[HoSt01] *Matthias Hollick, Ralf Steinmetz;* **Security Goals for Service Discovery in Ad-hoc Environments;** International Conference on Software, Telecommunications and Computer Networks (SoftCOM 2001), Split, October 2001, S. 1025-1032.

SECURITY GOALS FOR SERVICE DISCOVERY IN AD-HOC ENVIRONMENTS

Matthias Hollick [1], Ralf Steinmetz [2]

[1] Fraunhofer Institut für Integrierte Publikations- und Informationssysteme,
Dolivostraße 15, 64293 Darmstadt, Germany
[2] Darmstadt Technical University, KOM,
Merckstrasse 25, 64283 Darmstadt, Germany

matthias.hollick@ipsi.fraunhofer.de, ralf.steinmetz@kom.tu-darmstadt.de

Abstract: *Networked services are a key component of forthcoming networking paradigms. The advent of ad-hoc and proximity environments gives good reason for service discovery to support (zero)configuration of devices and services. However, the uncertainty of security issues concerning service information presents a major obstacle. This paper substantiates the most important security concerns coupled to service discovery within ad-hoc networks. A close inspection of state of the art technologies of service discovery/lookup protocols and frameworks with respect to their security mechanisms leads to a revised understanding of the problem area.*

KEYWORDS: Ad-hoc Networking, Security, Service Discovery, Service Lookup, and Zero-configuration.

INTRODUCTION

The Internet is expected to receive the impact of millions of mobile and wireless devices in near future. Not only the 3rd generation of cell-phones, but also the steadily growing community of small and independent devices, using wireless local and personal area networks built on top of IEEE 801.11 or Bluetooth have to be taken into account. The wireless Internet presents a challenge, which is driven by nomadic and mobile users, small and pervasive - sometimes autonomous - devices, and ad-hoc and proximity networking with nearly ubiquitous coverage.
In this context the problem of finding appropriate information, to configure devices and services, presents a major challenge. But not only the simplification of the configuration process has to be considered. To allow for omnipresent service availability new and immense security issues have to be taken care of. These security questions remain mostly unnamed today, but have to be solved, once large-scale deployment of wireless Internet devices begins.
The remainder of this paper comprises four sections. Section 1 gives a brief motivation of our work. Next we introduce a common viewpoint on security goals for service discovery. Section 2 presents a conscious evaluation of security mechanisms in today's service discovery protocols and discusses which security goals should be available to allow for a secure service discovery process.

1 MOTIVATION

Service Discovery has its root in the beginning of internetworking systems. The early hosts in the Internet offered dedicated services and used fixed name to address mappings. Influenced by the

evolution from a mostly static Internet towards a dynamic structure, service discovery incorporates well-known ports, central repositories or dynamic service discovery protocols. Heading towards self-configuring networks and hosts, based on Internet-technology, various steps have to be taken. The first step necessary involves the IP configuration of the interface. Next the resolution of host names and, optionally, the allocation of multicast addresses may be of interest. The last and maybe most important issue is coupled to service discovery. The special needs of ad-hoc environments are mainly addressed by actual service discovery protocols.
Our investigation does include today's protocols related to zero-configuration and service discovery for networked services in ad-hoc environments. These are the Service Location Protocol (SLP), the Universal Plug and Play Simple Service Discovery Protocol (SSDP), the service discovery within Salutation and the Secure Service Discovery Service (SDS). Moreover we investigate the JINI Lookup Service and the Bluetooth Service Discovery Protocol (SDP).
In addition we analyze the Domain Name System Security Framework (DNSSec) because of its well thought out security processes related to name resolution and service lookup for public information. We will not consider protocols like LDAP or directory services like the Novell Directory Service (NDS) or Microsoft Active Directory (AD) deeply, because they are inadequate for ad-hoc usage.

