RFID Privacy Workshop

Concerns, Consensus, and Questions

Stephen A. Weis
Massachusetts Institute of Technology

Radio frequency identification devices (RFID) are at the center of much debate and controversy. Backers have hyped them as a godsend to supply-chain efficiency, while some privacy advocacy groups, such as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN; www.nocards.org) have labeled RFID as the "worst thing that ever happened to consumer privacy." A group of technologists, industry proponents, academics, and privacy advocates gathered for the RFID Privacy Workshop at the Massachusetts Institute of Technology on 15 November 2003 to discuss privacy issues in RFID systems. The workshop featured keynote speeches by Mario Rivas, executive vice president of Phillips Semiconductor, CASPIAN founder Katherine Albrecht, and Computerworld Canada columnist Peter de Jager. Approximately 300 attendees listened to 17 presentations, demonstrations, and panel discussions during the one-day workshop.

The workshop invited members of the RFID manufacturing industry, academia, the press, and privacy advocate groups to submit papers on an array of RFID privacy-related topics. Papers were selected with the goal of presenting a wide range of viewpoints and positions. Speakers presented their own work and participated in panel discussions and audience question-and-answer sessions. Proceedings from the workshop, including presented papers, speakers' slides, and streaming video of all presentations, are available at www.rfidprivacy.org.

What are they?

RFID tags—small microchips attached to antennas—and tag readers comprise a basic RFID system. Readers query tags via radio signals and the tags respond with identifying information, which might include manufacturing information, product codes, or unique serial numbers. One of the first uses of the RFID idea was the *identification, friend or foe* systems deployed on aircraft during World War II. In recent years, toll systems, supply-chain management, and inventory-control applications use RFID.

In his keynote speech, Rivas said that Phillips has shipped over one billion tags, which have helped to track objects as varied as microchips and cattle. They are even in automobile "immobilizers," which prevent cars from starting unless a particular RFID tag, perhaps on the owner's keychain, is nearby. He speculated that RFID systems could save up to 25 percent of shelving costs and 65 percent of some receiving costs by streamlining shipping, receiving, and inventory control. RFID tags also can prevent "shrinkage" (the industry's euphemism for employee theft) by detecting unauthorized inventory movement.

Most RFID devices used to track products moving through supply chains are embedded in shipping pallets, rather than on individual items. Pallet-level tracking poses little threat to consumer privacy because individual pallets don't link to a single consumer. Nevertheless, even this use of RFID could facilitate corporate espionage by allowing competitors to monitor inventory levels, a point that speaker Ross Stapleton-Gray, founder of Stapleton-Gray & Associates, a systems-analysis and project-management firm, discussed. Nevertheless, the RFID industry has widely publicized its plans to tag individual consumer items with low-cost RFID chips called electronic product codes (EPC) tags.

EPC tags are poised to replace the ubiquitous UPC barcode now on most consumer goods. EPC tags are passive, powered by the radio-frequency signals that interrogate and read them. Thus, tags do not need costly and bulky batteries, which means that manufacturers can incorporate them directly into product packaging or embed them in high-value consumer products such as shoes or jackets. There are even plans for tags that could be directly printed on paper because paper manufacturers could embed RFID tags directly into product packaging, retailers and manufacturers would not have to label their own products. And because they do not require batteries, such tags could be functional for many years—or decades—after they leave a store.

RFID pros and cons

Clothing and apparel companies Swatch, Prada, and Benetton have RFID tags in their products. Katherine Albrecht, who led a successful boycott against Benetton regarding its RFID-labeled products, claims that these tags pose a serious threat to consumer privacy because they can be used to track people as they move about the physical world. Tags also could broadcast personal information, such as underwear brands or medical prescriptions, to passersby with an RFID reader. For these reasons, Albrecht expressed concerns about rushing headlong into RFID deployment, and called for the establishment of RFID fair-information practices.

