Security Analysis of the Object Name Service

Benjamin Fabian, Oliver Günther and Sarah Spiekermann
Institute of Information Systems
Humboldt-University Berlin
Spandauer Str. 1, 10178 Berlin, Germany
e-mail: {bfabian, guenther, sspiek}@wiwi.hu-berlin.de

***Abstract*— The EPCglobal network is designed to function as a global information retrieval network for objects carrying RFID tags with an Electronic Product Code (EPC). To locate corresponding information sources a so-called Object Name Service (ONS) is used. We take a look at privacy and security implications of ONS deployment and evaluate possible mitigation strategies.**

I. The EPC Network

The idea of the "Electronic Product Code" (EPC) standard is to assign a globally unique number to every RFID tag. This EPC is serving as an identifier for the physical object carrying the tag, which can now be recognized, identified and tracked by an IT infrastructure [1].
Though the EPC standard is actually a meta framework for different encoding schemes and name spaces, most EPCs have a structure similar to the one shown in Fig. 1 [2] that depicts an example EPC for one of the most popular standards, the Serialized Global Trade Identification Number (SGTIN) [1, p.12].

Header	EPC Manager = Company Identifier	Object Class	Serial Number
(Flags for number system in use)	47400	11015	473201

Fig. 1. Example Electronic Product Code (EPC)

EPCglobal, having its origins in the Auto-ID labs of MIT, is a joint venture between EAN International (now GS1) and the Uniform Code Council (UCC) with the focus on developing and establishing global standards for RFID, EPC and the EPC network.
According to their intention, information about an object should in general not be stored on its RFID tag itself, but instead be supplied by distributed servers on the Internet [3]. By using the EPC and the help of an Object Name Service (ONS) it will be possible to locate EPC Discovery and EPC Information Services (EPC-IS), which are collections of available data about the particular object [4].
One of the advantages the EPC Network offers is to let many parties (e.g. manufacturers, suppliers, shops or after-sale service providers) dynamically register any kind of EPC Information Service for the objects they are concerned with, thereby creating an open way to exchange product related information.
It can be easily anticipated that in general a static list of available services might be outdated soon. A solution would be to first ask the ONS for a recent list of sources each time you like to access information about a particular object. After retrieving this list you could directly contact all or some of the EPC Information Services you are interested in (Fig. 2) [5]. All these procedures will in most cases not be conducted manually, but in an automated fashion, e.g. by the use of web services [6, p.4].
Example application scenarios are supply chain management [6] – increasing efficiency, flexibility and co-operation – or smart homes [7], where a home IT infrastructure needs to identify objects of the real world to provide services.
Since ONS is one of the major building blocks of the global network infrastructure as foreseen by EPCglobal, we investigate it with a view to security issues.

II. ONS Technical Details

Technically spoken the ONS is a subset of the Domain Name System (DNS) [8][9]. The main design idea is to first encode the EPC into a syntactically correct domain name, then to use the existing DNS infrastructure to query for additional information. This procedure makes use of the NAPTR (Name Authority Pointer) DNS record, which is also used with the SIP protocol for VoIP to map an E.164 telephone number into a Uniform Resource Identifier (URI) [10].
The ONS resolution process is described in [11] and [5]. After a RFID reader has received an EPC in binary form, it forwards it to some local middleware system (Fig. 3). To retrieve the list of relevant EPC-IS servers for this particular object, the middleware system converts the EPC to its URI form [1, p.53] (e.g. `urn:epc:id:sgtin:47400.11015.473201`).
Then it is handed over to the local ONS resolver, which in turn translates the URI form into a domain name (e.g. `11015.47400.sgtin.id.onsepc.com`) by following a well-defined procedure [11, Section 5]. This name is part of a sub domain of `onsepc.com`, which is reserved for ONS use.
The current ONS specification states that the serial part (item level, in our example: 473201) of the EPC should not be encoded for now, but leaves room for such a possibility [11, Section 3.2.1]:

