General Security Concept for Embedded P2P Systems

Stefan Kraxberger
Institute for Applied Information Processing and Communications
Graz University of Technology
Graz, Austria

Udo Payer
Institute for Applied Information Processing and Communications
Graz University of Technology
Graz, Austria

Stefan Tillich
Institute for Applied Information Processing and Communications
Graz University of Technology
Graz, Austria

ABSTRACT

The importance of P2P systems in real-world applications has grown significantly over the recent years. Although P2P systems have found its way into almost every field of application the lack of an adequate general security concept, research for specific security mechanisms and implementations of possible security improvements is still limiting their full potential. We are focusing on getting an overall view on the security of embedded P2P systems and on finding promising mechanisms and solutions to this challenging task. This work tries to make the first step towards secure heterogeneous pure P2P systems by specifying an appropriate overall security concept.

Categories and Subject Descriptors

C.2.0 [**Computer Communication Networks**]: [security and protection]

General Terms

Security

Keywords

security, p2p systems

1. INTRODUCTION

The idea of peer-to-peer (P2P) systems has been around for a long time and also the *Internet* itself was conceived as peer-to-peer system in the first place [2]. It can be said that the Usenet is the first implementation of a P2P system since it copied files between computers without central control. Another important system, the Domain Name System (DNS) makes use of P2P principles and its request/response mechanism is so simple, efficient and scalable thus many routing protocols made use of these mechanism. In the late 90's, as the Internet expanded in unprecedented manner, the prevalent networking concept became the client-server model since the use-case patterns of the Internet changed towards more asymmetry and centralization. The client-server model was therefore the straightforward choice at that time. But at the beginning of the new century, with linear growing Internet users [4] and exponentially growing network traffic [5], the client-server model was not able anymore to deliver the anticipated network transfer rates.

This was the time as the first file sharing clients appeared which used the P2P concept to achieve higher transfer rates and faster downloads as it is able with the *traditional* client-server model. The first file sharing application has been Napster, which became very fast very popular. Shortly after, the P2P concept has been applied to applications from almost every domain, not only to file sharing, and also several variations of the P2P concept itself have been introduced. Therefore, basically mechanisms on how data can be stored redundantly, retrieved faster and how peers can be organized have been studied. But research on how peers can interact securely or the whole P2P system itself can be made secure is in its infancy. But even worse, most of the *secure* approaches only apply concepts from the client-server model to the P2P world which are obviously not adequate. This means that at this point no overall security concept for P2P systems exist which addresses the relevant topics in a P2P manner, thus leaving them vulnerable in real-life scenarios. We are currently designing and developing such an concept for heterogeneous pure P2P systems. We are trying to accomplish that in several steps starting with the specification of general concept on security levels.

Therefore, the target of this work was to design and specify a general security concept for embedded P2P systems. Existent security concepts are only intended for structured P2P networks with no or are not applicable for heterogenous pure P2P networks. The security concept which we are envisioning takes the broad range of different devices into account which must be able to participate in such a embedded P2P system. Therefore, an important aspect of the design is the search and definition of security primitives and mechanisms which can also effectively be used on systems with limited resources like embedded devices or sensor nodes(e.g. computation power, amount of available memory and energy, etc.).

2. RELATED WORK

The first research work which addressed security on several levels in P2P systems was the one from Castro et al. [1]. This work deals with structured P2P networks and routing security in the context of distributed hash tables (DHT). In

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3892
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3892

this paper some general ideas about how to achieve a secure P2P system are stated. They identified 3 requirements for secure routing which in their case are secure assignment of node IDs, secure maintenance of the routing table and secure message forwarding. They also investigated the impact of different attacks on structured P2P systems and the efficiency of their solution. But since they are only dealing with structured P2P systems and they are not taking embedded systems into account this work can only provide some basic advice according the secure node ID generation which will not be covered in our work since we do not allow for dynamic peer ID generation.

A similar structured P2P network approach with slightly different architecture which also addressed the 3 requirements as pointed out by [1] is the one from Wang et al. [6]. Instead of using a ring topology for the P2P system they based their system on the Internet Autonomous System Topology in which the peers are organized by their physical network locality. In this approach the peers are grouped together into teams as their basic unit. In the proposed system only selected peers perform routing activities. Instead of using IP addresses in conjunction with certificates and node IDs they propose to use a network physical characteristic, called net-print. The reliance of the IDs on the RTT to selected routers as a trustworthy component is disputable. The other requirements are addressed in a similar manner as in [**?**].

