[MeWoHoSt01] *Andreas Meissner, Lars Wolf, Matthias Hollick, Ralf Steinmetz;* **Security Issues in Group Integrity Management for Multimedia Multicasting;** Third International Conference on Information, Communications & Signal Processing (ICICS 2001), Singapore. Nanyang, October 2001, CD.

Security Awareness in Service Discovery for Multimedia Collaboration

Matthias Hollick
GMD - German National Research Center for Information Technology
Institute IPSI, Dept. MOBILE - Mobile Interactive Media
Dolivostraße 15, D-64293 Darmstadt
Phone +49-6151-869-847
matthias.hollick@darmstadt.gmd.de

ABSTRACT

Multimedia capable devices for professional and private use grow digital these days. With the advent of short-range wireless communication capabilities, these devices gain new potentials such as enabling seamless collaboration within groups of devices. As a side effect of these technologies, new problems emerge, especially in the area of security. This paper focuses on security issues when forming (peer)groups among these devices. Our primary goal is to establish security awareness via the service discovery process. We show that the combination of the pure Internet Protocol and today's state of the art service discovery protocols lacks the necessary features for solving the problem described. We introduce a novel design of a service discovery system as a solution for security aware ad-hoc usage.

Categories and Subject Descriptors

C.2 [**Computer-Communication Networks**]; C.2.0 General--Security and protection; C.2.1 Network Architecture and Design--Wireless communication protection; C.2.2 Network Protocols--Applications.

General Terms

Management, Design, Reliability, Security, and Human Factors.

Keywords

Zero-configuration, Multimedia, Service Discovery, Service Location Protocol, Security, and Ad-hoc Networking.

1. INTRODUCTION AND MOTIVATION

Multimedia capable devices for professional and private use grow digital these days. However, they are mostly stand-alone solutions and use different types of storage media and communication interfaces to exchange their recordings. The internetworking of multimedia devices introduces new usage paradigms, especially with the advent of short-range wireless communication capabilities. As an example, we will look at the collaboration among groups of devices. Also, as a side effect of these technologies, new problems emerge, for example in the area of security. Traditionally, security is built upon trust relationships and the corresponding authentication of users and/or devices. This allows distinguishing between valid and invalid use of services and permits access control. In ad-hoc communication the mapping of trust relationships from the real world to the digital domain cannot be performed easily. There may be no online authorities available, or the dynamic nature of the association may inhibit the use of extensive communication.

Our goal is to establish a secure enclave or community on top of a network with uncertain security properties, allowing for service discovery. Real world examples include personal area networks or spontaneous networks formed by nomadic users spanning multiple devices within one or multiple administrative domains. We approach the problem assuming an IP-based network. The ad-hoc situation advocates the use of dynamic and autoconfigured IP-addresses as a first step. Thereafter, service operations are the glue actions between the hosts. Within our framework, they form the base mechanism to establish the notion of trust and precede the discovery of appropriate services.

Starting with a capability and security evaluation of IP autoconfiguration, we subsequently describe the foundations of the Service Location Protocol (SLP), which represents a state-of-the-art approach towards service discovery within IP-networks. Thereafter, we describe our novel framework to pinpoint security issues of ad-hoc communication using the service discovery process.

2. IP AUTOCONFIGURATION

IP autoconfiguration is a feature in both IPv4 and IPv6. While being an add-on to IPv4 it is a default feature in IPv6. RFC 2462 describes the steps to autoconfigure itself in IPv6 [12]. This process is composed of a few actions only. The system first creates a link-local address, and secondly, verifies the uniqueness of this address. After that, the system determines what information to autoconfigure: Addresses, other information, or both. To do so, RFC 2461 defines the neighbor discovery protocol - a conceptual model of a data-structure organization that a host maintains in interacting with neighboring nodes. Neighbor discovery distinguishes the whole configuration process in *stateless*, *stateful*, or a *combination* of both. Stateful configuration incorporates a DHCP server to handle state [2]; stateless configuration is left entirely to the hosts, while the combination may use a router to advertise routing prefixes and leaving the generation of the host part of the address to the system itself.

If we assume a pure ad-hoc network, the communication among hosts attached to the same link is possible after the generation of a stateless link-local address. The duplicate address detection algorithm queries all hosts attached to the link if the chosen address is already in use. An adversary listening on the same link and roughly answering the discovery messages can attack the availability of stateless autoconfiguration. As a solution, neighbor discovery messages can be protected using the IPSec Authentication Header mode [1]. However, if we assume hosts communicating in a pure ad-hoc environment there will be most probably no pre-existing security association and no easy way to establish one. As opposed to the ad-hoc situation, a partly or fully managed network may introduce preconfigured security associations at the expense of spontaneity. To summarize, autoconfiguration in IP can only be secured if manual pre-configuration exist.