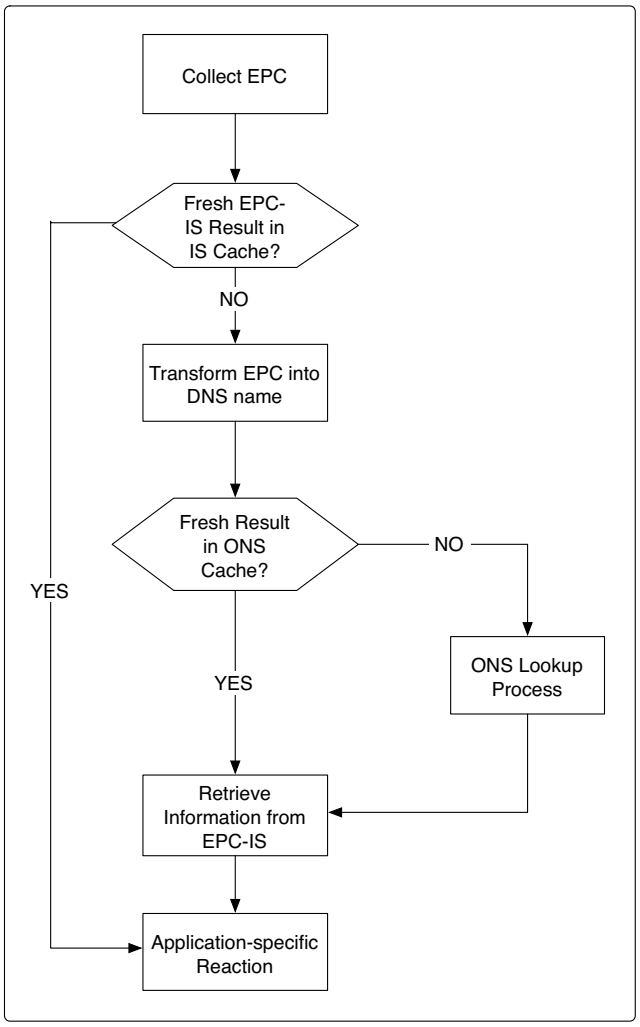

Fig. 2. EPC Information Retrieval (high level view)

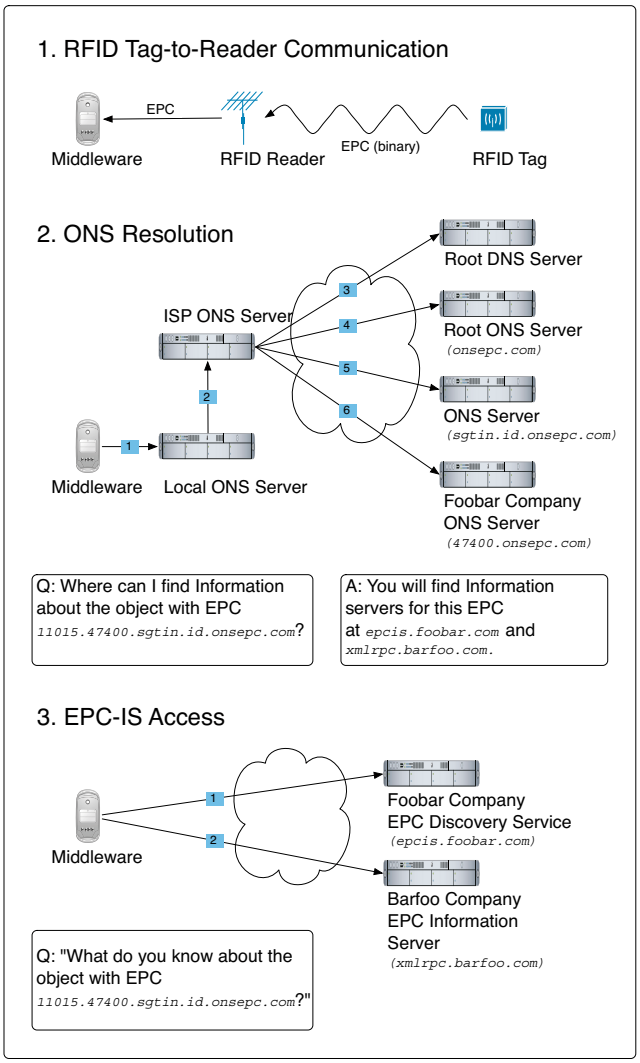

Fig. 3. Using the EPC Network

> *The ability to specify an ONS query at the serial number level of granularity as well as the architectural and economic impacts of that capability is an open issue that will be addressed in subsequent versions of this document. Its lack of mention here should not be construed as making that behavior legal or illegal.*

