Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 6, 2008

Yongchao. Song
Huawei
Ben Y. Zhao
U. of California, Santa Barbara
Xingfeng. Jiang
Haifeng. Jiang
Huawei

February 3, 2008

P2PSIP Security Analysis and Evaluation
draft-song-p2psip-security-eval-00

Status of this Memo

Copyright Notice

Abstract

This document provides an analysis and evaluation of security with P2PSIP overlay network. The draft compares security difference between C/S and P2P, then partitions the P2PSIP architecture into layers, and analyze the security issues in each layer and the

security relationship among the layers. Security issues with different kind of application scenarios are distinct. This draft classifies the application scenarios into two main types, and the security threats with these two types of scenarios are analyzed in detail.

Table of Contents

1. Introduction

As pointed out in Peer-to-Peer SIP (P2PSIP) concepts and terminology document [I-D.ietf-p2psip-concepts], building a P2PSIP system has many security consideration. The intention of this draft is not to provide a solution but to give some guidelines and references for the development of P2PSIP peer and client protocol. The interaction with conventional SIP and other systems are not included at present.

This document compares security difference between C/S and P2P, and then partitions the P2P applications into four main layers, and analyze the security issues in each layer, and their relationship from security perspective.

The detailed security requirements of P2PSIP overlay network are dependent on the deployment scenarios[I-D.bryan-p2psip-app-scenarios] in the real world. In this draft, the application scenarios are divided into two types in general according to the likely deployment method. The security issues with each type are analyzed in detail.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The terminology and definitions used in this document are compatible with P2PSIP Work Group Draft "Concepts and Terminology for Peer to Peer SIP" [I-D.ietf-p2psip-concepts]. We also introduce the following important new terms used in this document, and they are also interpreted when used inline.

P2P Overlay Base:A P2P Overlay Base includes all the Peers that participate in the p2p overlay. The P2P Overlay Base provides distributed storage and routing services to both peers and clients.

Trusted P2P Overlay Base:All peers in a Trusted P2P Overlay Base are trusted. The Peers in the overlay are all of good behaviors and under control due to deployment. For example, a carrier deploys a Trusted P2P Overlay Base to provide service to his customers, and all the peers are the carrier's devices.

Untrusted P2P Overlay Base: Peers in a Untrusted P2P Overlay Base are not all trusted. There may exist some malicious behaving nodes in the P2P Overlay Base.

3. Security Comparison between C/S and P2P

	C/S	P2P
transport	authenticate between client and server	authenticate between neighbors
routing	need one hop security transport layer security can ensure it	need hop by hop security to ensure the end to end security
storage	server is trusted for storage	responsible peer may not trusted, need end to end security
application	out of scope of this specification	out of scope of this specification

Figure 1 Comparision between C/S and P2P security

In Client Server(C/S) architecture, a client asks for a specific service only from a specific server. And the following process of the server is transparent to the client. The destination contact address(i.e. the address of that server) can be acquired from the

trusted DNS system directly. So there only exist security issues with one hop. What we need to do is making a client be secure to that server, and making that server be secure to this client, and typically nothing more.

However, in P2P Overlay, the distinct architecture from C/S makes the security issues change.

First, One overlay is an autonomous system, each peer in the system can provide distributed storage and transport services for other P2P entities, and the p2p overlay is self-organization. Whereas in C/S architecture, only a specific server provides certain services to the clients.

Second, a peer sends messages though Key-Based-Routing and he doesn't know where the destination is. There exist intermediate nodes between the source and destination. Whereas in C/S architecture, a client sends its request directly to a server.

Third, one peer does not know whether he should trust the information acquired from the overlay. Whereas in C/S architecture, the information acquired from the server is always trustful.

So in P2P overlay, security issues not only exist between end to end entities, but also between hop by hop services. They are not only related to the routing security, but also related to the content security.

4. Security Analysis with P2P Layers

The security of P2PSIP has close relationship with each layer security of P2PSIP architecture. Here we splits the P2PSIP architecture into four main layers, as shown in the following figure, and analyze the security issues from the p2psip architecture perspective.