3. SERVICE DISCOVERY AND SECURITY

In the real world the concept of trust is the most important basis for security awareness between persons. To bridge the gap between reality and the digital realm we have to translate this notion of trust [13]. Our approach uses the service discovery process in analogy to the human perception of the surrounding world. Service discovery, being the core of the security process in ad-hoc environments, requires inline security and reliability.

In [7] a summary of security mechanisms for service discovery is presented. In the following we consider aspects of availability, authenticity and privacy as necessary for the data-plane. Availability, confidentiality and integrity should be regarded as crucial for the communication circumstances.

Since the basics of service discovery for ad-hoc environments are well known and differ only slightly in various protocols, we take the Service Location Protocol (SLP) as an example for the following discussion.

The Service Location Protocol was designed to alleviate the administrative burden and to allow quick adoption to ad-hoc situations [3] [4]. SLP dynamically publishes and retrieves service information. To do so, SLP introduces User Agent (UA), Service Agent (SA) and Directory Agent (DA), which are related to application processes. The UA acts on behalf of the user to request and retrieve service information from a DA or SA. The SA advertises one or more services. The DA operates as a service information cache, which collects service advertisements and, as a result, allows for better scalability. The service information is described using Uniform Resource Locators (URLs). The data structure comprises unique service types and description attributes, which are defined within so-called service templates.

SLP has only weak security mechanisms. A threat analysis can be found in [6]. Essentially the only security features SLP supports are the authenticity and integrity of service information. These rudimentary features are based on pre-established security relationships. The availability and reachability of the protocol entities is partially assured using multicast mechanisms, which increase the robustness of the protocol. The requirements we demand in a security aware SLP are shown in Table 1. Herein, we distinguish the security goals for the control plane (communication circumstances) and the data plane (data) of the protocol. We consider the security goals as a strong basis. However, there may be scenarios where the goals described are not strong enough.

Table 1. Security goals for Secure SLP

Property	SLP	Secure SLP
Integrity (data)	Optional	Yes
Authenticity (circumstances)	Optional	Yes
Confidentiality (data)	No	Negotiation
Anonymity / Pseudonymity (circumstances)	No	Negotiation
Hiding, covered communication (data)	No	No
Unobservability, untraceability (circumstances)	No	No
Availability (data)	Partially	Partially
Reachability (circumstances)	Partially	Partially
Nonrepudiation (circumstances)	No	No

3.1 A Framework for Secure Service Discovery

To address the problems mentioned above, we start with the protocol facilities the service location protocol provides and thereafter introduce additional components, policies and semantics to enhance the process of service discovery and allow for additional security measures. For the ad-hoc usage scenarios we investigate, there will likely be no DAs. Therefore, and due to space constraints, we will limit our discussion to cover the direct information exchange between UA and SA only. In the Following we give a brief outline of the protocol modifications to bring in security.

To allow for confidential service information we introduce security groups and take for granted that SLP can be combined with cryptographic means to ensure confidentiality within security groups. The left pane in fig.1 depicts the SLP standard interaction using the so-called direct mode (without DA), which represents an end-to-end communication. The right pane of fig. 1 illustrates security groups, which are indexed with the letters a, and b. If we assume confidential communication inside these groups, an outside attacker would have no possibility to eavesdrop or to inject false service information. However, in the case of our secure SLP, we convey the security problem to the secure establishment of the security groups.

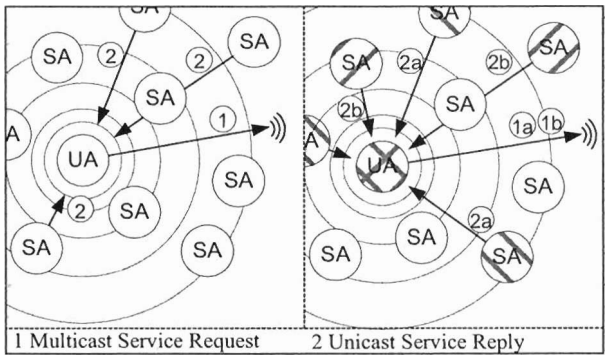

Fig. 1. SLP Operation With and Without Security Groups

Military history as an analogy demonstrates that knowing about friends and enemies is crucial for security. Imagine radar stations

used to reveal airplanes on the battlefield: The knowledge about speed and direction and a genuine identification, if available, let the operator decide how to react. To solve our problem of establishing security groups, we thus first have to identify which SAs we trust. To do so, we may use pre-established security relationships for all our personal devices. For unfamiliar devices we have to learn about their behavior. Our findings if services are "good" or "bad" lead to a transaction history each UA keeps locally. This history expresses the reputation we attribute to the system or service in question.