2 SERVICE DISCOVERY PROTOCOLS AND SECURITY

Our investigation addresses the different security building blocks of the protocols and frameworks mentioned above. Most of the protocols use client-server mechanisms. In the spirit of multilateral security, we consider the security perspective from client side and from server side, assuming that there may be malicious clients and servers to protect against. Moreover, we consider the combined perspective of client and server against outside attackers.
Protocols often can be distinguished in a control-plane, which carries out the establishment of a proper communication channel (communication circumstances) and a data-plane, which deals with pulling or pushing data between the protocol entities. We consider this categorization as applicable for all protocols in question, even if the protocol specifications do not mention this distinction, because the security goals differ significantly for both planes. The security metrics we evaluate against (see fig. 1) are derived from several works in the area of security. In the context of multilateral security Wolf and Pfitzmann establish a characteristic of security goals, which present a useful starting point [WP00]. In Section 2.8 we will use application scenarios to describe the meaning of the security goals in relation to service discovery.

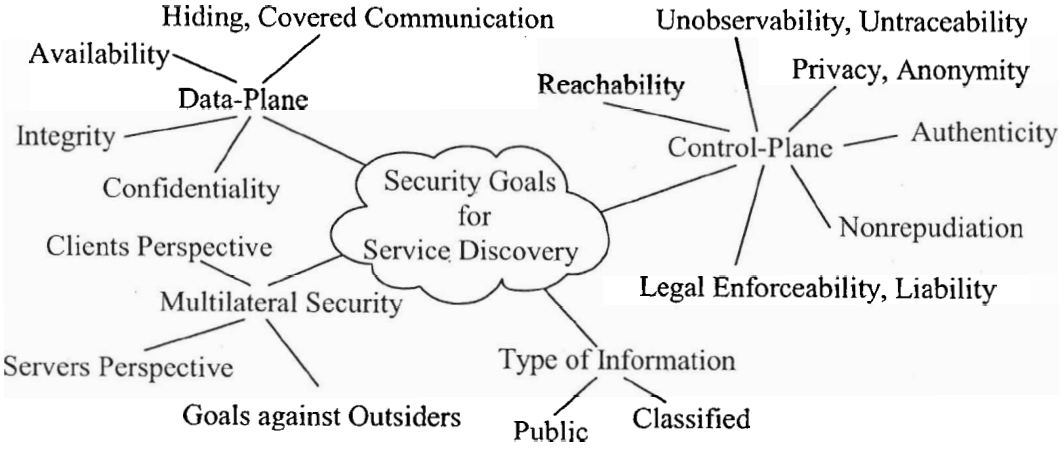

Figure 1 - Security goals and variables for our analysis, derived from [Sch96, WP00, Hol01a]

The necessity of security for service discovery is directly connected to the process of establishing security awareness within unfamiliar ad-hoc network environments. As described in [Hol01b] *"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"*. Thus security awareness goes hand in hand with the confidence we correlate with the service discovery process.

2.1 JINI Lookup Service

The JINI Lookup Service presents a core component within the JINI Framework [Sun00a, Sun00b, Wal99]. It allows registration and lookup of service information, which is coupled to service proxies. These proxies, together with service providers, implement the actual service. Since the lookup process involves the shipment of code, we face *security problems similar to mobile agent based communication* paradigms. Since JINI is a proprietary technology and hides the underlying communication infrastructure, the approaches and solutions have to be regarded within the closed JINI domain (JINI does assume a single pervasive JINI infrastructure spread all over the world) and not within the open Internet domain.
The integrated security in JINI can be derived from RMI and JAVA security [Sun00a]. Both do not care about service information security by default. There are proposals to enhance the security mechanisms within JINI. One possibility would be the RMI-security extension, which is based on *trusted code* and *code signing* to establish trust among the entities. Another approach is presented in [HKV00]. It enables *authenticity*, *integrity* and *confidentiality* for the entire process of service lookup but requires an existing public key infrastructure in place. Both methods help to establish security among the JINI federation at the cost of spontaneity. There are other approaches dealing with JINI and security e.g. in [EN01] but because of their limited feasibility for open ad-hoc communication we skip introducing these.

