A Peer-To-Peer Approach for Resolving RFIDs

Christian Decker, Michael Leuchtner, Michael Beigl
TecO, University of Karlsruhe
Vincenz-Priessnitz-Str. 1, 76131 Karlsruhe, Germany
http://www.teco.edu
{cdecker, leuchtner, beigl}@teco.edu

ABSTRACT
We present a system using a Peer-to-Peer network for resolving associations of Radio Frequency Identification (RFID) tagged objects to their virtual presence. A query, which consists of an identification string, is sent to the network and receives the appropriate resolution data. We pay particular attention to the authenticity and security of the exchanged data, in order to prevent tracing of resolution queries. The usage of a Peer-to-Peer network enables an non-authoritarian yet easily managed extension by further resolving services, such that these services do not need to share any information with an authoritative organization. Supply Chain Management (SCM) and Customer Relationship Management (CRM) represent potential application areas.

Keywords
Peer-to-Peer, RFID, Resolving Service, SCM, CRM

INTRODUCTION

In Ubicomp there is ongoing research regarding the unification of the real world with the virtual world, leading to the electronic acquisition of real world activities. Projects like CoolTown[1] have demonstrated the diversity of applications enabled by the transition of real world to virtual presences. CoolTown experimented with beacons, RFID transponders and other small devices that provide a unique identification string. This string was then mapped onto a URL in order to create the association with the virtual presence. The resolving mechanism here could either be manually selected or relied on a service similar to a domain name service (DNS). However, we present a Peer-to-Peer (P2P) approach for resolving such associations.

Motivation

In our approach we are using RFID transponders in order to identify objects. The transponders are cheap, small and robust. Nevertheless, available memory on the transponders enables storage of additional information apart from the built-in identification string. The usage of a P2P network has particular advantages when compared to other approaches. Other than centralized resolving services, the P2P approach does not necessitate the sharing of any information about a virtual presence with the network. DNS-like or tree-based resolving services typically require centralized knowledge about object-virtual presence associations, because the root node of the tree has to know all associations in order to perform a successful resolution. In a P2P approach no single authority can trace all resolution queries. Together with a strong encryption of queries and their responses this provides anonymity and security. Furthermore, P2P networks allow non-authoritarian extension. The information offered by a participant in this network is not restricted to a particular format..

Requirements

The P2P network for resolving RFIDs consists of enquirers, resolving services ("resolver") and an intermediate network directing queries and responses to respective parties. The enquirer and resolver do not talk directly to each other. Their communication is performed via multiple, intermediate peer systems. On a cautionary note, as neither party imposes control over the P2P network, their communication is susceptible to attacks like man-in-the-middle [2]. This implies that queries and responses have to be encrypted and authenticated in order to prohibit unwarranted disclosure of the content of the communication and to validate packet origin.

IMPLEMENTATION

We established a P2P network on several computers in our department using the JXTA[3] protocol set. A RFID reader for I-Code transponders was connected via a serial line to the enquirer. Two resolving services were then included on the network. The setup is summarized in figure 1.

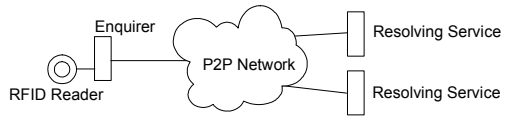


Figure 1: P2P Setup with Enquirer and Resolvers

When an object with an attached RFID transponder was read, the enquirer queried the network and the resolving service for the identification string and replied with extensive information regarding the virtual presence of this object. As a consequence of the requirements we used GnuPG[4], a freely available tool for secure communication using an asymmetric Public-Key algorithm. We consider communication authenticated and secure when the enquirer holds a valid public key for each resolving service. On the other hand, a resolving service must also possess the appropriate public key of the enquirer. Public and private keys were generated beforehand and installed on the respective computers. The key lengths were set to 1024 bits providing a strong encryption. The resolving mechanism works as follows: When a transponder is read it pro-

vides a fixed identification string of 8 bytes and a service identification string of 44 bytes from its memory. The enquirer uses the service identification to query the resolver. The network replies with peer advertisements matching the service identification. At this point the authenticity of the resolving service has not yet been proven. The enquirer therefore connects to all advertised peers. A message M_q containing a randomly chosen session ID, the service identification and the RFID from the transponder is encrypted with the public key of the resolving service, signed using the enquirer's private key and then sent to each connected peer. A resolving service can now verify the authenticity of the message using the public key of the enquirer and decrypt the message using his private key. The query request can then be fulfilled by the resolving service. A message M_r containing the received session ID, the service description and the response data is then encrypted, signed and sent back to the enquirer, which can now prove the authenticity of the resolving service. The next figure summarizes the resolving mechanism.

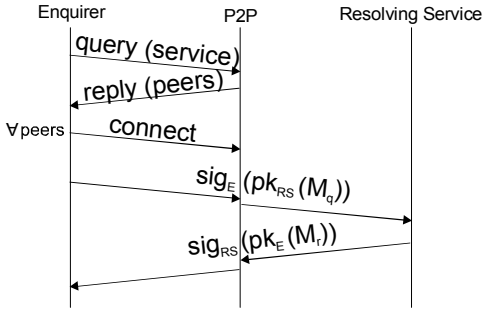


Figure 2: Resolving Mechanism

Our tests showed an average response time of six seconds for a query, mainly caused by the encryption algorithm and the delays while waiting for replies of peer advertisements.

