Radio Frequency Identification as a Challenge to Information Security and Privacy

Jorma Kajava
Oulu University, Finland

Juhani Anttila
Quality Integration, Finland

Rauno Varonen
Oulu University, Finland

INTRODUCTION

New technology has continuously changed the face of computing, and each change has involved an improvement in computer architecture and information processing. There are strong indications that the next paradigm shift in information technology will be kicked off by tiny radio frequency identification (RFID) tags. These lowly devices are being ushered in by corporations like Wal-Mart to facilitate business logistics, but other uses are waiting in the wings. As usual with any technology, criminally-minded individuals have been quick to exploit smart tags for their own purposes. Thus, it is in place to take a look at the dark side of RFID technology to see how it may affect the security and privacy of citizens.

BACKGROUND

Information security work is a relentless struggle against evil. Previously, a balance was sought chiefly between usability and security, but recently a new axis has been added, namely, social control and privacy. However, this is still a simplification that does not reflect the so-called real world sufficiently well, considering that there are more aspects to it than those four. For example, there is the three-way relationship involving the individual, organization, and technology that should be taken into account, not to mention certain business aspects.

On the road to the information society, we have passed through the agricultural and the industrial society. The large-scale application of computers and wireless communications are characteristics of the automation society, a precursor to the information society (Anttiroiko, 2003). Despite the progress we have made, it appears that taking small steps is not enough in order to get to the destination. What is needed is a comprehensive change at the global level.

One impulse that triggered a wave of change across the globe was the Universal Bar Code which, although originally designed to facilitate supply chain management, inventory management, and product identification, will inevitably affect most aspects of information processing and business. Behind this impulse was a decision taken by Wal-Mart in the 1970s to stop handling goods that are not bar coded. Now the company has issued a similar demand: all products must have an RFID (radio frequency identification) tag by the end of 2005.

RFID tags are computer chips that broadcast a 96-bit code that can be used to uniquely label individual items, rather than just product types (as does the UBC). RFID systems comprise a transponder, or tag, that responds to wireless signals produced by a transceiver, or tag reader, which also powers the tag. Readers identify tags placed in all products by referring to an associated database. A typical reading distance, without line of sight, is two to eight meters.

Product identification tags come in two varieties: the first one is placed on packaging, while the other type is placed on the product. For obvious reasons, the latter type is much more likely to put personal privacy in jeopardy.

Little attention was attached to reading devices such as Wal-Mart's prior to 2004, when international RFID frequency ranges were determined. As a result, each continent now has its own specific standards. Even more importantly, each tag is equipped with circuits for two different frequency ranges (Want, 2004).

Mobile phones are also getting new features. For example, the city of Oulu introduced a new parking pay system which can be accessed through cell phones. In autumn 2004, a new mobile service was presented enabling cell phones to be used as automated readers for RFID tags.

Table 1. Basic rights of citizens in the European union

• Right to liberty and security (article 6)
• Protection of personal data (article 8)
• Freedom of expression and information (article 11)
• Workers' right to information and consultation within the undertaking (article 27)
• Right of access to documents (article 42

LEGAL STANDARDS WITHIN THE EUROPEAN UNION

In our society, citizens and organizations have rights and responsibilities regarding information. A continuous debate focuses on fundamental individual and communal liberties and rights, although no general solution that all parties would find satisfactory is in sight.

Citizens of the European Union have at least the following basic rights presented in Table 1 (European Commission, 2000).

To ensure that these rights are respected, information security solutions must be well balanced. It is impossible to stop progress or even slow it down, for technological innovations, which inevitably create new challenges, possibilities, and threats, are part and parcel of our society and lifestyle.

INFORMATION SECURITY DEMANDS

Discussions on information security often begin with a reiteration of the dimensions of the so-called CIA model, to wit, Confidentiality, Integrity, and Availability (Anttila, Kajava, & Varonen, 2004; BSI, 1993; Canadian Royal Mounted Police, 1981; ISO, 1995, 2001; Longley & Chain, 1989; Parker, 1981; Schweitzer, 1990). In terms of RFID tags, these dimensions are essential, but even more important is another, less discussed, dimension: Traceability. Most people are aware of its existence, thanks to its application in mobile phone tracking systems and satellite surveillance systems. Despite the advantages that traceability offers, there is also a downside, for tracing the position of an individual may violate the individual's personal location privacy and constitutional rights.

Another challenge that such surveillance gives rise to, involves the right of authorities to use a person's cell phone to locate him, for example, when a mishap is suspected to have occurred.

Satellite surveillance is a more convoluted phenomenon. Can it be justified by reason, or is it just a matter of the stronger side dictating the rules? Moreover, as satellites know no national boundaries, which national legislation should be observed? Harmonizing legislation in any area is a daunting task, and information security is no exception. To give an example of the range of approaches, we could cite a case from the late 1990s. An armed robbery took place on an Italian motorway, but the perpetrators were caught thanks to a photo taken by an American surveillance satellite, revealing their car's licence number. At the same time, a debate raged in Finland over the right of the police to acquire telephone data on two men suspected of involvement in drug trafficking.

INVESTMENTS AND EXISTING APPLICATIONS

Although the spirit of the times seems to be that the pervasive introduction of RFID systems is a thing of the future, big players are already jockeying for position. IBM and Hewlett-Packard, for example, have invested $250 million and $150 million, respectively, on RFID-related research projects.

Some projects are no longer on the drawing board. In the Japanese city of Osaka, city authorities have launched an initiative in which schoolchildren in certain parts of town are equipped with RFID tags. These tags are placed in their clothes, bags, or name tags and are used to keep track of the children's whereabouts. RFID readers are positioned at the school gate and other critical places along the way to school.

This decision indicates that the children's parents and local authorities set more value on security than privacy. Strictly speaking, though, this is not completely true; after all, they are only creating a more extensive surveillance network around their children, while keeping their own privacy intact.

Another area where RFID technology has been applied for years is the satellite surveillance of expensive cars. Should one of these cars be stolen, locating it is generally not a difficult task. Moreover, owners are within their legal rights to install RFID tags on their cars in order to protect their property.