This newly created domain name is now queried for by using the usual DNS protocol. This implies that the (for now partial) EPC moves through the subsequent local networks and the Internet in clear text, and can be read, stored and analyzed by any interested party on its way through the DNS hierarchy.

III. DNS Heritage

DNS is an old and central Internet service with a long history of security issues in the protocol itself and in particular implementations. This can easily be verified by consulting established security sites as CERT [12], SecurityFocus [13] and the SANS Institute's "Top 20 List of Internet Security Vulnerabilities" [14]. Interestingly, a corresponding RFC 3833, "Threat Analysis of the Domain Name System" was only published in 2004 [15] after long decades of use. Some of the main known threats identified there are:

- *Packet interception*: Manipulating IP packets carrying DNS information
- *Query prediction*: Manipulating the query and answer schemes of the DNS protocol
- *Cache poisoning*: Various ways to inject manipulated information into DNS caches
- *Betrayal by trusted server*: Attackers controlling DNS servers in use
- *Denial of service*: Comparable to any network service, though DNS itself might be used as an amplifier to attack third parties [15, p.7]

The underlying reason for most of these vulnerabilities consists of the fact that even though DNS is a highly exposed service by definition, it has in its original (and widely used)

form no way of authenticating a client, the server nor the information that is provided. These weaknesses directly transfer to ONS.

IV. EPC Confidentiality and Privacy

There are many contexts where the EPC of a RFID tag could be regarded as highly sensitive information – be it in private [16] or in business environments (e.g. product and raw material flows constitute valuable market information). Many different ideas for securing the wireless RFID tag to reader communication have been proposed, for examples and overview confer to [17][18][19][20].

Even if the complete serial number is not known, the combination of object class and company identifier of the EPC is usually enough to determine the kind of object it belongs to. If the use of the EPCglobal network becomes ubiquitous and widespread, the eavesdropper could easily add fake serial parts to the captured incomplete EPC and query the corresponding EPC-IS servers until a match is found.

This can be used to identify assets of an entity, be it an individual, a household, a company or another organization. If you happen to wear a rare item, or a rare combination of belongings, tracking you might be accomplished even without knowing the actual serial numbers, just using the object classes.

The proposed solutions to mitigate these privacy problems mostly do not take into account what happens to the EPC once it is determined by a reading process. To make use of the information stored in the EPC network about a given EPC you need to locate the corresponding EPC-IS servers first. Even if later on the connections to these servers are secured by using for example SSL/TLS, the initial ONS look-up process has neither been authenticated nor encrypted in the first place.

The DNS encoded main part of the EPC which identifies the asset categories will first traverse every network between the middleware and a possibly local DNS server in clear text – this could include a local wireless network. Depending on the configuration of DNS caching and resolution process, this partial EPC will also be transmitted to additional DNS servers in the resolution path, which might include the root DNS servers, servers for `onsepc.com` and down the necessary hierarchy [8, Section 2.6 on resolution], until the resolving process finally gets to query a DNS server of the company that serves as main reference for the object in question (usually the manufacturer).

All traversed ISPs might capture the partial EPC – this includes network taps placed by governmental organizations of countries the packets may cross. It follows that attack trees [21] describing for example the profiling of someone's assets will have new branches that represent remote tactics (Fig. 4) – in addition to those already identified in [16].

As will be seen, there is no easy-to-deploy solution to this problem given the proposed workings of ONS. The main privacy enhancing strategy lies in obfuscating the source IP or the real physical orign of the query.