3.2 From Default Mode to Secure Mode

Due to space constraints we describe only one part of the design in detail. We focus on the transition from insecure to confidential mode of the protocol. Provided that we know about the trustworthiness of given SAs we have to establish a secret between all members of the prospective security group. The cryptographic primitives of a shared secret among all group members are out of scope for this contribution. Nevertheless it is of utmost importance to insure the validity of the initial keys using appropriate mechanisms to prevent active attacks (e.g. man-in-the middle attacks).

Having introduced these basic assumptions, we extract the correct chronological order of protocol interactions involved. These steps are partly depicted in figure 2 below and described in detail in the following. As a prerequisite we presume that all hosts can communicate sharing the same link to be able to build upon IP autoconfiguration. The steps are illustrated assuming a pull model originating at the UA:

1) Query the SA for public information about the security policy.
2) Match the own policy against the SAs policy. Include user interaction if necessary.
3) Exchange secrets to allow for confidentiality against outsiders (not necessarily coupled to the assurance of authenticity of the communication partner!).
4) Switch to pair-wise confidential communication mode, e.g. using IPSec.

As a result a secure communication, which assures that the entities talk to the same (not necessarily authentic!) communication partner for the rest of the process can be guaranteed. If the entities cannot match their policy the normal (insecure) SLP operations can be employed.

Depending on whether we want to perform access control on a per-user/-device or on a per-group of users/devices basis, we have to choose an appropriate key exchange method. To perform access control different mechanisms can be used. A federation of one principal and multiple devices may use a form of imprinting as described in [10] to ensure the authenticity of the communication partner. For a group of principals with multiple devices these administrative domains can be brought together with group based paradigms like join/invite messages from a master, or elections among the actual participating hosts if new hosts request to join the secure group. Moreover, mechanisms like community based service location or the resurrecting duckling model in [11] can be applied to the scenario. To finish the steps of protocol interactions:

5a) Peer mode (only one UA and one SA) can start to enforce access control and will continue to communicate confidentially.

5b) Group mode access control will give the privileges depending on group membership (security domain or group). Since secure multiparty communication using multicast is out of scope of IPSec, a separate mechanism has to be specified. Having established a common secret, the group has to switch to confidential multicast communication.

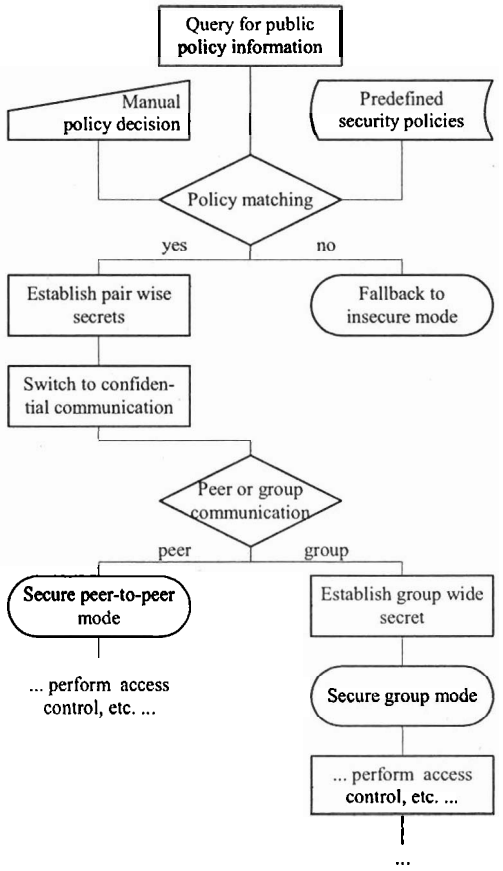

Fig. 2. Partial Decision Diagram to Establish Secure Service Discovery with SLP

At the implementation level the Service Location Protocol has to be enhanced to allow for access control and confidential communication:

- We make a distinction between public and private service information. The public information is used to be compatible to SLP and mapped to the default scope.

  We misuse the scope feature of SLP to distinguish between private and public information. The scopes will be negotiated dynamically between UA and SA and present only a logical boundary. A second cryptographic security boundary is en-

forced using IPSec or a proprietary group communication approach.

- UA and SA need to be able to agree upon a secret. To counteract man in the middle attacks there have to be ways to ensure the validity of this secret.
- We propose the use of SLP to distribute certificates. Since we expect no Certificate Authority in reach, these may be self-signed. To do so, a mapping between X.509 certificates to SLP attributes is underway.

