Abstract

P2P (Peer to peer) networks have been a growing trend for almost a decade now. P2P networks are robust and highly scalable networks that are also fault tolerant because of decentralization. SIP (Session initiation protocol) is a protocol that can be used to initiate and control sessions in networked environments. SIP is not yet widely used on P2P networks, but it can become a popular solution for establishing multimedia connections in the future. Networks brought up a new aspect into person to person communication by increasing the allowed distance between the communicating persons to thousands of kilometers. In this paper we first introduce person to person communication in networked environments and discuss security issues related to it. We then proceed to explore the underlying protocols and requirements in P2P networks and finally analyze security issues in person to person communication in P2P networks.

KEYWORDS: P2P, SIP, Security

1 Introduction

It has been possible to do person to person communication over different networks for over a century. It is part of most of our everyday life and is increasingly important in business world. Engineers have been trying to find means to expand person to person communication in networks into different environments since it was first invented. Currently used person to person communication systems include traditional phone calls, text messages (SMS), VoIP (Voice over IP) and different kinds of software that can be used to send messages over IP.

Person to person communication in networks has some risks, no matter how it is done. One can sometimes disguise oneself and pose as another. Eavesdropping is another very common attack on person to person communication. Some other threats, which are perhaps not as acknowledged by the majority are denial of service (for example spamming e-mails or keeping someone’s phone lines busy by calling) and network faults such as single point of failure.

P2P networks are known to be used in different file sharing environments, such as Kazaa [1]. What is unknown to the majority is that P2P networks are based on different kinds of algorithms, such as Chord, which implements a distributed hash table (DHT) abstraction. We will take a quick look at some P2P algorithms and then concentrate on Chord [2].

SIP has been used in networks for some time now, and has been so convincingly reliable and efficient that internet architecture designers have been giving some thought to using SIP in person to person communication in P2P networks. We explore different aspects of SIP and find out what are the key points of the protocol and why it is as good as it is.

We then take a closer look at which of the usual threats of person to person communication apply in P2P networks and which can be ignored due to the nature of a protocol or protocols used. We also examine what new threats exist due to the P2P protocol used, or the network environment itself. In addition to the above, we analyze the benefits that P2P networks have to offer, such as anonymous callers and the fact that there’s no single point of failure problem.

Different aspects of P2P networks have been explored thoroughly, nonetheless we try to come up with ways to improve the security related issues that it implements. We also try to give the analysis a more human perspective, and focus on what is important to humans regarding security in person to person communication in P2P networks.

2 Person to person communication

Person to person communication in networks has been evolving for a long time, so there are naturally a lot of applications that support it. PSTN (Public Switched Telephone Network) is probably the most common method of person to person communication. Other methods include Global System for Mobile Communications (GSM) and a variety of instant messaging applications (IM) that use IP. We introduce these methods more thoroughly one by one later in this section.

These methods give us the basic platform that we need for our everyday communication. There are different ways of taking advantage of the given methods. These ways include normal phone calls, phone calls using a cellular, text messaging, communication using SIP, phone call redirection and voice mail. All the above mentioned methods use SIP to establish a connection with the recipient. There are also methods that do not use SIP, at least not yet. The main method used is called Instant messaging, although it can also be implemented to use SIP. There are several different instant messaging softwares, which you can get for free, such as Messenger, IRC, ICQ and AOL. These softwares do not traditionally use SIP, but there are no reasons why they could or should not use SIP.
2.1 Public Switched Telephone Network (PSTN)

PSTN is a network that uses different signaling protocols, such as ISDN (Integrated Services Digital Network), ISUP (ISDN User Part) and FGB (Feature Group B) circuit associated signaling.[3] PSTN uses SS7 to initialize and control phone calls. PSTN is the most common and second oldest of the currently used person to person communication methods, only Morse-coding is older.

2.2 GSM

GSM (Global System for Mobile Communications) is a European digital communications standard. It uses a rate of 9600 bps using TDMA (Time Division Multiple Access) communications scheme.[4] GSM is very interoperable and can therefore be used in devices such as phones, faxes and pagers.

2.3 Instant Messaging (IM)

Instant messaging works, as its name hints, by sending messages to recipients instantly. It is normally used by computers that connect to the internet. IM guarantees to deliver messages to a recipient instantly, if they are online. Some IM systems also provide offline-messages that are stored into an intermediate’s memory and delivered to the recipient when he/she comes online. Users of IM can keep a list of contacts, similar to phonebooks used by cellular phones, from which you can select a contact and send him/her a message.

3 Risks in networked person to person communication

There are many attacks that are possible to implement on most, if not all current networked person to person communication methods, as we mentioned earlier in the paper. There are of course also things that can go wrong in the network environment without anyone’s intention. We first explain some of the network related problems after which we introduce some common attacks and later discuss the details of some of the more relevant attacks.