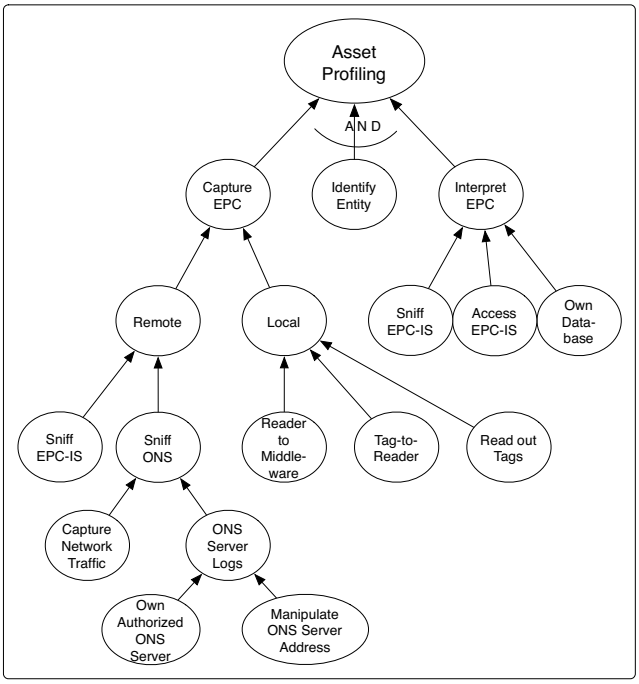

Fig. 4. New Branches for Attack Trees (Example Asset Profiling)

V. ONS Integrity

Integrity in the ONS context refers to the correctness and completeness of the returned information., i.e. addresses of EPC Information Services corresponding to the queried EPC. An attacker controlling intermediate DNS servers or launching a successful man-in-the-middle attack on the communication could forge the returned list of URIs and include – for example – a server under her control. If there are no sufficient authentication measures for the EPC-IS in place, the attacker could deliver forged information about this particular or other related EPCs from a similar domain.

To give short examples: if the query was initiated by a smart refrigerator to order matching ingredients for a cooking recipe, this could result in spoiled meals; if the query was issues by a smart medicine cabinet (as a precursor to an even smarter "home medical advisor" [22, p.51]) to prevent harmful drug mixes, this might constitute an even larger threat to personal safety.

VI. ONS Availability

If the global EPC network becomes widespread reality, more and more business processes (B2B, B2C) as well as private applications will be able to use it without human intervention. This would leave these processes highly dependable on a working EPC resolution service for finding matching information sources.

ONS will constitute a service highly exposed to attacks from the Internet, if only due to its necessary widespread accessibility. This could include Distributed Denial-of-Service (DDoS) attacks overwhelming the server or its network connection by

issuing countless and intense queries, or targeted exploits that shut down the server software or its operating system.
Therefore an integration of the EPC network (with ONS as proposed) into core business processes could leave even formerly non-IT related companies dependable on the availability of Internet services. This will most probably increase overall business risk.

VII. Mitigation Attempts

A. Network Design

Larger enterprises may be able to reduce risks to EPC-confidentiality by using a well-designed network structure, especially a carefully planned DNS server hierarchy. All ONS queries from internal machines at any company site could be forwarded – preferably using Virtual Private Networks (VPN) – to a central company DNS server, which in turn does the external resolution process.
Even then all the EPCs that are resolved by the company could be intercepted outside of the Intranet borders, but not easily assigned to particular locations – though an attacker might apply a careful analysis of time, possibly combining this information with captured EPCs from region-specific objects. As a simple example consider a company using smart offices with ubiquitous RFID readers, where outsiders might witness the introduction and the actual kind of new items (such as newly introduced laptops of a specific manufacturer) anywhere in the enterprise.
If a company just uses an internal and private version of the EPC network without depending on outside information – for example if only self-manufactured items are of interest – no EPC leakage to outsiders would occur, and risks to integrity and availability could be limited likewise to internal attackers. But this special case would deprive the company of the intended advantages of a global and dynamically updated EPC network, as only company-internal data sources about EPCs could be accessed.
Another countermeasure could be the prolonging of ONS and EPC-IS caching times to reduce the frequency of the EPC crossing the Internet. Depending on the application scenario, the EPC-IS dynamics and the demand for fresh information risk-reducing caching strategies might be viable.

