RFID is attracting enormous interest as it quickly becomes a widely deployed pervasive technology. At the PERTEC (Pervasive RFID/Near Field Communication Technology and Applications) workshop on 19 March 2007 (part of PerCom 2007), about 30 researchers from Europe, Asia, and the US discussed issues in this field. Topics included management of data ownership in supply chains generated through RFID, integration of RFID and sensors, security and privacy, NFC applications, RFID-based location sensing, and emerging research challenges.

**LINKING DATA ACCESS WITH THE PHYSICAL FLOW OF ITEMS**

Alexander Ilic and his colleagues at ETH Zurich (the Swiss Federal Institute of Technology) reported on how access rights to item-level data in complex business relationships can be linked to whoever can prove that he or she physically possesses an item. Their technique uses RFID to confirm proof of physical possession, with transfer of ownership established simply by one person handing the physical item to another. Such a process could also help verify a product’s pedigree.

Unlike at the Pervasive Technology Applied workshop at Pervasive 2006, no one at this workshop disputed the actual advent of item-level RFID tagging. Instead, the discussion focused on when item-level tagging would happen—in six months or 10 years—and what kinds of products would be the first to be tagged—pharmaceuticals or cloth. The participants concluded that from partial tracking information. For example, if everyday objects have embedded RFID tags, simple constraints, such as that goods can only be in one place at a time or that a train can’t leave the rail track, would let attackers estimate the system’s state and possibly predict its future actions.

Another problem is that data from multiple sources (including RFID) can be correlated, making it difficult to ensure privacy in practice.

Regarding this problem, Yasunobu Nohara showed by simulation results that RFID systems under real-world constraints break the assumption of unlinkability. Ari Juels from RSA Labs and Stephen Weiss from Google discussed privacy in RFID systems where symmetric-key cryptographic operations are possible. They base their definition of privacy on an experiment: they consider an RFID protocol private for some parameter values if no adversary has a significant advantage in this experiment. The adversary’s goal is to distinguish between two different tags within the limits of its computational power and functionality—call bounds; that is, at least two tags must be uncorrupted. Juels and Weiss believe that their parameterized definitions are useful for designing and analyzing privacy-preserving RFID protocols. They have examined several published systems.
that fail to fulfill their privacy definition. So, they believe that they have highlighted potential design flaws.

Mikko Lehtonen from ETH Zurich argued for a pragmatic approach to security. Rather than looking for optimal security, he suggested finding an appropriate level of security that takes into account the actual cost of security. RFID offers a huge variety of security approaches, starting from simple ID coding to lightweight cryptography. The ultimate goal for one of the most demanding problems in today's supply chains—anticounterfeiting—is to find cost-effective solutions based on the value of the products to be secured. The subsequent discussion centered around whether you could use RFID to prevent the sale of counterfeit products. The general consensus was that buyers and sellers could more efficiently process consignments with RFID. However, participants also agreed that if the consumer was happy with a counterfeit, RFID would be of little help to the manufacturer. This seems to call for a reassessment of using RFID to prevent counterfeiting, considering that some customers might have no interest in genuine products.

Paul Moskowitz from IBM presented the clipped RFID tag (see figure 1), where you can physically tear off some part of the antenna. This mechanism provides a simple way to control the tag’s read range, reducing that range from several meters to centimeters. This technique can help protect data access; a data spy would have to come very close to read the tag. The clipped tag still provides the same functionality and hence can offer additional services to the user. Furthermore, clipped tags let users easily assess the system’s state without additional tools. This presentation led to an extended discussion of the perception of privacy. Would users believe that after they tear off part of the antenna, the read range is actually reduced? Also, how could providers of clipped tags prove this reduction to users? This seems to be an open issue; however, most participants felt that such a visible and physical action would increase users’ trust in their ability to be in control.

Christian Metzger and his colleagues from ETH Zurich described another technical approach to preserve privacy: a “watchdog tag” that displays the otherwise invisible reads and writes of RFID tags. Their implementation of this tag recognizes start and end pulses of RFID readers and displays the downloaded data sizes accordingly. This approach increases the visibility of access to personal data.

PAVING THE ROAD TO THE END USER: NFC

Yaw Anokwa and his colleagues from the University of Washington described how a custom NFC device attached to a phone can enable new kinds of interactions. For example, a user walks by a poster advertising a movie. Touching the NFC-tagged poster with an NFC-enabled cell phone provides the phone with a link to where the user can download the movie trailer through mobile Internet. Other options are to buy movie tickets and to download them to the phone and check them through an NFC port at the theater. Such capabilities combine a virtual world with the real world. In the following discussion, participants generally agreed that it’s essential to explore the design space for such new technologies through working prototypes, even if creating them involves significant effort.

Manfred Aigner and his colleagues from the Graz University of Technology presented a mechanism to implement virtual coupons using NFC. Two advantages of such an approach over traditional coupons include automated processing and remote delivery. These vouchers are also appealing for advertisement and ticketing. However, because these coupons have monetary value, assessing potential threats and possible attacks against such a system is essential. The presented solution focused mainly on security issues.

Many research projects are investing gating NFC. At Percom 2007, the best demo award went to Gregor Broll, who showed a novel interaction technique and infrastructure for interactive NFC applications. In his demo, a traditional vending machine (for public-transport and cinema tickets) was replaced by a NFC-tagged poster users could interact with by NFC-enabled cell phones.