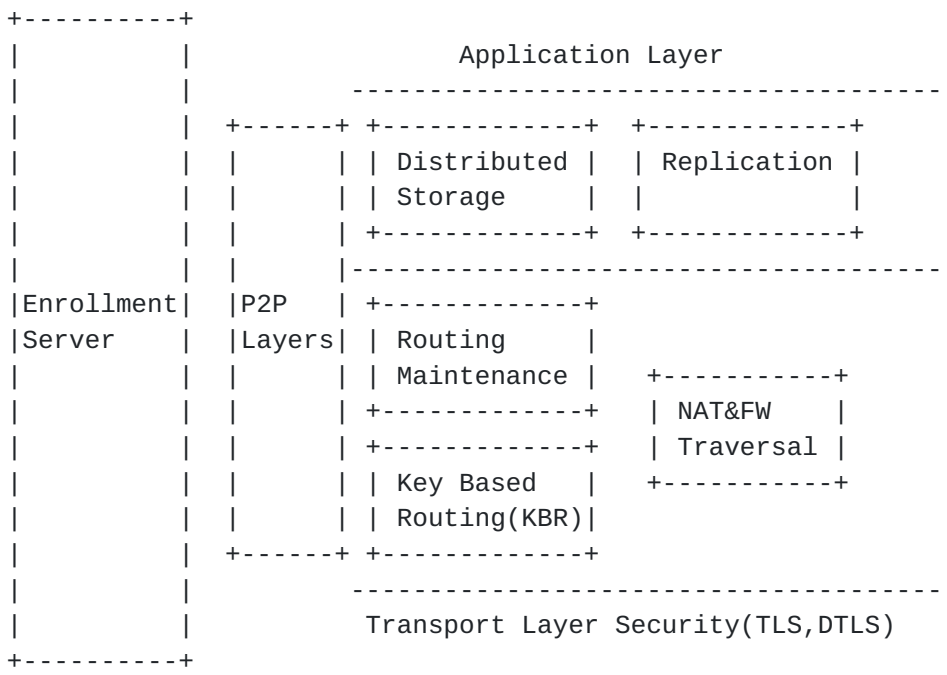

Figure 2 P2PSIP architecture

The four main layers are:

Application Layer: Provides the user application, and invokes the services provided by the Distributed Storage and Replication Layer.

Distributed Storage and Replication Layer: Stores and Manages the resource objects. Each peer's responsible resource objects are determined by the specific P2P algorithm. Replication may be utilized to ensure the availability of resource objects under churn.

Routing Maintenance and KBR Layer: Maintains the routing table, and do the Key Based Routing(KBR). NAT and Firewall traversal may be involved to establish direct connections.

Transport Layer: Provides transport service for the upper layers.

The security measures adopted in the lower layer may impact the upper layer security choices. And not every security threat needs to be considered in all layers, however, it is typically only required to be solved in one layer. And the interesting issue is in which layer should the specific security threat be considered and solved. We have our primary analysis for each layer in the following sub sections.

4.1. Transport Layer Security

P2PSIP overlay mostly run on top of the Internet, messages between associated nodes should be protected against attacks(such as Man-in-the-Middle). In order to establish the identity trust association, nodes SHOULD authenticate each other, TLS and DTLS are preferable to solve these problems. If transport service security is fully protected, we can prevent nodes without valid identities to participate in the overlay. This layer must provides reliable and secure hop by hop transport service for the p2p overlay, though that is not enough.

4.2. Routing Maintenance and KBR layer Security

Each Peer in the P2PSIP overlay provides key based routing service to other peers, and a routing maintenance mechanism is used to keep the routing table timely and correct for the routing service. There are some security threats with the routing table updating interaction and the key based routing.

Even if all the nodes participating in the P2PSIP overlay are with valid identities, the overlay may still be attacked by responding with fake routing table to UPDATE requests. If the routing table is false, the routing determination based on it will be false too. So, verification mechanisms SHOULD be adopted to verify if the routing table one learned from another is correct or not. A correct routing table is important for hop by hop security.

Second, some attacker who is not responsible for the destination ID, responds to some requests when he is in the intermediate routing path(May respond with a fabricated resource object or just says that the searched resource object doesn't exist). Should the source node verify whether the response peer is responsible for the request? When and how does the source peer do that? Whether the response peer is responsible for the request is important for the end to end security.

Third, some attackers may discard the messages when forwarding, or on purpose forward the message to a wrong next hop. Should the overlay need a method to detect the misbehaving forwardings?

Chosen-ID attack makes the above security issues much more worse.

Fourth, some attacks may cause the overlay under high churn rate. Overlay wastes much more traffic to update the routing table, and transfer relative resource objects under churn.

The first and fourth issue above is about routing maintenance

function security, and the remain two issues are about the KBR function security.

4.3. Distributed Storage and Replication Layer Security

Distributed storage and replication layer provides distributed storage service for the resource objects that located in one's responsible resource ID range, and the replication service to keep the availability of resource objects under churn. The security issues in this layer are typically end to end, and about the content and authority security.