B. Virtual Private Networks (VPN) and Extranets

The idea of concentrating ONS queries to prevent an exact locating of the corresponding items could be extended to trusted business partners or neighbors that form a so-called extranet [23, p.247] (Fig. 5).
All parties connect to a central ONS server via Virtual Private Networks (VPN), and this server issues the ONS queries to the outside world. Beyond this point no protection by VPN might be feasible, if access to many different ”third parties” beyond the borders of the extranet is required, as the possible communication partners are nearly countless and not known in advance – the problem of key management for building VPNs to every company offering a relevant ONS and EPC-IS server would render such solutions not scalable.

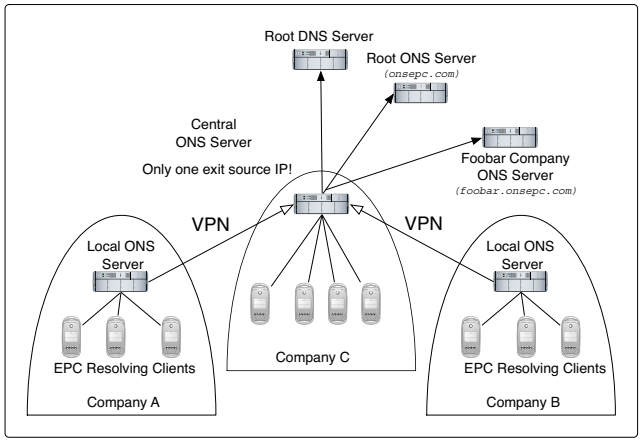

Fig. 5. VPN and Extranets

Apart from issues of trust and administrative overhead there will be an increased network load for the central party, depending on the scale of RFID reader deployment, caching strategies and the intense of usage of the EPC Network by every single partner. The deployment of an Extranet could only limit threats to EPC confidentiality, but not to information integrity or ONS availability.

C. Anonymous Mixes

The culmination of the concentration strategy above, i.e. collecting ONS queries from different sources to hide the real source IP address, is the use of so-called anonymous mixes [24], a strategy that might be viable also for private households (Fig. 6).

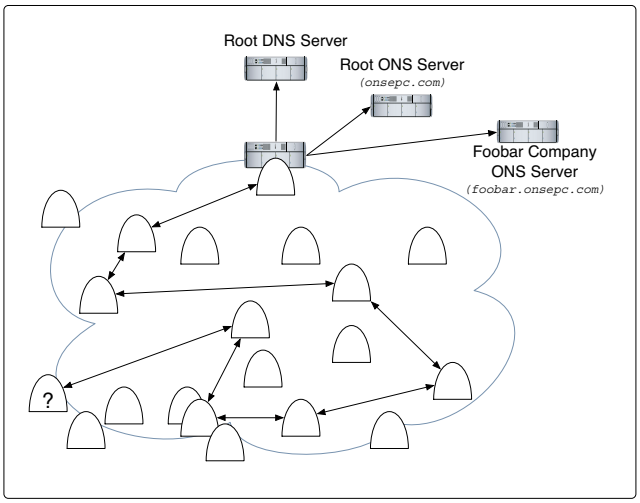

Fig. 6. Anonymous Mixes for EPC Network Traffic

There are approaches such as Onion Routing [25] and especially TOR [26], which basically transform and mix Internet traffic from many different sources in such a way that it would

be highly difficult to match a packet to a particular source.
TOR could also anonymize traffic to EPC-IS servers, and has the potential to become highly relevant to a privacy preserving use of the EPC network.
Again, this approach offers enhanced confidentiality, but does not necessarily increase the integrity of the received messages nor could it do anything about ONS server availability, as any host offering services needs to be somehow addressable and is therefore attackable.