2.2 Service Discovery within Salutation

Salutation presents a framework for service discovery and information exchange between service providers and service users [Sal99]. The framework covers a wide set of appliances and takes dynamic ad-hoc scenarios into account. Salutation allows methods to advertise services or find out about their capabilities. Since Salutation is transport independent it allows interconnecting devices over heterogeneous access structures and additionally provides a virtual data pipe for the communication partners.
Security within Salutation is reduced to *user identification* and *-authentication*. The architecture defines a set of credentials; a principal to identify the communication partner, and a verifier to authenticate the principal [Sal99]. In other words, a user-ID and password are the only security relevant parameters specified in the core standard. This authentication data is then to be given to the Salutation Functional Unit (service provider). The server authenticates the client but has to be trusted beforehand. For service information there are no security-mechanisms whatsoever.
The *availability* of the Salutation service depends on the underlying transport layer. Within Internet environments Salutation supports broadcast mechanisms for the discovery of Service Managers, which provides *some robustness* within ad-hoc environments.

2.3 Service Discovery Protocol (SDP)

The Bluetooth service discovery protocol builds upon the Bluetooth link layer facilities [Blu01]. Since the Bluetooth link layer is security aware, SDP inherits some of these capabilities by design. SDP does not instruct to use security mechanisms - the emphasis lies on the *link layer secu-*

rity facilities. Only paired devices (which in effect means a *pre-shared secret* is already established) may use security mechanisms according to their security level definition or their access profile [Mue99]. The available security mechanisms in Bluetooth allow for *authenticity* and *integrity* of the communication. Encryption allows for *confidentiality*. The availability of the service discovery cannot be guaranteed in a strong manner. However, we are not aware of any Bluetooth implementation introducing security measures for service information. Bluetooth advises to "start" security at the link layer and "restart" it at the application layer. The service discovery process hence depends on the link layer security.
Since the Bluetooth system architecture embraces security at link layer, our zero-configuration model is circumvented, rendering the idea of security at the service discovery layer useless for the closed Bluetooth architecture. The general security mechanisms in Bluetooth present some useful ideas on how to carry out key establishment between communication partners, however.

2.4 Service Location Protocol (SLP)

The IETFs Service Location Protocol [Gut99, GPD99] aims to provide a robust protocol for service discovery of networked services and thus simplifies the administration and configuration of computer systems. The protocol mechanisms are very lightweight, especially with respect to security. For practical purposes security within SLP features *authentication* within one administrative domain, if preconfigured (static) security-associations exist among the hosts. So called authentication blocks can be requested on behalf of User Agents (UA) or Directory Agents (DA). This ensures the integrity of the service information by means of authenticating the DA or Service Agent (SA). These are the only security related mechanisms within SLP, being optional moreover. A further separation in data- and control-plane reveals that security only applies to the data-plane in SLP - control plane security mechanisms may be implemented by policy but are not encouraged in the standard.
The bootstrap sequence of SLP assumes an *implicit trust among all protocol entities*. To maximize *robustness* the initial query for DAs introduces the risk of malicious DAs, which may take "control" over the service information within an ad-hoc networks of equal SAs by simply being present. A thorough threat analysis of SLP can be found in [Hol01c]. To summarize, SLP provides only for authenticity of service information. The user portion of the SLP framework hereby trusts the DA or SA, the DA trusts the SA. Restricted to these one way trust relationships SLP is not able to introduce access control mechanisms.

2.5 Simple Service Discovery Protocol (SSDP)

The Simple Service Discovery Protocol within the Universal Plug and Play framework [UPnP00] presents a very lightweight approach. SSDP is based on the http protocol over unicast and multicast UDP [GCL+99]. The first SSDP interactions include OPTIONS and ANNOUNCE for discovery purposes. Some other service or device specific parameters can be transferred using SSDPs description mechanism. Security mechanisms are not described within the SSDP. Concerning the architecture of the protocol, it is impossible to think about Transport Layer Security (TLS), which requires TCP. [GCL+99] states "Security considerations: to be determined" - which essentially means *no security* in place. The *robustness* of the discovery process is improved using multicast mechanisms.

