (Advanced Encryption Standard)

AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware. Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 column-major order matrix of bytes, termed the state, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special finite field.

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The numbers of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

3.1 High-level description of the algorithm

KeyExpansion — round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

AddRoundKey— each byte of the state is combined with a block of the round key using bitwise xor.

SubBytes — a non-linear substitution step where each byte is replaced with another according to a lookup table.

ShiftRows — a transposition step where each row of the state is shifted cyclically a certain number of steps.

MixColumns — a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey

Final Round (no MixColumns)
SubBytes
ShiftRows
AddRoundKey.

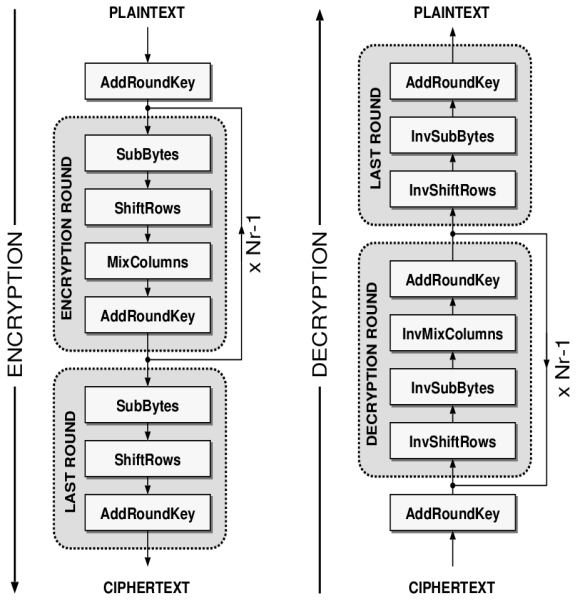

Figure 3: Working of AES Algorithm

3.2 Triple DES

In cryptography, Triple DES is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.

The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.

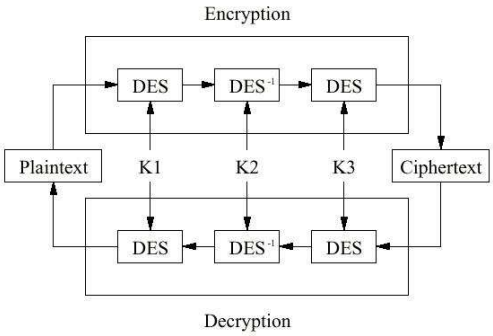

Figure 4: Working of Triple DES

3.3 Algorithm:

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

ciphertext = EK3(DK2(EK1(plaintext)))

I.e. DES encrypt with K1, DES decrypt with K2, then DES encrypt with K3.

Decryption is the reverse:

plaintext = DK1(EK2(DK3(ciphertext)))

I.e., decrypt with K3, encrypt with K2, then decrypt with K1.
Each triple encryption encrypts one block of 64 bits of data.
In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying option 2, and provides backward compatibility with DES with keying option 3.

Conclusion

Security in Hybrid peer to peer network is achieved using client side key cryptography. An intermediate server is used for generating key used for encryption and data is encrypted using symmetric algorithm. This approach successfully avoids Man in the middle attack. Data size limited to 5 MB is supposed to be tested at time of execution.

References

[1] R. Ranjan, A. Harwood, and R. Buyya, "Peer-to-peer based resource discovery in global grids: a tutorial," *IEEE Commun. Surv.*, vol. 10, no. 2. and P. Trunfio, "Peer-to-Peer resource discovery in Grids: Models and systems," *Future Generation Computer Systems* archive, vol. 23, no. 7, Aug. 2007.

[2] Krishnan, R., Smith, M. D., Tang, Z., & Telang, R. (2004, January). The impact of free-riding on peer-to-peer networks. In System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on (pp. 10-pp). IEEE.

[3] Basu, A., Fleming, S., Stanier, J., Naicken, S., Wakeman, I., & Gurbani, V. K. (2013). The state of peer-to-peer network simulators. ACM Computing Surveys (CSUR), 45(4), 46.

[4] Darlagiannis, Vasilios (2005). "Hybrid Peer-to-Peer Systems". In Steinmetz, Ralf & Wehrle, Klaus. *Peer-to-Peer Systems and Applications*. Springer. ISBN 9783540291923.

[5] Li, Deng et al. (2009). Vasilakos, A.V. et al., ed. *An Efficient, Scalable, and Robust P2P Overlay for Autonomic Communication.* Springer. p. 329. ISBN 978-0-387-09752-7.

[6] Stutzbach, Daniel et al. (2005). "The scalability of swarming peer-to-peer content delivery". In Boutaba, Raouf et al. *NETWORKING 2005 -- Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless*

Communications Systems. Springer. pp. 15–26. ISBN 978-3-540-25809-4.

[7] Gareth Tyson, Andreas Mauthe, Sebastian Kaune, Mu Mu and Thomas Plagemann. Corelli: A Dynamic Replication Service for Supporting Latency-Dependent Content in Community Networks. In Proc. 16th ACM/SPIE Multimedia Computing and Networking Conference (MMCN), San Jose, CA (2009).

[8] Glorioso, Andrea et al. (2010). "The Social Impact of P2P Systems". In Shen et al. *Handbook of Peer-to-Peer Networking*. Springer. p. 48.ISBN 978-0-387-09750-3.

[9] John Borland, Judge: File-Swapping Tools are Legal ,http://news.cnet.com/Judge-Fileswapping-tools-are-legal/2100-1027_3-998363.html/

[10] Ahson, Syed A. & Ilyas, Mohammad, ed. (2008). *SIP Handbook: Services, Technologies, and Security of Session Initiation Protocol*. Taylor & Francis. p. 204. ISBN 9781420066043.