The well-known P2P framework JXTA also states to be a secure P2P network [7]. JXTA makes use of well known mechanisms like SSL/TLS [3], X.509v3 certificates and other common security primitives, protocols and standards. Nevertheless, these mechanisms are used only for point-to-point encryption and for peer authentication. There are no secure routing primitives or any special authentication mechanisms for group security. No general security concept exists which addresses the security requirements, as stated in [1], directly in the JXTA framework. There are no explicit mechanisms to protect the P2P network against attacks from adversaries or threats from misbehaving and selfish peers. The primary goal of JXTA in terms of security is to provide cryptographic primitives (encryption, digital signatures, hashing, ...) as service the to the application layer.

These projects have started to think about a security concepts for P2P network in the one way or in the other. Nevertheless, either the concepts and mechanisms are to specialized or to general. Therefore, we are trying with this research to provide a consistent security concept for embedded P2P systems.

3. P2P SECURITY CONCEPT

We are currently developing an embedded P2P system which has been designed with an adequate security concept as its basis. This security concept takes into account the special requirements of embedded P2P systems. The most importation requirement is scalability. This means that the security concept must be able to be applied to peers ranging from workstation class to wireless sensor nodes. This already identifies the second requirement mobility. Since, also mobile peers can participate in our embedded P2P system the underlying mechanisms (especially routing) must be able to cope with a changing environment in a secure and efficient manner. The last requirement is transparency. Since we peers with different capabilities participate in the embedded P2P system the security level which can be achieved for a specific communication session with a distinct peer must be obtainable in advance. The security concept for the P2P system features two domains of security, which are closely related.

- Routing security
- Group security

Both domains will be considered with the same basic *group* concepts in mind. A group is simply a virtual aggregation of an arbitrary amount of peers which follow the same rules (policies?) and use the same protocols. Every peer can communicate with any other peer inside a group. Routing security will be regarded in terms of a *base group* or a *default group*. Every peer belongs to this default group after he has joined the P2P system. All of the routing aspects are managed inside of this group because every peer can be used to find paths to other peers. Thus, the following security aspects apply to both domains.

1. Establishing secure communication
2. Performing secure communication
3. Upholding secure communication

Point 1 relates to the secure joining of peers, where the new peer and an existing group member perform mutual authentication with their credentials. When the new peer successfully joins the group, it will be provided with a secret key which is shared amongst all group members (session key). With this session key, members of a group can communicate securely (point 2). In the context of routing security, this means that the P2P routing information is protected with the session key. In the context of *normal* groups, all group messages are protected with the session key. The benefits of a session key are that it can be updated to protect against side-channel attacks or to exclude misbehaving nodes from the P2P system. Point 3 relates to how to prevent and limit damage from exposed session keys.

3.1 Security levels

The overall security for the P2P system can be set individually for routing and each group on three separate axes. These three axes conform to the three group security aspects given above.

- Admission security (entity authentication and authorization)
- Data security (message authentication and confidentiality)
- Session key protection (rekeying and local side-channel attack countermeasures)

For each axis, three levels of security are defined as stated in the following figure.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3892
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3892

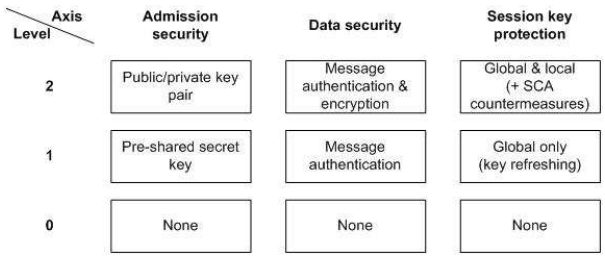

Figure 1: Levels of security

Each box contains the security measures for a specific axis under a specific security level. For example, data security level 2 demands that each message within a group needs to be authenticated and encrypted with the current session key of the group. Admission security refers to joining the P2P system or groups. Data security refers to the the protection of the data payload for routing (i.e. the routing information) or for the group communication. Session key protection refers to how the session key of a group is protected from being learned by an attacker (e.g. through means of side-channel attacks) and how to limit the damage in case that an attacker actually gets hold of the session key.