Networks consist of components such as routers, user equipment, underlying topologies, service providers, different kinds of cables and sometimes wireless technologies. We can already see from that brief description that there are a number of things that can go wrong. Cables can break, routers can shut down, user equipment can fail, service providers’ configurations can fail and wireless links may get scrambled.

In addition to the above mentioned problems there are problems associated with the quality of service that we get from our service providers. Phone lines can be busy, meaning that we cannot establish a connection to our service provider due to congestion in the network. That kind of situations are not common in today’s world, but exist during local or national emergencies or catastrophes. In centralized networks there is also the problem of a single point of failure, which means that if a key point fails the service can become unavailable to everyone.

We next introduce some of the most common attacks briefly and later take a closer look at some of the attacks.

Denial of Service (DoS) is one such attack. The goal of a DoS attack can for example be to congest targets network connection, so no one can reach the target.

Impersonating another person is also a very common attack. This attack and the DoS attack are both applicable to most of the networked person to person communication methods. The goal in this attack is to for example gain the targets trust and take advantage of it.

Eavesdropping is another popular attack, where the goal is to get the data being sent between the communicating persons.

Man in the middle attack is an attack that is usually automated by software. This attack is implemented by intercepting messages being sent and forward them to the correct endpoint. The goal of the attack is to receive all the messages being sent (this part is eavesdropping) and possibly change the data inside the messages.

3.1 Denial of Service

Implementing a DoS attack can be done in several ways that include creating congestion in the network the target is using and tampering with target’s equipments. We will next introduce three basic types of DoS attacks in more detail. These three attack types are consumption of resources, destruction or reconfiguration of configuration information and physical destruction or alteration of network components.[5]

- Consumption of resources means that the attacker tries to exhaust one or many of target’s resources in order to prevent the target from operating normally. These resources can be for example phone lines, network bandwidth, memory or disk space. Exhausting targets phone lines can be trivial, depending on the target’s number of phone lines, but to exhaust a major corporation’s network bandwidth demands a lot of effort and resources from the attacker, which often makes the attack less feasible.

- Destruction or reconfiguration of configuration information means that the attacker tries to somehow change target’s configurations, such as router configuration, which could easily result in network problems. Another example is changing target’s equipments registry information, which often results in malfunctioning devices.

- Physical destruction or alteration of network components means tampering the actual devices physically. This can range from breaking hardware into pieces to cutting wires. Attacks such as this are always hard to protect against, because the target has to either be located in a very secure place or guarded continuously.

There are three common ways of implementing DoS attacks. These three variations are normal DoS, DDoS (Distributed DoS) and DRDoS (Distributed Reflection DoS) [6]. We briefly introduce the two latter forms of DoS.
4 Peer to Peer (P2P) networks

We will first introduce the basics of P2P networks in this section and then move on to describing one P2P network algorithm, namely Chord.

P2P networks vary from other networks in that they do not implement the popular client-server model, but use so called peers that can act both as clients and servers. P2P networks consist of symmetric peers that are able to communicate with each other without any centralized server. Either of the communicating ends can initiate a connection to the other peer, which makes P2P networks very scalable and robust. A P2P network can operate normally even if half of the peers go offline for one reason or another.[7]

However, the key point in P2P networks is not two peers that are able to communicate with each other as equals, but rather the type and location of the nodes. Normal home computers become a crucial part of the network topology in P2P networks by taking an active role in delivering network information.[7]

There are many P2P network implementations from which the first big brake through software was Napster, a music sharing program. P2P network technologies have continued to evolve since Napster and have become very popular. We will next take a look at Chord, which is an algorithm used to implement P2P networks, in more detail.[7]

4.1 Chord

The basic problem in P2P networks is how to find a node based on a given key. Chord is one solution to this problem, in fact it only supports one function, which is mapping a given key onto a node.[2]

Chord is a protocol, which describes ways to find locations of keys, and handles joining and more importantly expected and unexpected departure of nodes. We focus on the main protocol of Chord, although many versions and extensions have been developed to it.

There are five basic problems in P2P networks that Chord’s effectiveness is based on. These five problems are load balancing, decentralization, scalability, availability and naming. We will next describe how Chord solves each of these problems.[2]

• Chord provides a degree of natural load balancing by spreading keys evenly among nodes. This is achieved by distributing keys in the same way a distributed hash function would.

• Every node shares approximately the same load in Chord, which makes it evenly distributed and therefore decentralized. This is one of the key points that make Chord robust and hence usable in P2P networks.

• Chord scales well even in larger systems, because the cost of a lookup grows as the log of the number of nodes. Chord’s scalability is especially comfortable in that it does not require any parameter tweaking to achieve this.

• Chord handles joining and leaving of nodes automatically, which guarantees that the respected node always maps on the given key.