First, how to protect resource objects against unauthorized data operation such as obtainment, modification or removing?

Second, should the P2PSIP overlay need a method to prevent attackers from publishing malicious information that will cause a DDOS attack? For example, Peer A may publish a very popular resource record with the contact address of Peer B without B's permission. That causes unexpected lots of connections to B which will make Peer B down.

Third, overlays work well for a reasonable amount of resource objects, but crash more or less when inserting millions of resource objects per node. Spam attacks can make overlays go down. Open issue: Should the spam attack be considered in the distributed storage layer? Or is it only the responsibility of the application layer to handle this problem?

Replication security is to TODO.

4.4. Application Layer Security

Application layer security requirements are out of scope of this specification.

5. Security Analysis with Application Scenarios

As described in the security considerations section in application scenarios draft[I-D.draft-bryan-p2psip-app-scenarios], the security requirements of the various application scenarios vary tremendously. So in this section, we divide the application scenarios into two main types, instead of analyzing all the security threats with each specific scenario described in the application scenarios draft, we just analyze the relative security threats of these two types, which represent most of the likely deployment scenarios in the real world. For example, the "Public P2P VoIP Service Providers" scenario in section 4.1.1 of application scenarios

draft[I-D.draft-bryan-p2psip-app-scenarios] may be deployed using the first type(refer to section 5.1 of this specification), and the "Open Global P2P VoIP Network" scenario in section 4.1.2 of application scenarios draft may be deployed using the second type(refer to section 5.2 of this specification).

5.1. Trusted P2P Overlay Base

In a trusted P2P Overlay Base, all the peers are deployed with trustful nodes. They are of good behaviors. They may deployed to provide reliable and high quality services, and may also do some management issues for the overlay. All P2PSIP clients access the overlay service through the associated trusted peer. Shown as the following figure 3.

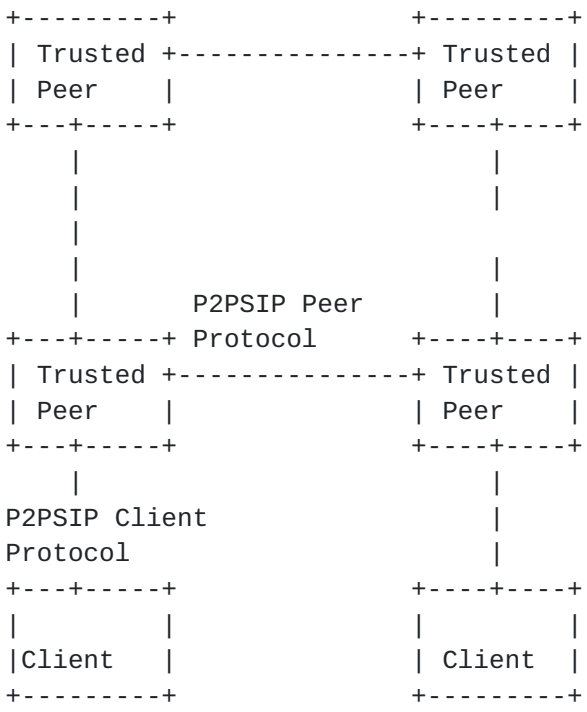

Figure 3 Trusted P2P Overlay Base

As for this type of scenarios, we regard the P2P Overlay Base to be secure. The security issues to be considered are the transport security between trusted peers and the security issues associated with clients. Because clients doesn't provide routing service for the overlay. Security issues more focus on distributed storage layer. Some of the attacks are described in the p2p-security-requirement draft[I-D.matuszewski-p2psip-security-requirement].

Possible Attacks	Descriptions	Considerations
Transport Related	1.Message Privacy 2.ID hijack	TLS and DTLS
Unauthorized Data Operation	Unauthorized Access, Modification, Removing	Certificate Mechanism
Man In the Middle	In the progress of Authentication between client and its associated peer	Authentication Security
data pollution and poison	1.Publish Fake Resource Objects 2.Publish malicious contact information (DDOS attack)	1.Check Mechanism? 2.Black List?
Spam Attack	Publish lots of redundant resources	1. Check Mechanism? 2. Limit one's publication number?

Figure 4 Possible Attacks on the Trusted Overlay Base Scenarios

5.2. Untrusted P2P Overlay Base

In an untrusted P2P Overlay Base, there are peers who are not trusted by other peers. Some of untrusted peers may do harmful things or abnormal behaviors to the overlay due to malicious or unknown intentions. There may or may not exist trusted peers in the overlay. Shown as the following Figure 5.

Please view in a fixed-width font such as Courier.