For practical applications the following combinations of security levels can be considered as principally sensible:

Admission Security	Data Security	Key Protection
0	0	0
1	1	0
1	1	1
1	1	2
1	2	0
1	2	1
1	2	2
2	1	0
2	1	1
2	1	2
2	2	0
2	2	1
2	2	2

Table 1: Practical possible security levels

The other possible combinations are either invalid (e.g. enabled session key protection without an available session key) or not sensible from a security standpoint (e.g. enabled data security without admission security). The three axes and the corresponding security levels are explained in more detail in the following sections.

3.2 Admission security

Credentials for admission security regarding routing and groups fall into one of the following two basic categories:

- Pre-shared secret key (admission security level 1)
- Individual public/private key pair for each peer, authenticity of public key is established by certification with a global public/private key (admission security level 2)

For joining the P2P system (routing security) and for securing each single group, one type of credential must be selected. Pre-shared secret keys simplify the process of establishing session keys, but they bear a higher potential damage to the security in the case of their exposure. Individual public/private key pairs require more complex cryptographic primitives and protocols, but they limit the damage of key exposure and can even allow for the exclusion of misbehaving peers from groups and/or the embedded P2P system.

The credentials are included statically in the P2P application which must be delivered in a secure fashion onto the respective target device. The list of authorized members of groups is therefore by default static with the following exceptions:

- New devices supplied with the appropriate credentials enter the P2P network
- A key validation service can provide dynamic authorization for groups and/or the whole P2P system

With individual public/private key pairs for group security, there are several options for static authorization of peers:

- A single key pair with an attribute certificate of the public key containing the list of groups which can be joined
- A separate key pair per peer for each group, where the public keys for the same group are certified with a different group public/private key pair

Moreover, individual public keys could be authenticated and authorized dynamically by an additional service, therefore allowing for dynamic group management and the exclusion of misbehaving peers. In the authentication process for joining the P2P system or a specific group, the credentials are used in a mutual authentication protocol (e.g. three-way challenge-response) and then used to communicate the session key to the new peer. In order to join a group, a peer must have the required credential. In order to join *normal* groups, a peer must be already a member of the P2P system (i.e. in the possession of the routing credentials). The group then authorizes entry of the peer into the group or denies it. Authentication and authorization should be possible with every member of the group. The default decision for admission will be based statically on the presented credentials. An additional dynamic group authorization service is possible but currently out of the scope of our research.

3.3 Data security

Once a device has joined the P2P system (routing security) or a group (group security) through successful authentication and authorization, it will receive the corresponding session key. The session key is used to protect the data exchanged within the group (P2P routing information or group communication) via the unprotected network infrastructure. The data must be at least authenticated (as originating from an authentic peer or group member). This corresponds to data security level 1. Optionally, the data can also be encrypted which refers to data security level 2.

3.4 Session key protection

Session key protection involves two strategies.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3892
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3892

- Hardening the extraction of session keys from devices via side-channel attacks
- Limiting the value of session keys learned by an attacker

As the session keys will be the most frequently used ones, they will also be the most vulnerable against side-channel attacks. Side-channel resistant implementation of the cryptographic primitives can be included in peers which are expected to be subject to side-channel attacks. Periodic refreshing of the session key decreases the chance of successful side-channel attacks and can be used to limit the damage of exposed session keys.

At session key protection level 0, the session key is never refreshed. At level 1, the session key is refreshed at certain intervals. Session key protection level 2 additionally uses side-channel resistant implementations of the cryptographic primitives on the respective peer.

The admission credentials (pre-shared secret key or private key) will be protected by use of the same side-channel attack resistant implementations as the session key when level 2 of session key protection is enabled.

3.5 Global security considerations

The basic assumption for P2P system security is that most of the authenticated peers will be well behaved. Attackers which are in the possession of some credentials for the P2P application (malicious insiders) will be considered as an exceptional case. They must be detected by the peer or network monitoring modules by identifying suspicious behavior (e.g. dropping of packets). Depending on the type of credential and the available security services, the attacker can be excluded from the P2P system (see Section Dealing with exposed credentials). Attackers without proper credentials (malicious outsiders) cannot participate in the P2P network and are restricted to attacking the raw communication infrastructure.

3.6 Dealing with exposed credentials

The following list contains obtainable credentials and the appropriate countermeasures to exclude an attacker which is in possession of such a credential.