• There are no constraints on naming keys with Chord. As a result, the users of Chord are given high flexibility on how they map their nodes onto Chord keys.
5 Session Initiation Protocol (SIP)

There are two main protocols used for session initiation. Those two protocols are SIP [8] and H.323 [9]. SIP is more of an all around protocol, which can be used to session initiation together with various underlying protocols, where as H.323 is focused more on Voice over IP (VoIP). We present SIP and its main functionality in the beginning of this section and later concentrate on how it can be deployed in P2P networks.

SIP is an application layer protocol, which is able to establish, modify and terminate multimedia sessions that can be for instance telephone calls that are established over the internet (IP calls). SIP has also built in functionality for inviting participants to ongoing sessions, such as multicast conferences. SIP also supports adding and removing media on existing sessions. Users of SIP can operate with a single externally visible identifier even if they move around. This is achieved by SIP’s capability to transparently support name mapping and redirection services, which support personal mobility. SIP offers five types of session initiation services, which are user location, user availability, user capabilities, session setups and session management.[8] We next briefly introduce these five services and then move on to SIP in P2P networks.

- User location means the determination of the end system, which is to be used in the communication.
- User availability means acquiring information about the called party’s willingness to engage in communication.
- User capabilities mean negotiating the media type and required parameters to be used in the communication.
- Session setup means the establishment of session parameters at both ends, meaning both the calling and called party.
- Session management includes transfer and termination of sessions, invoking services and modifying session parameters.

SIP can be implemented to P2P networks and it has been the basis for SIPPEER [10], which is a SIP-based P2P Internet Telephony Client Adaptor. SIP is a very interoperable design that can be used in various contexts. This is one of the reasons why there has been some discussion about using SIP in P2P networks. SIP can be used in P2P networks to implement various Distributed Hash Table (DHT) methods, such as peer discovery and user registration.[2] [8] This works by replacing DNS [11] with P2P for the next hop lookup in SIP. We will explore some of SIP’s security related features in the Person to person communication risks in P2P networks section, but other detailed features of SIP are not in the scope of this paper.

6 Person to person communication risks in P2P networks

In this section we further explore the risks discussed in section 3, but from P2P networks point of view. We discuss the possibility of new risks and threats that P2P network environment introduces in addition to the above mentioned risks. We leave the problems that we introduce unanswered in this section and try to suggest solutions to them in the next section.

6.1 Network related problems

Some of the network related problems exist in P2P networks, but many of them are also solved by basic features of P2P networks. We introduce some of these features in the next section.

6.2 Denial of Service

DoS attack is one of the easiest attacks to implement, as we discussed earlier in this paper. Although P2P networks make DoS attacks less feasible, as we introduce in section 7.2, it does not diminish the fact that an attacker can still successfully send large amounts of phony packets to a target, or otherwise try to exhaust target’s resources. The other two types of DoS attacks, destruction or reconfiguration of configuration information and physical destruction or alteration of network components, are also valid in P2P networks.

6.3 Impersonation

Impersonation is an unsolved problem in P2P networks. P2P networks usually handle registration quite loosely, meaning it is not extremely hard to register to a P2P network with another person’s identity. From that point on messages sent to that identity flow to the registrar. This means that there is no built-in feature that would take care of the problem.

6.4 Eavesdropping and Man in the middle

Eavesdropping and Man in the middle attacks apply to P2P networks as well. One can register a computer to a P2P network using SIP’s REGISTER message as stated in [12] and become a gateway for another node to gain access to the P2P network and then capture and forward all packets sent to the accessing node. Eavesdropping can also be done by for example capturing packets sent in the network or being close to the communicating person and listening to what he or she is saying.

6.5 Rogue nodes

Rogue nodes are also a great problem in P2P networks. A rogue node is a node that seems to be following the rules of the network, but is conducting malicious actions in the network. Such actions can for example include one of the attacks introduced earlier in this section.

6.6 Congestion in Distributed Hash Tables (DHT)

A DHT can become congested, which means that some of its nodes become unavailable, because they are serving other request and do not reply to DHT related queries. This can
be achieved by for example using a certain DoS attack called pipe stoppage [14].

### 7 Improvements to security in person to person communication in P2P networks

In this section we discuss how P2P networks solve some of the problems we have introduced in previous sections and how some problems can be solved with different existing protocols. There are also problems that can not be solved by current technologies. We explore some possible scenarios on how to solve the problems in addition to the problems that already have a solution.

#### 7.1 Network related problems

P2P network environment solves some of the network related problems we introduced in section 3. There is no single point of failure in P2P networks, because of their basic structure that takes advantage of distributing network information to various nodes. The remaining part of the network would work normally even if a catastrophe would disable major parts of the network. Single nodes can naturally become unavailable as a result of a local problem, but it does not affect the whole system, which could be the case in regular networks, if the node was a base router for instance.