LOCALIZATION BY RFID

Steve Hinske from ETH Zurich presented several interesting scenarios and use cases for using multiple RFID tags to locate objects. The basic idea is to distribute readers (or at least the antennas) over the surface on which objects will be located. If an object has several attached tags, you could estimate that object’s location and orientation.

Evan Welbourne from the University of Washington presented a large-scale project that deployed 100 readers and more than 1,000 tags throughout the university campus. Such a large installation provided valuable insight into user concerns. In particular, important concerns were location privacy, the ability to control the data, and the data’s availability to others.

Akhilesh Saxena from NEC started his presentation with the vision of the Star Trek tricorder, a device that provides full understanding of what’s out there. He presented a prototype that lets people efficiently scan the environment for services. Workshop participants agreed that making virtual information about physical objects easily visible and accessible can create completely new ways to access information.
PERTINENT RESEARCH CHALLENGES

In the afternoon, small groups discussed security, privacy, and trust; localization and RFID; and NFC end-user issues. The prime objective was to jointly define a research agenda in this field. The groups also considered the main market opportunities and the obstacles to getting these technologies accepted in the real world.

Security, privacy, and trust

An initial discussion point was how security, privacy, and trust are related. Is user trust really related to security and privacy technologies, or is it related more to the user’s perception of the technology? Sound mechanisms for privacy and security seem to be a prerequisite for genuine trust. However, in some cases users don’t really seem to care (for example, in customer loyalty programs and building-access systems that use RFID, where users receive an immediate benefit). So, it’s valid to ask whether trust is overrated. On this topic, an open research question is how to use legislation to complement technologies. Assessing this will require interdisciplinary research.

One threat to existing RFID solutions that isn’t yet well understood is cloning attacks. How can you ensure that tags aren’t cloned or copied? Finding a practical, economical way to prevent such attacks remains an issue for large-scale deployments. For solutions based on tag authentication, key distribution is an important issue. Here, new architectures and algorithms are a main challenge.

Data management is another central concern. Where should data be stored, and what are the implications of that choice? Clearly, for some applications, storing data on the tag is preferable, while for others, data storage in the back end is preferable. An in-depth assessment would help system designers make informed decisions. For example, if tags are readable by standard readers, you can’t really prevent storage and provision of additional data by third parties, especially on the Internet. In this area, interesting questions are, who can provide what information for products, and what forms of control will be available to the manufacturer or owner of the good?

Workshop participants also discussed whether tagged objects can be used anonymously. How would a technology that enables truly anonymous use actually work? One important consideration is that a wide range of data mining techniques exist. With the addition of real-world constraints, current technologies seem insufficient to prevent tracking of users. This discussion led to the question of how data mining can provide new value in corporate environments, given the data provided from tracking goods. This research area shows significant potential for improving business processes.

Location and RFID

This group first assessed why you would use RFID for location at all. For coarse-grained location, RFID is a cheap, effective method that you can use to track many objects simultaneously. It’s also unobtrusive and maintenance free.

For coarse-grained location, RFID is a cheap, effective method that you can use to track many objects simultaneously. It’s also unobtrusive and maintenance free.

Interesting research topics include using reader power level or signal strength combined with triangulation, trilateration, or multilateration.

End-user issues in NFC

This group’s discussions centered on the value proposition of NFC for end users, and what incentive manufacturers have to provide NFC-related features. An open question is integrating NFC at the end-user level with the EPC (electronic product code) global database. Who would benefit from such an integration, and what would be the resulting applications?

End-user innovation was another promising topic. Can we build tools and infrastructures that let end users use ubiquitous RFID tags? What’s needed to spark user innovation in this field? How can we give users the power to leverage this technology? The group agreed that that solving this problem goes beyond just including readers in mobile devices.

Another important area is the use of multiple tags for interaction. This approach lets you construct complex but passive interactive systems. (One example of this approach, presented in the main conference, turned simple surfaces such as posters into more complex interfaces—for example, for operating appliances.) The participants agreed that many research issues remain open. The physicality of the interaction with tags can add new affordances (ways of interacting) to interactive applications. Additionally, mechanisms already used in the physical world can be used with such objects—for example, locking an object away to prevent others from accessing it.

Collaborative use of NFC seems
promising. One simple example is virtual graffiti on products and places. Users can annotate tagged objects with their comments and share them with others. The application scenarios range from restaurant recommendation to activists providing in-depth information on malpractice in product manufacturing. This can empower consumers in the long term and make it possible to create alternative information systems parallel to information that companies provide.

This workshop was the first of its kind. The discussions clearly showed that RFID technology is about to reach the tipping point of generating return on investment in industrial applications. Additionally, the advent of NFC technology could popularize RFID in the same way that the metaphor of the WWW has turned the network of corporate and university computers into the Internet that the masses experience today. New applications and new forms of interaction with mobile phones could result in new roles for our mobile phones. Users no longer communicate only with people but also are empowered to interact with objects—the Internet of things approaches the end user.

For more information on the PERTEC workshop, see www.autoidlabs.org/events/pertec2007. The workshop papers were published in Proc. 5th Ann. IEEE Int’l Conf. Pervasive Computing and Communications Workshops (PerComW 07), IEEE Computer Society Press.

REFERENCES