2.6 Secure Service Discovery Service (SDS)

The Secure Service Discovery Service within the ICEBERG Framework concentrates on securely providing appropriate information on internetworked services [JBK98]. SDS is used to interface

with directory services or to directly act upon multicast mechanisms. The attacker model used to design the SDS is very strong and thus the protocol includes measures to ensure *authenticity* and *integrity* of client and server, and *confidentiality* for the communication. *Access controls* to allow for *confidential information* are in place, too [CZH+99]. The matter of *availability* is addressed using multicast messages to increase the *robustness* of the protocol.
The security aspect looks promising, but is only achievable within an existing trusted environment, provided by a public key infrastructure [CZH+99]. Dealing with pure ad-hoc scenarios, SDS faces the same problems mentioned for the other protocols earlier. There is no embodiment of trust between the hosts and thus all mechanisms in SDS will fail if the infrastructure behind disappears. SDS provides an enhanced robustness for directory-like service infrastructures thus increasing *availability* and *robustness* even in dynamic environments.

2.7 Domain Name System (DNS) and Domain Name System Security (DNSSec)

The Domain Name System (DNS) [Moc87a] [Moc87b] is a core part of the Internet by providing a mapping between user-friendly domain names and the corresponding IP-addresses. Recent changes in DNS allow for service lookup, using so-called Service Location Resource Records (SRV-RR) [VEG00]. Additionally, the mechanism for dynamic update of resource records [ETRB97] makes DNS applicable for service lookup and -registration in environments with at least one primary DNS server. Taken seriously, DNS is not feasible for pure ad-hoc environments but needs some pre-configuration. However, its nearly ubiquitous nature in today's Internet and its quality to assure the *authenticity* and *integrity* of information by means of self-deployed mechanisms are worth being investigated. The rich features for *public key-* and *secret key distribution*, origin *authentication* and *integrity* and *transaction-* plus *request authentication* are described in various RFCs, [Eas99] and [VGEW00] being the most important ones.
To summarize, DNSSec and its successors provide means to guarantee the *authenticity and integrity of resource records and transactions*. Moreover, *authorization* of dynamic updates can be achieved. The main obstacle related to ad-hoc environments is the requirement of a primary DNS server, if secure dynamic updates are performed. Additionally there have to be *preconfigured security associations* to trust at least one master-zone key, which allows to follow the validation path to the server being discussed. The DNSSec mechanisms fall short against attacks mounted on *privacy*, *confidentiality*, and *denial of service*, however.

2.8 Security Evaluation and Summary

The diagram shown in fig. 1 acts as the base for our security investigation. Having briefly described the protocol functions, we now introduce real world scenarios as a yardstick to measure the protocols against the security goals. Moreover, we introduce the syntax used throughout the synopsis in table 1 below (the numbering by alphabet does not imply an order of importance of the security goals). Since we regard the examples as typical, they can be seen as basic security requirements for service discovery and thus should be met by a "secure" protocol:

(a) Reachability (availability of control plane) and **(b)** availability of data:
"Imagine Sandra's PDA being a trusted device and acting as her personal security assistant. Having purchased a season ticket for the opera, she wants the information about the virtual ticket check-in being available to allow for reliable entrance."

(c) Data integrity and **(d)** authenticity of the communication circumstances (control plane):
"A traveler using a public - location based - service, such as a timetable service on an airport, wants to rely on the displayed time of departure of his plane, thus requiring integrity of the service information."

(e) Data confidentiality:
"During a conference developers meet to discuss top secret problems of a new product design. Since they use a wireless LAN and do not want to emanate data nor service information they want to dynamically join a secure ad-hoc community." [Hol01a]

(f) Privacy (anonymity or pseudonymity of the communication circumstances (control plane)):
"During a walk through the city, each store polls the integrated Bluetooth interface of your cellular phone if you ask for service information. This allows tracking down your actual position and collecting information about your interests and shopping behavior if privacy is not preserved."

