International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 4, April 2013 **ISSN 2319 - 4847**

A Brief Comparison of Security Patterns for Peer to Peer Systems

Rahul J. Vaghela[1], Kalpesh Patel[2]

[1]PG Student, Department of Computer Engineering, L.D. College Of Engineering, Gujarat Technological University, Ahmedabad

[2]Assistant Professor, Department of Computer Engineering, L.D. College Of Engineering, Gujarat Technological University, Ahmedabad

ABSTRACT

The Peer to Peer Networks are depends on securely distributing the Identities. So P2P Networks are vulnerable to attacks against Identities which includes Eclipse Attack, Sybil Attack etc. In the defence against such attacks The Security Patterns are provided and compared. The Paper includes CA Certification using central Server for securely providing the Identities to Users of P2P System. This Paper also includes the distributed approach defined as Self Certification to Provide the Security in such a Network. In this Paper we have compared these patterns using theoretical analysis and Simulated Network.

Keywords: Security Pattern, Peer to Peer System, Sybil Attack, Identity Management**,** Self Certification, Reputation

1. INTRODUCTION

A P2P networks are dynamic and distributed networks. Normally, the main difference between the concepts of P2P network and traditional server-client network is that the file downloading is not provided by a central server. Nowadays, P2P technology is widely used for files sharing, instance message communication and distributed computing. The security issues are inherent features accompanying with P2P systems. It is highly suspected to various forms of malicious attacks. It can not only be attacked from the malicious nodes outside the P2P network but also vulnerable to its own peers. The thousands to millions of anonymous peers provide an ideal attack environment for attackers. In addition, the popularity of P2P also leads different kinds of Security Issues.

Protection against the Sybil attack [1] is a fundamental requirement for many of todays distributed applications. A concrete example of this would be an online voting system where one person can vote using many online identities. By picking IP addresses as the resource for blacklisting users in Anonymizing networks, it provides less defence against the Sybil attacks. So, some approach has to be adopted to provide defence against Sybil attacks. Trusted Certification [2] is one of those approaches that has the potential to completely eliminate Sybil attacks. However, trusted certification relies on a central authority (CA), such as the administrator who can guarantee that each person has a single identity represented by one Certificate. CA for the actual certificate issuance acts itself as a Registration Authority that authenticates and authorizes users. In this way, it can be ensured that users cannot get new credentials after their issued credential is blacklisted.

In P2P network – an ambitious approach to protect the P2P network without using any central component. The past activities of the peers are used to determine whether a peer is a malicious peer or a good peer. Once the malicious peer detected it will be cut off the network as good peers do not perform any transaction with them. Thus we can significantly reduce the malicious activities from the network.

All peers in the P2P network are identified by identity certificates. The past behavioral knowledge of a given peer is attached to its identity. The identity certificates are generated using self-certification [3], and all peers maintain their own certificate authority which issues the identity certificate(s) to the peer. Each peer owns the past information pertaining to all its past transactions with other peers in the network, and stores it locally. A two-party cryptographic protocol not only protects such information from its owner, but also facilitates secure exchange of information – reputation [4] between the two peers participating in a transaction.

The Paper also present a short Comparison of CA Certification Pattern and Self Certification based on the analysis of the Simulated Network.

The paper is organized as follows. The First section gives the little introduction about the security patterns. The Second section gives the brief description of the CA Certification and Self Certification patterns. The Next Section includes comparison of these patterns and then the conclusion is provided.

2. SECURITY PATTERN

One of the most exciting developments in software engineering is the emergence of design patterns as an approach to capturing, reusing, and teaching software design expertise. Because of the popularity of design patterns in the software engineering community, the natural inclination is to assume that anything going by the name "security patterns" should be described using a UML diagram and include sample source code.
A security pattern is a well-understood solution to a recurring information security problem. We can define the Security Pattern as following:

"A Security Pattern describes a particular recurring security problem that arises in a specific context and presents a well-proven generic scheme for its solution."[5][6]

3. VARIOUS SECURITY PATTERNS

This Section Provides brief introduction to the Security Patterns Covered in the paper. First we take a look of the CA certification pattern that was of centralised nature. Later we focus on distributed approach of Self Certification pattern.