DISCUSSION AND APPLICATIONS

Apart from the strengths like anonymity, authenticity and security, there are also weaknesses. The exchange of the public keys is an overhead during protocol initialization, making the setup of new resolving services and enquirers inconvenient. An initial direct and secure connection between enquirer and resolving service can be applied. Furthermore, the management of possibly several thousand keys on a machine requires a large effort to secure the enquirer and resolving services. There are also performance issues: the signature of all messages arriving at the resolving service must be checked for each known enquirer, which causes a huge load when the network scales up. Advanced features like group creation implemented in JXTA might be helpful to balance the load. On the application side we see a huge potential, when manufacturers can electronically trace their items. Applications in the field of SCM and CRM systems might benefit from the ubiquity of extensive information about items, which becomes easily and securely accessible by our approach. The major strengths of the P2P approach are the non-authoritative extensibility by just adding another resolving service or enquirer and the anonymity. A manufacturer providing a resolving service does not need to share any information with an authoritative organization, and can use his own identification scheme for his items. Anonymity grants that queries for item identifications are not traceable by others. Furthermore, the asymmetric encryption ensures authenticity and protects exchanged data. The control of information is completely on the manufacturer's side. Therefore we also see an application area in workflow management systems controlling processes interwoven between various manufacturers.

RELATED WORK

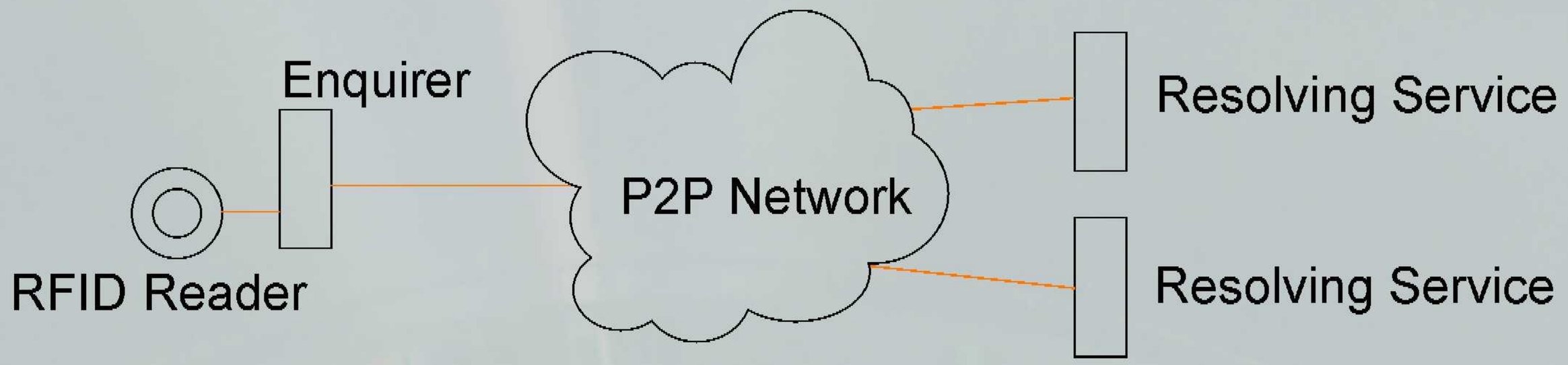
Auto-ID center[5] aims to create standards for an "Internet of things". Identification of objects is based on RFID transponders. The resolving service uses a DNS like tree-based system called Object Naming Service (ONS) returning a resource address for extensive information about an object. With CueCat[6] users could scan an item's barcode which was sent encrypted over the Internet to CueCat's manufacturer returning the URL of an appropriate website about the item. The encryption was cracked and it was found that the manufacturer collected personal data from each scanner device. In research on security on P2P networks reputation-based approaches and protocols like XREP[2] were developed to handle various attacks. However, reputations need to be shared and as in our scenario enquirers don't share information this method cannot be applied here.

CONCLUSION AND FUTURE WORK

We presented a system design and its implementation for resolving RFIDs using a P2P network where queries and responses are encrypted and signed. This approach is marked by anonymity, security and non-traceability of queries and responses. Furthermore, it enables easy adhoc and non-authoritative extension and redundancy. Ubicomp applications benefit from this system as it provides a middleware for resolving associations between real-world objects and their virtual presence. Future investigations will look into group creation for performance and redundancy reasons and into possibilities of using this system as a generic resolving mechanism.

REFERENCES

1. Kindberg T. et al. (2000). People, Places, Things: Web Presence for the Real World. *WMCSA 2000*, p 19.
2. Damiani E. et al. A reputation-based approach for choosing reliable resources in peer-to-peer networks. *ACM CCS 2002*, 207-216
3. Project JXTA. http://www.jxta.org [accessed:7/10/2003]
4. GNU Privacy Guard (GnuPG). http://www.gnupg.org [accessed: 7/10/2003]
5. Auto-ID Center. http://www.autoidcenter.com [accessed: 7/10/2003]
6. CueCat. http://www.cuecat.com [accessed: 7/10/2003]



A Peer-To-Peer Approach for Resolving RFIDs

Christian Decker, Michael Leuchtner, Michael Beigl

RESOLVING APPROACHES

- central server
  i.e. one server responses to all queries
- tree-based
  distributed, but one root knows all, e.g. DNS

DISADVANTAGES

- no anonymity, i.e. queries are traceable
- authoritarian
- single-point-of failure

P2P is a promising approach for resolving services

VULNERABILITIES

- attacks, e.g. man-in-the-middle, replay
- authentication, e.g. risk of identification spoofing
- sniffing

REQUIREMENTS

queries and responses need to be encrypted and authenticated in order to protect their content and to prove their origin

SOLUTION

- use of a strong asymmetric Public Key approach
- keys are exchanged via a secure connection
- every query and response is encrypted and signed

BENEFITS

- every message is protected, authenticated and not traceable
- easy and non-authoritarian extension of the P2P network by further resolvers
- resolver does not need to share information to an authoritarian organization

APPLICATIONS

the P2P approach is applicable for gathering extensive information about items in SCM and CRM scenarios

TECO