(g) Nonrepudiation (control plane), **(h)** Untraceability (control plane), **(i)** Liability (control plane), and **(k)** Covered communication (data plane):
*There may be some scenarios requiring the very specific security goals **(g), (h), (i)** or **(k)**. However, we consider the effort to realize the goals only viable in few situations. Moreover, the technical requisites may be very complex (e.g. to allow for nonrepudiation there need to be a trusted time-stamp service, etc.).*

As we analyzed security under the aspect of multilateral security, we have to introduce subcategories. The label **(x.1)** means the security goal **(x)** from the client's perspective (is it possible to communicate confidential?, are the messages **I receive** authentic?, is the integrity of data **I receive** guaranteed?, is the server / are the server messages available **to me**?). The label **(x.2)** denotes the server's perspective and **(x.3)** indicates the combined perspective of both, client and server. Some combinations are not appropriate and thus discarded (e.g. confidentiality always is a common goal of both, client and server). Since none of the protocols we looked into met the security goals **(g.1), (g.2), (h.3), (i.3), (k.1), (k.2), and (k.3)** we exclude these security goals in the summary below. Our rating scheme distinguishes between security goal met **(Yes),** security goal missed **(No)** or optional components necessary to reach the security goal **(Opt.).** Since availability is critical to measure in absolute values, we decided to introduce a rating scale **(++, +, o, –, – –)**. We rate one or two plus' for a *distributed* architecture using *multicast* or *broadcast* mechanisms, because of increased robustness. Zero denotes only distribution of the components or only multicast / broadcast mechanism. One or two minus' mean very weak or not available protocol mechanisms.

Table 1. Summary of the security mechanisms in service discovery protocols

Security Goal	(a)		(b)		(c)		(d)		(e)	(f)		
Sec. Subgoal	(a.1)	(a.2)	(b.1)	(b.2)	(c.1)	(c.2)	(d.1)	(d.2)	(e.3)	(f.1)	(f.2)	(f.3)
JINI	+	o	– –	o	Opt.	Opt.	Opt.	Opt.	No	No	No	No
Salutation	+	o	o	o	No	No	No	No	No	No	No	No
SDP	++	+	+	+	Yes*	Yes*	Yes*	Yes*	Yes*	No	No	Yes*
SLP	+	o	+	o	Yes*	No	Yes*	No	No	No	No	No
SSDP (UpnP)	o	o	– –	o	No	No	No	No	No	No	No	No
SDS	++	+	+	+	Yes	Yes	Yes	Yes	Yes	No	No	Yes
DNS (DNSSec)	o	o	+	o	Yes	Opt.	Yes	Opt.	No	No	No	No

* See corresponding section for further explanation.

3 CONCLUSION

We have used well-known principles to clarify the role of security for service discovery within ad-hoc networks. It turned out that there is no common denominator describing security associated with the discovery of service information - neither at the control plane, nor at the data plane of the protocols reviewed.
Our example scenarios have illustrated, that the current approaches towards security within service discovery are inadequate, especially bearing in mind a future, where lots of networked devices may interact autonomously or on behalf of their owner. Moreover, our examples introduce a common viewpoint on essential security goals for service discovery in ad-hoc environments. As we have shown, all protocols miss the target. The protocols being close to our specification (SDP and SDS) build upon pre-existent security associations, thus presenting a very questionable prerequisite in an ad-hoc environment of unknown communication partners. Nevertheless, these two protocols are the only ones designed for confidentiality, thus allowing for classified information. As a future directive, the trade-off between spontaneity and security has to be investigated thoroughly. We strongly believe, that leaving service information totally unprotected will lead to a severe decrease of confidence by significantly reducing privacy and confidentiality of the communication. In addition, we emphasize the need for ad-hoc mechanisms leading towards security associations between devices - service discovery playing the key role here.
Having established a coherent view on how to treat security related to service information within ad-hoc environments, future work will concentrate on engineering technically viable security solutions for ad-hoc environments based on the foundation of service discovery.

ACKNOWLEDGEMENT

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. [SECCO]

REFERENCES

[Blu01] Bluetooth SIG: "*Specification of the Bluetooth System - Version 1.1*", February 2001.

[CZH+99] Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, Anthony D. Joseph, and Randy H. Katz: "*An architecture for a secure service discovery service*", Fifth Annual International Conference on Mobile Computing and Networks (MobiCom '99), Seattle, Washington, August 1999.