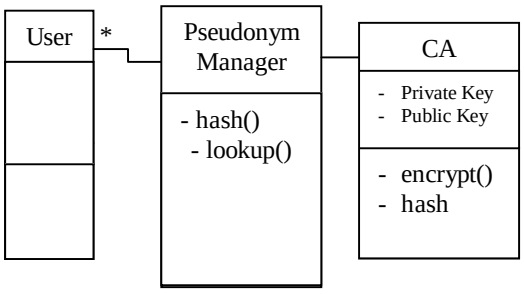
a. CA Certification Pattern:

- Problem Definition:

Sybil attack is the form of the attack which deals with the computer security. It is an attack against identity in which an individual entity masquerades as multiple simultaneous identities. A concrete example of this would be an online voting system where one person can vote using many online identities. Anonymous authentication scheme may be vulnerable to Sybil attacks if users can get new credentials after their issued credential is blacklisted.

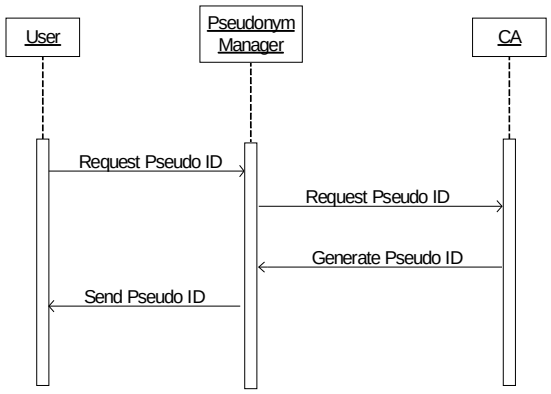
- Solution:

This solution using three independent components: the Pseudonym Manager (PM), the CA service and Network Manager (NM) as shown in Figures. Having this separation allows us to benefit from existing and well tested Network Manager and CA. In this model, the pseudonym Manager acts as a Registration Authority by authenticating the users and validating their requests before forwarding the requests to the CA. The pseudonym Manager maintains records of the pseudonyms issued to the authenticated users.



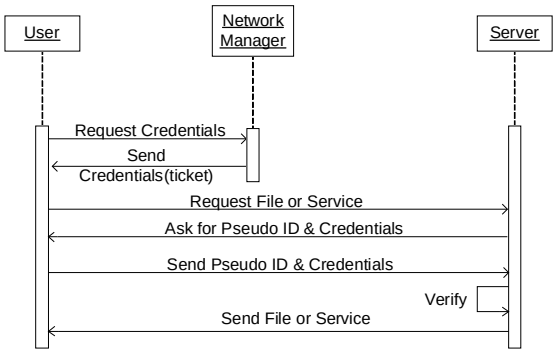
1. Class Diagram for CA Certification Pattern

In our model Central Authority (CA) is included which issues the Certificates to the Users. The pseudonym manager exploits a CA for the actual certificate issuance, acting itself as a Registration Authority that authenticates and authorizes users for the CA.
First, the User must interact with PM in order to get the Pseudonym ID to get anonymous connection. The PM requests CA for Certificate [8] Issuance to ensure that the user cannot have multiple connections to the server.



2. Sequence Diagram for Issuing Certificate

Thus, the user is authenticated and issued a Certificate. The PM then registers the certificate to the corresponding user and issues the pseudonym ID to the user. Now by the given pseudonym ID, the user requests NM for Credentials to get access to the anonymous network services. After acquiring the credentials, the user can access services he wants from the network.