D. DNSSEC

The main approach to address the security shortcomings of DNS is called DNSSEC (DNS Security Extensions) [27][28][29]. It actually introduces two different and independent procedures, one of these, called TSIG (Transaction Signature [30]), provides mutual authentication between two DNS servers by using shared secrets, which introduces big problems of scalability.
The other method provides origin authenticity and data integrity for the delivered DNS information by using public-key cryptography to sign sets of resource records (RRsets). These signatures are stored itself in a different RR type. The server's public key could be transferred out-of-band, or itself be stored in a RR of type DNSKEY. To verify a DNS server's public key it is envisaged to build chains of trust down from the root of the DNS, where each parent DNS server signs the keys of its children after having verified its correctness by some external means.
DNSSEC is a very important approach for securing the Internet at a critical protocol level, but has not been widely adopted so far. Reasons might be the scalability problems of key management and the difficulties in building chains of trust between servers of many different organizations. Therefore global ONS information integrity could only be assured by DNSSEC in the long run, if the Internet community as a whole adopts it.
However, even if DNSSEC could be widely configured to actually encrypt the DNS information, which is not a stated goal so far [27, Section 4, p.8], the company prefix of a given EPC could still be guessed by following the sequence of IP addresses the ONS queries are sent to.
No additional protection against the availability problem of ONS servers is offered by deploying DNSSEC, on the contrary – signature checking introduces additional load to the involved servers [15, p.7].

VIII. Summary

Using the EPCglobal network – as it is designed today – to manage information about objects introduces many new risks. In this paper we have focused on the corresponding lookup service ONS because of the confidentiality issues purely implied by its current design. We assume the actual EPC-IS communication to be more easily securable by SSL/TLS – though integrity problems through improper certificate handling might spoil this assumption, and availability problems do occur likewise.
If ONS is based on DNS as has been proposed in the specifications, a whole new branch of privacy problems do arise, which could only in part be mitigated by security technology, and would even then require huge efforts in network design.
For companies and individuals alike traffic anonymizers like TOR [26] could present an interesting partial solution to privacy-preserving ONS use and EPC-IS access. This approach should be investigated further, e.g. in relation to scalability, manageability and adverse effects due to possible authentication measures for accessing the EPC-IS.
Integrity of ONS information could be dealt with by deploying DNSSEC, though this needs to be set up between all your possible business partners and information service providers, which seems very unlikely given the current diverse and complex state of the Internet.
Availability of ONS and EPC-IS servers is a problem that would have to be approached and dealt with by every company in the resolution path.
Using automated business processes on top of the EPCnetwork and ONS might introduce the same level of dependency on the Internet for traditional businesses tomorrow as for e-commerce companies today.

IX. Further Research

The main movement from barcode to RFID tags containing an EPC has started from the business viewpoint of saving costs and simplifying supply chains, without taking into account privacy-concerns of individuals.
The second step, i.e. the implementation of a global EPC-network to store heterogeneous information about the corresponding objects, appears at least in part be motivated by future after sale applications. Again, it seems that security and privacy are no integral part of the original design, but – if at all – an afterthought.
This leads to many questions for further research, some of which are:

- Is the plan of a global information storage acceptable at all for individuals owning the objects?
- What about the other stakeholders, e.g. companies in the supply chain who would need to offer access to possibly sensitive information?
- What would be the exact security and privacy requirements for all stakeholders?
- What conflicts of interest might arise?
- What part of an EPC and what kind of stored information should be considered public, and how should access rights be configured?
- Should these access rights already influence the results of the lookup service?

Based on a deeper analysis of the multilateral requirements we aim to design an alternative model along with protocols for its implementation.

References

[1] EPCglobal. (2004) EPC Tag Data Standards Version 1.1. EPCglobal. [Online]. Available: http://www.epcglobalinc.com/standards_technology/specifications.html

[2] EPCglobal (US). Electronic Product Code. [Online]. Available: http://www.epcglobalus.org/Network/Electronic%20Product%20Code.html

[3] EPCglobal. About the EPCglobal network. [Online]. Available: http://www.epcglobalinc.org/about/about_epc_network.html

[4] M. Harrison, "EPC information service (EPCIS)," *Auto-ID Labs Research Workshop*, 2004. [Online]. Available: http://www.m-lab.ch/auto-id/SwissReWorkshop/agenda.html