4. CONCLUSION

Internetworking of multimedia devices in ad-hoc environments allows for new forms of applications. The acceptance of such collaborations of multimedia devices depends largely on usability and security issues. Any solution or implementation will have to negotiate spontaneity against security. To solve the problem, we have motivated and illustrated a novel approach that makes use of service discovery, which aids in creating spontaneous security groups in ad-hoc environments. Moreover, our approach supports the introduction of security into the service discovery process to allow for classified service information for closed groups. The semantics we use can be demonstrated using a metaphor of our everyday live; where we interact with different people, friends and strangers based on our perception of trust and confidence. Our approach allows partly translating this into a digital world and helps dealing with the problems and security threats in this digital world. The history of previous actions is collected at each host and provides a sense of reputation [8].

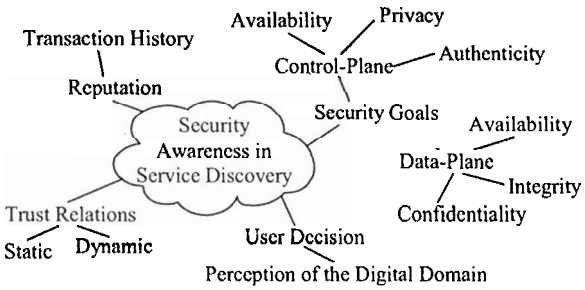

Fig. 3. Mind-Map of Security Awareness in Service Discovery

A condensed synopsis of the parameters of our framework is depicted in fig. 3. Thus we conclude: "*Security aware service discovery defines the task of finding appropriate information of the existence, location, base and security configuration of networked services, emphasizing and facilitating the perception of security within the digital domain*".

We assume that there will be no automatic solution to deal with trust and confidence within ad-hoc environments. Since the user will often initiate the service discovery process, he will likely interpret the answer and the corresponding security parameters and supplement the process of gathering information. This introduces the perception of context and situation.

5. ACKNOWLEDGMENT

This work is funded by the German Research Council (DFG) as part of the program Security in Information and Communication Technologies within the SECCO project.

6. REFERENCES

[1] Kent, Atkinson; Security Architecture for the Internet Protocol, Proposed Internet Standard RFC 2401; November 1998.

[2] Jim Bound, Mike Carney, Charles E. Perkins, and Ralf Drohms; Dynamic Host Configuration Protocol for IPv6 (DHCPv6); Internet Draft, draft-ietf-dhc-dhcpv6-18.txt; April 2001.

[3] Erik Guttman, Charles E. Perkins, and Michael Day; Service Location Protocol, Version 2; Proposed Internet Standard RFC 2608; June 1999.

[4] Eric Guttmann; Service Location Protocol: Automatic Discovery of IP Network Services; IEEE Internet Computing 3(4), pp 71-80; July 1999.

[5] Matthias Hollick; Secure Service Centered Networking for Nomadic Usage; In Communications and Multimedia Security Issues of the New Century, IFIP TC6 / TC11 Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01), Darmstadt; May 2001.

[6] Matthias Hollick; Security for Ad-Hoc Service Information Threat Analysis of the Service Location Protocol; Technical Report available at <http://www.darmstadt.gmd.de/mobile/projects/secco/pub>

[7] Matthias Hollick; A Synopsis on Security for Service Discovery in Ad-Hoc Environments; Technical Report available at <http://www.darmstadt.gmd.de/mobile/projects/secco/pub>

[8] Richard Lethin; Reputation; In Peer-to-Peer - Harnessing the Benefits of a Disruptive Technology, edited by Andy Oram, O'Reilly, pp 341-353; March 2001.

[9] E. Nordmark, W. Simpson; Neighbor Discovery for IP Version 6 (IPv6), Proposed Internet Standard RFC 2641; December 1998.

[10] Frank Stajano; The Resurrecting Duckling - what next?; In B. Christianson, B. Crispo and M. Roe (Eds.); Security Protocols, 8th International Workshop Proceedings, Lecture Notes in Computer Science; 2000.

[11] Frank Stajano, Ross Anderson; The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks; In B. Christianson, B. Crispo and M. Roe (Eds.); Security Protocols, 7th International Workshop Proceedings, Lecture Notes in Computer Science; 1999.

[12] S. Thomson, T. Narten, IPv6 Stateless Address Autoconfiguration; Proposed Internet Standard RFC 2642; December 1998.

[13] Marc Waldmann, Lorrie Faith Cranor, and Avi Rubin; Trust; In Peer-to-Peer - Harnessing the Benefits of a Disruptive Technology, edited by Andy Oram, O'Reilly, pp 242-270; March 2001.