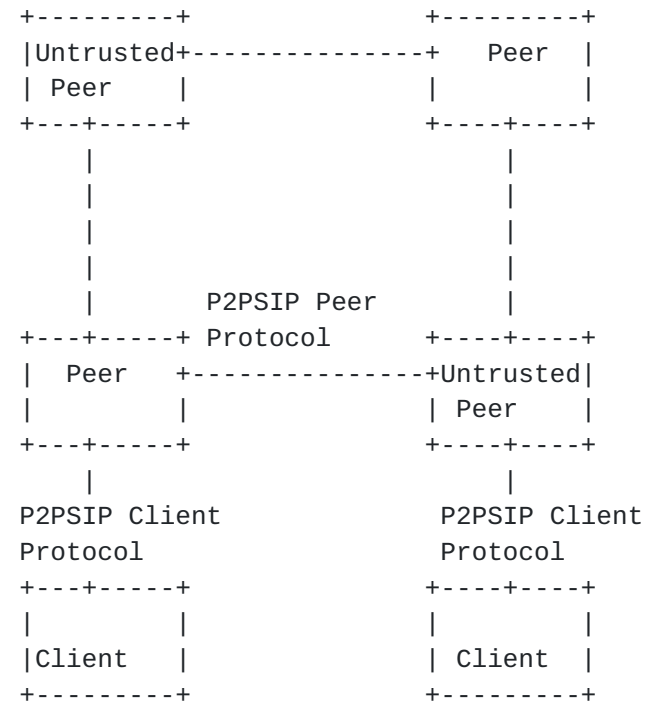

Figure 5 Untrusted P2P Overlay Base

As for this type of scenarios, the security threats with the Trusted P2P Overlay Base still exist, besides that, even more security issues emerge, because there may exist malicious peers in this type of scenarios. Each layer of the P2PSIP architecture and the enrollment may be attacked, the attacks beyond those in the Trusted Overlay Base scenarios are listed in the followings Figure 6.

Possible Attacks	Descriptions	Considerations
Identity Attack	1.Chosen-ID attack 2.Sybil Attack 3.Fabricated response from the intermediate peer	1.Enrollment Server 2.A proof mechanism to verify whether it is a true root?
Forwarding Attack	1.discard messages 2.Forwarding to a wrong next hop node 3.modify messages when forwarding	1.message signature? 2.A diagnosis mechanism for detecting which intermediate peer is a bad man?
Replay Attack	Intermediate peer stores messages and replays	Timestamp to recognize timed messages?
Routing Table Attack	give malicious response info to an updating routing table request	Per DHT specific?

Figure 6 Possible Attacks on the Untrusted Overlay Base Scenarios

As for these security issues, the diagnosis draft[I-D.zheng-p2psip-diagnose] provides a framework using an ECHO message to diagnose the problems in the P2PSIP overlay.

6. Open Issues

1. Do we need a verification mechanism to verify if the routing table one learned from another is correct or not?

2. Should the source node verify whether the response peer is responsible for the request? When and how does the source peer do that?

3. Should the overlay need a method to detect the misbehaving forwardings?

4. How to protect resource objects against unauthorized data operations? And in which layer should we do that?

5. Should the P2PSIP overlay need a method to prevent attackers from publishing Malicious Information or Spams? And in which layer should we address these problems?

7. Security Considerations

This document analyzes and evaluates security in P2PSIP overlay networks, but it does not introduce any security risk by itself.

8. IANA Considerations

There are no IANA considerations associated to this memo.

9. Acknowledgments

We would like to thank Zheng Hewen for his contribution to part of this specification. We would like to thank Eunsoo Shim, Li Feng, Hu Xinyu, Ning Zong for their valuable comments. And many authors' discussion in the p2psip and p2p-hackers mailing list are contributed to this draft.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4981] J. Risson, "Survey of Research towards Robust Peer-to-Peer Networks: Search Methods", RFC 4981, September 2007.

[I-D.ietf-p2psip-concepts] Bryan, D., "Concepts and Terminology for Peer to Peer SIP", draft-ietf- p2psip-concepts-00 (work in progress), June 2007.