#### 7.2 Denial of Service and congestion in P2P networks

DoS attacks are never easy to block. P2P networks improve the situation, at least if they are implemented with SIP, but the improvement is only marginal. The improvement is the result of having to register to the network, especially if a PKI [15], which enables the verification of users, has been implemented. Most DoS attacks could possibly be avoided by implementing simple but critical changes to the P2P network topology as presented in [13].

Detection of misbehaving peers is not an easy problem to solve. Making strict rules about succeeding in sending packets to their respective receivers could be one way to improve the situation, but on the other hand it might kick out legitimate users, which can not be allowed. One such example could be to introduce certificate based protection, as discussed in [12]. There are other solutions to this problem, but we present them in the next section, because they are more closely related to impersonation.

Finally, there is no network protocol that could prevent an attacker from destroying someone’s network connectivity by for instance physically damaging the hardware, which leads to the conclusion that DoS attacks can not be totally avoided.

#### 7.3 Impersonation and rogue nodes

Impersonation and rogue nodes are hard to fight against, because it would basically require a large scale ring of trust, which is not easy to accomplish. Registering to P2P networks is the point where validity of a registrar has to be checked. There are possible solutions to making registration more secure. One such solution is to use a PKI. This would solve the impersonation problem. This however leaves the question of a trusted third party wide open, although PKI is widely used in today’s business world, which indicates that the problem can be solved. A PKI system could be introduced so that the public portion of a user’s key would be stored in the overlay, which enables the system to verify that the user is the same user that used the name before [16]. One option would be a global DNS type of system that can be used to validate users [16].

### 7.4 Man in the middle and Eavesdropping

Man in the middle attack can not be avoided, but it can be made more difficult by validating registrars as described in previous section. Peers forward traffic in P2P networks, so there is nothing that stops someone from storing all forwarded data. SIP and other protocols, such as SIPPEER [10] do offer mechanisms for using secure and encrypted traffic in both signaling and media transfer, which is a satisfactory solution to both man in the middle and a part of eavesdropping problems.

Eavesdropping as such can never be prevented, because it can be done by standing next to a communicating person, as we stated earlier. We therefore leave that part of eavesdropping issues unanswered. The other part of eavesdropping problems mentioned refers to eavesdropping, where the attacker gathers data being sent between two or more communicating entities. Even though the attacker is able to receive data, he or she is presented with the problem of decrypting it, which often makes the attack unfeasible.

### 8 Anonymous callers

Anonymous callers are often treated as vulnerability in P2P networks. This is also true in most cases, but it also adds flexibility into the network. Anonymous callers have been partially accepted in PSTN networks by not showing the caller’s number to the receiver, if the caller has this function enabled. There is however no such intermediate as a phone company that can verify the caller, in between two peers in a P2P network.

Constructing P2P networks that have an authentication system of some kind have been discussed shortly in section 7. These methods include PKI and a certificate based approach. Another related approach is discussed in [17]. It is based on centralized security servers that would maintain encryption keys that are needed to open encrypted media on the distributed overlay network [17]. This approach seems scalable, even though it introduces centralization, and could therefore be used in large P2P networks. We believe that one or many of these earlier mentioned methods are probably the direction where P2P networks are headed in the future.

### 9 Conclusion

We discussed some of the basic person to person communication methods in networked environment in the begin-
ning of the paper and concluded that Public Switched Telephone Network (PSTN), GSM and Instant Messaging (IM) are among the most popular methods. We therefore focused our attack analyses into attacks that are common in those environments, which are Denial of Service (DoS), Impersonation, Man in the middle and Eavesdropping.

Next we introduced protocols related to our chosen architecture, which consists of P2P networks and SIP. We introduced Chord as an option for managing and distributing keys in P2P networks. We then introduced SIP as the underlying protocol for handling signaling in our P2P networks and analyzed the impact it has on our security related structure.

After discussing the underlying protocols and threats against the architecture we introduced the risks in person to person communication in P2P networks, which added rogue nodes and congestion in DHTs into the risks that we discussed earlier. We then introduced how P2P environment solves some of the introduced problems and finally discussed improvements to the remaining problems.

P2P networks and SIP solve some of the introduced problems, but there are also problems that are left unsolved. We discussed various solutions to some of the problems and concluded that some problems remain unanswered due to the easiness of implementing some of the discussed attacks. The latter problems include eavesdropping, where the attacker is close to the target so he or she can follow the conversation. Another problem that is left unsolved is preventing DoS attacks, because they can be implemented in various environments and by various methods.

We do however believe that many if not most of the problems presented could be avoided by introducing some kind of an authentication system. The downside is that it might introduce some overhead into the network. The question to be answered is therefore about drawing the line between security and scalability.

References