3. Sequence Diagram for Issuing Certificate

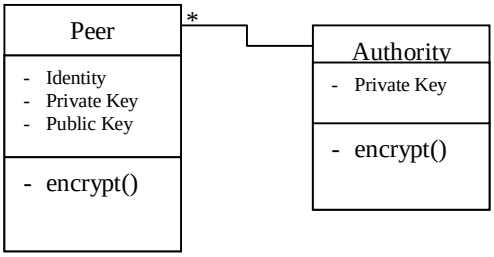
b. Self Certification Pattern:

- Problem Definition:

In P2P System, the Peer follows predefined Join or Leave protocol. The peers are connected with insecure communication channels. The peers those are participating or not can spread malware in the network. So, peers need a mechanism to judge the quality of the content before making Go/No-Go decision in transactions and thereby develop trust relationships with other peers. In the absence of any trusted central agency, an attacker can gather infinite identities and start issuing recommendations to it. A peer might modify the past information stored in the network to maliciously raise its own reputation [9].

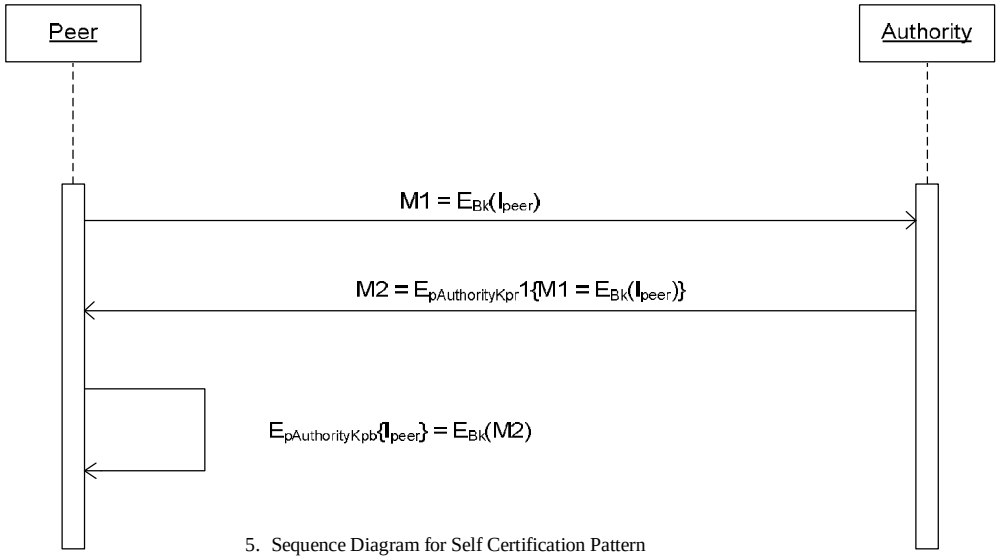
- Solution:

We will assign a role of some type of trusted third party authority that can provide the digital signature based authentication in Peer to Peer Network without using their original network id in encryption scheme of Self Certification Pattern. The whole description of pattern will be as follows.



4. Class Diagram for Self Certification Pattern

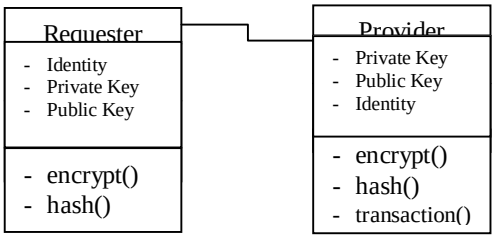
The above Diagram describes that the whole network is arranged into number of groups which can have some trusted authority to provide the signature based encryption scheme.