[Eas99] D. Eastlake: "*Domain Name System Security Extensions*", Proposed Internet Standard RFC 2535, March 1999.

[EN01] P. Eronen and P. Nikander: "*Decentralized Jini Security*", Proceedings of the Network and Distributed System Security Symposium (NDSS 2001), San Diego, California, February 2001.

[ETRB97] P. Vixie (Ed.), S. Thomson, Y. Rekhter, and J. Bound: "*Dynamic Updates in the Domain Name System (DNS UPDATE)*", Proposed Internet Standard RFC 2136, April 1997.

[GCL+99] Yaron Y. Goland, Ting Cai, Paul Leach, Ye Gu, and Shivaun Albright: "*Simple Service Discovery Protocol*", Internet Draft, draft-cai-ssdp-v1-03.txt, October 1999.

[GPD99] Erik Guttman, Charles E. Perkins, and Michael Day: "*Service Location Protocol, Version 2*", Proposed Internet Standard RFC 2608, June 1999.

[Gut99] Eric Guttmann: "*Service Location Protocol: Automatic Discovery of IP Network Services*", IEEE Internet Computing 3(4):71-80, July 1999.

[HKV00] P. Hasselmeyer, R. Kehr, and M. Voß: "*Trade-offs in a Secure Jini Service Architecture*", 3rd IFIP/GI International Conference on Trends towards a Universal Service Market (USM 2000), Munich, Germany, September 2000. Springer Verlag, ISBN 3-540-41024-4,

[Hol01a] 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.

[Hol01b] Matthias Hollick: "*Security Awareness in Service Location for Multimedia Collaboration*", To appear in ACM Multimedia 2001. Workshop for Multimedia Security. October 2001

[Hol01c] Matthias Hollick: *"Security for Ad-Hoc Service Information - Threat Analysis of the Service Location Protocol"*, Technical Report, available at <http://www.ipsi.fraunhofer.de/mobile/projects/secco/pub>

[JBK98] Anthony Joseph, B. R. Badrinath, and Randy Katz: "*A Case for Services over Cascaded Networks*", First ACM/IEEE International Conference on Wireless and Mobile Multimedia (WoWMoM'98), Dallas Texas, October 1998.

[Moc87a] P. V. Mockapetris: "*Domain names - concepts and facilities*", Proposed Internet Standard RFC 1034, November 1987.

[Moc87b] P. V. Mockapetris. "*Domain names - implementation and specification*", Proposed Internet Standard RFC 1035, November 1987.

[Mue99] Thomas Müller: "*Bluetooth Security Architecture*", Whitepaper, August 1999

[Sal99] The Salutation Consortium: "*Salutation Architecture Specification (Part-1) - Version 2.1*", 1999

[Sch96] Bruce Schneier: "*Applied Cryptography: Protocols, Algorithms, and Source Code in C - Second Edition*", John Wiley; New York, USA; 1996.

[SECCO] Project Homepage at <http://www.ipsi.fraunhofer.de/mobile/projects/secco>

[Sun00a] Sun Microsystems Inc.: "*JINI Architecture Specification - Revision 1.1*", October 2000

[Sun00b] Sun Microsystems Inc.: "*JINI Core Specification - Revision 1.1*", October 2000

[UPnP00] Universal Plug and Play Forum: "*Universal Plug and Play Device Architecture. Version 1.0*", June 2000.

[VEG00] P. Vixie, L. Esibov, and A. Gulbrandsen: "*A DNS RR for specifying the location of services (DNS SRV)*", Proposed Internet Standard RFC 2782, February 2000.

[VGEW00] P. Vixie, O. Gudmundsson, D. Eastlake, and B. Wellington: "*Secret Key Transaction Authentication for DNS (TSIG)*", Proposed Internet Standard RFC 2845, May 2000.

[Wal99] Jim Waldo: "*The JINI Architecture for Network-centric Computing*", Communications of the ACM, 42(7), July 1999.

[WP00] Gritta Wolf, Andreas Pfitzmann: "*Properties of protection goals and their integration into a user interface*", Computer Networks 32(6), p.p. 685-700 Elsevier, 2000