[5] Y. Uo, S. Suzuki, *et al.*, "Name service on the EPCnetwork," *Auto-ID Labs Research Workshop*, 2004. [Online]. Available: http://www.m-lab.ch/auto-id/SwissReWorkshop/agenda.html

[6] K. S. Leong, M. L. Ng, *et al.*, "EPC network architecture," *Auto-ID Labs Research Workshop*, 2004. [Online]. Available: http://www.m-lab.ch/auto-id/SwissReWorkshop/agenda.html

[7] S. Helal, W. Mann, H. El-Zabadani, J. King, Y. Kaddoura, and E. Jansen, "The Gator Tech Smart House: a programmable pervasive space," *IEEE Computer Magazine*, pp. 50–60, March 2005.

[8] P. Albitz and C. Liu, *DNS and BIND*, 4th ed. O'Reilly & Associates, 2001.

[9] A. Salamon. DNS related RFCs. [Online]. Available: http://www.dns.net/dnsrd/rfc/

[10] M. Mealling and R. Daniel, "The naming authority pointer (NAPTR) DNS resource record," *Request for Comments - RFC 2915*, September 2000.

[11] M. Mealling, "EPCglobal Object Name Service (ONS) 1.0," EPCglobal, 2004, freely available until March 2005 from http://www.epcglobalinc.org, archived by the authors.

[12] CERT. CERT Database. [Online]. Available: http://search.cert.org/

[13] SecurityFocus. SecurityFocus Vulns Archive. [Online]. Available: http://www.securityfocus.com/

[14] SANS Institute. SANS Top 20 Internet Security Vulnerabilities. [Online]. Available: http://www.sans.org/top20/

[15] D. Atkins and R. Austein, "Threat analysis of the domain name system (DNS)." *Request for Comments - RFC 3833*, 2004.

[16] S. Spiekermann and H. Ziekow, "RFID: a 7-point plan to ensure privacy," in *13th European Conference on Information Systems (ECIS)*, Regensburg, May 2005.

[17] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," in *Security in Pervasive Computing (SPC 2003)*, ser. LNCS 2802, D. Hutter *et al.*, Eds. Springer-Verlag, Berlin-Heidelberg, 2004, pp. 201–212.

[18] C. Floerkemeier, R. Schneider, and M. Langheinrich, "Scanning with a purpose – supporting the Fair Information Principles in RFID protocols," in *2nd International Symposium on Ubiquitous Computing Systems (UCS 2004)*, Tokyo, Japan, 2004.

[19] S. Spiekermann and O. Berthold, "Maintaining privacy in RFID enabled environments - proposal for a disable-model," in *Privacy, Security and Trust within the Context of Pervasive Computing*, ser. The Kluwer International Series in Engineering and Computer Science, P. Robinson, H. Vogt, and W. Wagealla, Eds. Springer Verlag, 2005.

[20] K. Rhee, J. Kwak, S. Kim, and D. Won, "Challenge-response based RFID authentication protocol for distributed database environment," in *Security in Pervasive Computing (SPC 2005)*, ser. LNCS 3450, D. Hutter and M. Ullmann, Eds. Springer-Verlag, Berlin-Heidelberg, 2005, pp. 70–84.

[21] B. Schneier, "Attack trees," *Dr. Dobb's Journal*, December 1999. [Online]. Available: http://www.schneier.com/paper-attacktrees-ddj-ft.html

[22] F. Stajano, *Security for Ubiquitous Computing*. John Wiley & Sons, 2002.

[23] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet Security*, 2nd ed. Addison-Wesley, 2003.

[24] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, February 1981.

[25] Onion Routing. [Online]. Available: http://www.onion-router.net/

[26] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router," in *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[27] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS security introduction and requirements," *Request for Comments - RFC 4033*, March 2005.

[28] DNSSEC. DNS Security Extensions web page. [Online]. Available: http://www.dnssec.org/

[29] O. Kolkman. (2005, March) DNSSEC - basics, risks and benefits. [Online]. Available: http://www.domainpulse.de/pages/d/programm/Kolkmann.ppt

[30] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)," *Request for Comments - RFC 2845*, May 2000.