[I-D.matuszewski-p2psip-security-requirement] M. Matuszewski, "Security requirements in P2PSIP", draft-matuszewski-p2psip-security-requirements-01 (work in progress), July 2007

[I-D.jennins-p2psip-security-mechanisms] C. Jennings, "Security Mechanisms for Peer to Peer SIP", draft-jennings-p2psip-security-00 (work in progress), February 2007

[I-D.bryan-p2psip-requirement] D. Bryan, "P2PSIP Protocol Framework and Requirements", draft-bryan-p2psip-requirements-00 (work in progress), July 2007

[P2PSIP-Concepts-Terminology] Dean Willis, "P2PSIP Concepts and Terminology", http://www3.ietf.org/ proceedings/07jul/slides/p2psip-13.pdf, July 2007

[I-D.draft-bryan-p2psip-app-scenarios]D. Bryan, "Application Scenarios for Peer-to-Peer Session Initiation Protocol", draft-bryan-p2psip- app-scenarios-00(work in progress), November 2007

[P2P-Vulnerabilities-Report] Marling Engle and Javed I. Khan, "Vulnerabilities of P2P Systems and a Critical Look at their Solutions", http://medianet.kent.edu/technicalreports.html, November 2006

[P2P-Sybil-Attack] John R. Douceur, "The Sybil Attack", In Proc. of IPTPS (Cambridge, MA, March 2002).

[P2P-Eclipse-Attack] Singh, A., Ngan, T.-W., Druschel, P., and Wallach, D., "Eclipse attacks on overlay networks: Threats and defenses" In Proc. of INFOCOM (Barcelona, Spain, April 2006)

[P2P-Namespace-Integrity] Krishna P. N. Puttaswamy, Ben Y. Zhao etc, "Protecting Namespace Integrity in Structured Overlays", IEEE, December 2007

[I-D.zheng-p2psip-diagnose] H. Zheng, "Diagnose P2PSIP Overlay Network Failures", draft- zheng-p2psip-diagnose-00 (work in progress), November 2007.

10.2. Informative References

[I-D.bryan-p2psip-reload] C. Jennings, B. Lowekamp, E. Rescorla and J. Rosenberg, "REsource LOcation And Discovery (RELOAD)", draft-bryan-p2psip-reload-02 (work in progress), November 2007.

[I-D.baset-p2psip-p2pp] S. Baset, H. Schulzrinne and M. Matuszewski, "Peer-to-Peer Protocol (P2PP)", draft-baset-p2psip-p2pp-01 (work in progress), November 2007.

[I-D.jiang-p2psip-sep] X. Jiang and H. Zheng, "Service Extensible P2P Peer Protocol", draft-jiang-p2psip-sep-00 (work in progress), November 2007.

[I-D.marocco-p2psip-xpp-pcan] Marocco, E. and E. Ivov, "XPP Extensions for Implementing a Passive P2PSIP Overlay Network based on

the CAN Distributed Hash Table", draft-marocco- p2psip-xpp-pcan-00 (work in progress), June 2007.

[I-D.matthews-p2psip-hip-hop] Cooper, E., "A Distributed Transport Function in P2PSIP using HIP for Multi-Hop Overlay Routing", draft-matthews-p2psip-hip-hop-00 (work in progress), June 2007.

[I-D.bryan-p2psip-dsip] D. Bryan, B. Lowekamp and C. Jennings, "dSIP: A P2P Approach to SIP Registration and Resource Location", draft-bryan-p2psip-dsip-00 (work in progress), February 2007.

[I-D.jennings-p2psip-asp] C. Jennings, J. Rosenberg and E. Rescorla,, "Address Settlement by Peer to Peer", draft-jennings-p2psip-asp-00 (work in progress), July 2007.

[I-D.zheng-p2psip-client] H. Zheng, "P2PSIP Client Protocol", draft-zheng-p2psip-client-protocol-00 (work in progress), October 2007.

[I-D.li-p2psip-client] L. Li, Ch. Zhang, Y. Wang and Y. Ji, "A SIP-based P2PSIP Client Protocol", draft-li-p2psip-client-protocol-00 (work in progress), November 2007.

Authors' Addresses

Song Yongchao
Huawei
Baixia Road No. 91
Nanjing, Jiangsu Province 210001
P.R.China

Phone: +86-25-84565081
Fax: +86-25-84565070
Email: melodysong@huawei.com

Ben Y. Zhao
U. of California, Santa Barbara
Santa Barbara, California
U.S.A

Phone: +1 805 893-3926
Fax: +1 805 893-8553
Email: ravenben@cs.ucsb.edu

Jiang Xingfeng
Huawei
Baixia Road No. 91
Nanjing, Jiangsu Province 210001
P.R.China

Phone: +86-25-84565079
Fax: +86-25-84565070
Email: jiang.x.f@huawei.com

Jiang Haifeng
Huawei
Baixia Road No. 91
Nanjing, Jiangsu Province 210001
P.R.China

Phone: +86-25-84565080
Fax: +86-25-84565070
Email: jianghaifeng@huawei.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).