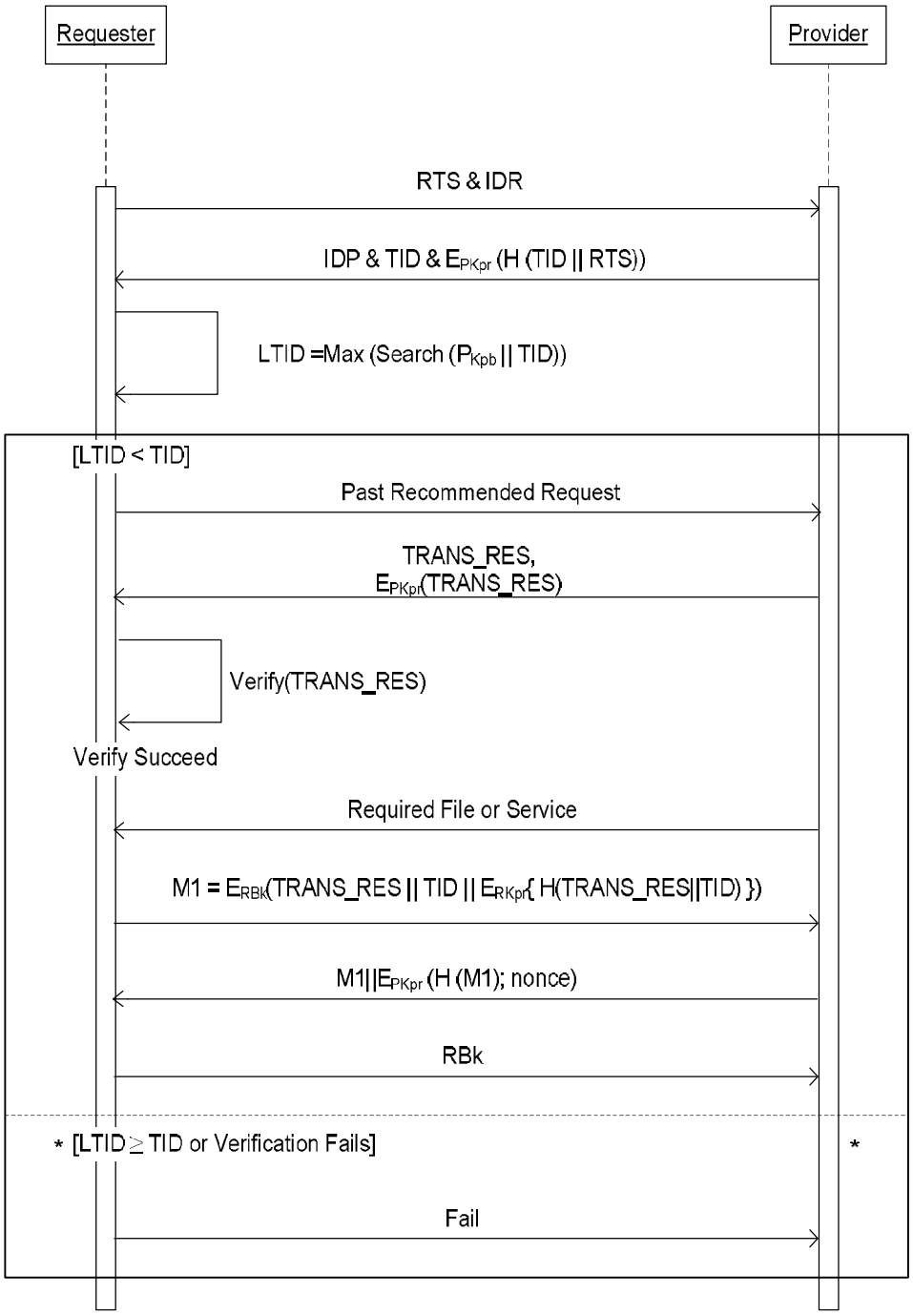
5. Sequence Diagram for Self Certification Pattern

$E_K\{X\}$ – Encryption of X using Key K
Bk – Blinding Key Generated by Peer itself
I_{peer} - Identity of Peer other than network id
Kpr – Private Key
Kpb – Public Key

Once the requester has selected the provider with highest reputation that was earned by the past behavior of a peer, it starts to exchange the information required to request the data from the provider. The following Diagram represents a class diagram with the parties participating in such a communication with their attributes and functions that they own.