Obtained credentials	Exclusion measure
Group session key	Negotiation of new group session key Group entry denied by dynamic key validation service
Routing session key	Negotiation of new routing session key P2P system entry denied by dynamic key validation service
Peer private group key	Negotiation of new group key
Peer private routing key	Negotiation of new routing key
Group pre-shared key	N/A
Routing pre-shared key	N/A
Global private key	N/A

Table 2: Measures against security breach

The above list contains the credentials with increasing severity of their exposure. Therefore, more critical credentials must be better protected against disclosure, e.g. by side-channel attack countermeasures. Also notable is that the disclosure of a private key can only be remedied with the help of a dynamic key validation service, which can revoke public keys at runtime. Attackers which possess authentic credentials and exhibit no apparent misbehavior cannot be detected by the P2P system.

3.7 Selection of security levels

For a specific P2P application, the selection of security levels can be done on several levels (globally, group-wise, or locally). As secure routing is a basic service underlying the whole P2P system, the routing security level is a global decision. Therefore, the admission security level and data security level for routing must be set globally. Furthermore it must be decided globally, whether the session key protection level for routing is set to 0 or not.

Group security levels are set group-wise. Most of the group security levels are decided by the group creator. This includes the admission security level and data security level for a group. Also the decision for a session key protection level of the group of 0 or 1/2 is done by the group creator. In both cases, for a session key protection level unequal to 0, each peer can feature individually level 1 or 2, as this involves only local differences of the implementation of the cryptographic primitives. The decision should be based on the degree of exposure to side-channel attacks.

4. CONCLUSION

Our work is the first step towards an general security concept for embedded P2P systems which are heterogenous in nature. We have divided the concept into two parts. A routing security concept and a group security concept. Both concepts are based on the same underlying understanding of a group. The routing concept currently is aware of one *base* group whereas the group security concept can handle an arbitrary amount of groups without breaking the security policies. We have also specified the different security levels which can be achieved using this concept, which are numerous, through the usage of different type of cryptography. Since not only the desired strength of the used cryptographic mechanisms is relevant in context of embedded P2P systems but also their resource requirements, in terms of computational power, memory and energy, one can easy determine the best combination of mechanisms and the corresponding security level by using the described security concept. Therefore, our work helps future middle-ware and applications designers and developers to select the appropriate cryptographic mechanisms and are able to specify a security level for their system.

5. OUTLOOK

In future we would like to extend the routing security concept to be able to handle an arbitrary number of groups. This means that it should not only be able to route information using the peers of the *base* group, which indeed are all the available peers, but rather to route messages only inside of group members or secure it in a way that only group members are able to read critical information which should be protected because of privacy or confidentiality matters.

We also would like to explore the benefits of using identity based cryptography in our security concept. Since, the highest security level requires the usage of public key cryptogra-

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3892
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3892

phy , although the performance of using computational expensive cryptography for embedded systems must be tested first. But research indicates that it is at least possible to perform this kind of cryptography even on wireless sensor nodes, which are the devices with the lowest computational power we intend to use for our embedded P2P network.

6. REFERENCES

[1] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D. S. Wallach. Secure routing for structured peer-to-peer overlay networks. *SIGOPS Oper. Syst. Rev.*, 36(SI):299–314, 2002.

[2] S. Crocker. Host software. RFC 1, Internet Engineering Task Force, April 1969.

[3] T. Dierks and E. Rescorla. The transport layer security (tls) protocol version 1.1. Technical Report 4346, Internet Engineering Task Force, April 2006. Updated by RFCs 4366, 4680, 4681.

[4] Miniwatts Marketing Group. Internet growth statistic. Internet, December 2008. `http://www.internetworldstats.com/stats.htm`.

[5] A. Odlyzko. Internet traffic growth: Sources and implications, 2003.

[6] H. Wang, Y. Zhu, and Y. Hu. An efficient and secure peer-to-peer overlay network. In *LCN '05: Proceedings of the The IEEE Conference on Local Computer Networks 30th Anniversary*, pages 764–771, Washington, DC, USA, 2005. IEEE Computer Society.

[7] W. Yeager and J. Williams. Secure peer-to-peer networking: The jxta example. *IT Professional*, 4(2):53–57, 2002.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2008.3892
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2008.3892