6. Class Diagram for Peer Information Exchange Protocol



7. Sequence Diagram for Peer Info Exchange Protocol

R	–	Requestor
P	–	Provider
RTS	–	Request for Transaction
TID	–	Transaction ID
H(x)	-	Hash value of x

The Sequence Diagram represents the whole communication scenario for Information Exchange Pattern. This protocol only assumes that inserts & search functions are available and are not resilient to peers that may not follow the recommended join & leave protocol of the network. Here the TRANS_RES will be requested to compute and verify the reputation of the Provider.

4. COMPARISON RESULT

This section presents a comparison of above described patterns on the basis of various parameters. First of all CA Certification depends on centralized server and Network Manager, so all the disadvantages related to centralized systems will be there. Besides that the following table gives the comparison on the basis of various network parameters.

Parameter	CA Certification Pattern	Self Certification Pattern
Communication Cost	Medium	Higher
Complexity	Medium	Higher
Single node Failure	Yes	No
Central Dependency	Yes	No
Security Degree	Medium	Higher
Attacker Detection	Medium	Higher
Implementation Cost	Less	High
Transaction Processing Time	High	Low (Improved)

5. CONCLUSION

From the Comparison of these two patterns we can conclude that the CA Certification having the simplicity of the centralized system but with the problems such as single node failure, while the Self Certification provides higher security with complex algorithm and network usage. Thus there is a tradeoff between Complexity and Security.

6. ACKNOWLEDGEMENTS

Rahul Vaghela wishes to thank Prof. Kalpesh Patel, for his guidance and help for doing this work. He also acknowledges Prof. D. A. Parikh, Head of computer department, and to all staff of computer department for full support for completion of this work.
Prof. Kalpesh Patel wishes to acknowledge his family and staff of computer department at L. D. College of engineering.

References

[1] J. R. Douceur, The Sybil attack, In Proceedings for the First International Workshop on Peer-to-Peer Systems (IPTPS'02), ser. LNCS, vol. 2429. Cambridge, MA, USA: Springer, Mar. 2002, pp. 251–260.
[2] L. Zhou, F. Schneider, and R. Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov.2002.
[3] C.V. Arulkumar, K. Jeyakumar, M. Malarmathi, T. Shanmugapriya,"Secure Communication in Unstructured P2P Networks based on Reputation Management and Self Certification", International Journal of Computer Applications (0975 – 8887) Volume 44– No15, April 2012.
[4] M. Gupta, P. Judge, and M. Ammar, "A Reputation System for Peer-to-Peer Networks," Proc. 13th Int'l Workshop Network and Operating Systems Support for Digital Audio and Video (NOSSDAV), 2003.

[5] Darrell M. Kienzle, Matthew C. Elder, David Tyree, James Edwards-Hewitt "Security Patterns Repository" Version 1.0.
[6] M. Schumacher, E. B.Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating security and systems engineering, Wiley 2006.
[7] Arunasri Chamarti, P.Rajasekhar, "Securing Anonymizing Networks from Sybil Attacks", IJCTA-2012,vol-3.
[8] Zhen Luo and Zhishu Li, "A Self-organized Public-Key Certificate System in P2P Network", JOURNAL OF NETWORKS, VOL. 6, NO. 10, OCTOBER 2011.
[9] B.V.S.N.Lakshmi, C.Prakasa Rao, "Managing P2P Reputation System Using Decentralized Approach International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-1, Issue-4, October 2012.

AUTHOR

Rahul Vaghela received the B.E. degree in Computer Engineering from Govt. Engg. College, Gandhinagar in 2011. He is receiving M.E. degree in Computer Science and Technology from Gujarat Technological University, Ahmedabad.