While there are many legitimate privacy concerns regarding RFID, some claims have no legitimate basis. Matt Reynolds, founder of ThingMagic, an RFID systems manufacturer, an RFID systems manufacturer, presented both theoretical and practical performance limits for RFID systems. While most EPC-type tags under federal broadcast regulations have a theoretical limit of approximately 10 meters, in practice, Reynolds said, reading ranges are much shorter.

Additionally, many tags are difficult to read when in proximity to metal or liquids. A thin metal-foil layer effectively blocks tag communications. Holding tags close to one's skin might also render them unreadable. Dan White, technical evangelist for NCR Corporation, demonstrated how difficult it is to accurately read RFID tags in the cluttered environment of a supermarket. White also demonstrated a small RFID "killing chamber," which could allow consumers to disable their tags at checkout.

Regardless of their physical performance limitations, threats attributed to RFID systems often go unanswered in the public forum. In his keynote speech, Peter de Jager discussed mistakes made by RFID industry in public relations. He believes that RFID manufacturers provided ammunition to privacy activists with marketing claims that RFID can "tag anything" as well as through a lack of public disclosure regarding the systems' capabilities and use.

De Jager discussed the recent revelation that Wal-Mart had conducted an unpublicized trial of item-level RFID tags manufactured by Alien Technology on unsuspecting customers in the town of Broken Arrow, Oklahoma. Illustrating how a sensationalist media could present the story, de Jager made-up the facetious, yet factually correct, tabloid headline: "Secret Human Trials of Alien Microchips Exposed in Broken Arrow." He suggested that RFID makers avoid evoking menacing notions of alien abductions or conspiracy theories when trying to earn public trust.

In addition to sensible public-relations approaches, researchers at the workshop proposed several technological solutions. One obstacle in securing RFID systems is that cost requirements limit the tags' computational resources. Currently, it costs approximately US$0.25 per tag to implement public-key cryptography or strong symmetric algorithms for EPC-type tags. A successful EPC system needs to cost under US$0.05 per tag.

Ari Juels, principal research scientist at RSA Laboratories, emphasized the danger of deploying RFID without proper security and offered two technical solutions. One is a minimalist cryptographic approach, using simple security mechanisms in RFID's tight resource limits. Another idea is the *blocker tag*, which sends false identification numbers to unauthorized readers and essentially hides valid tags from nearby snoops.

A proposal by Kenneth Fishkin, a researcher at Intel, leverages the passive powering of EPC-type RFID tags for added security. The power level an RFID tag receives drops as the tag-to-reader distance increases. Thus, we might configure tags to ignore queries below a minimum energy threshold. Valid queries would have to originate close by, making it more difficult for someone to read tags at a safe distance.

Free software advocate Richard Stallman offered a more proactive solution: arm consumers with RFID seek-and-destroy devices. He proposed developing a low-cost device to detect and deactivate RFID tags.

Public policy decisions needed

The best protection for vulnerable consumers might be a strong public policy on RFID privacy. A position paper, which several privacy groups, including CASPIAN, the Privacy Rights Clearinghouse (www.privacyrights.org), the ACLU (www.aclu.org), and several others, issued at the workshop, asked for a voluntary moratorium on item-level tagging. It called for a formal technology assessment and the adoption of a set of Principles of Fair Information Practice specified in the position paper. Privacy Rights Clearinghouse Director Beth Givins suggested several RFID rights and responsibilities, including keeping RFID systems open, preventing involuntary tracking of individuals, and avoiding coercion of consumers to keep live tags.

Summarizing the day's presentations, Harvard Law professor Jerry Kang framed the RFID issue as part of a larger debate. He suggested that rather than focusing on technique, participants should delve into the political issues relevant to RFID. Kang posed several substantive choices that society must make about RFID and privacy in general: Who controls the information that RFID systems generate? How do people make difficult decisions about using RFID in the presence of coercion or lack of viable alternatives? When does society have the right to override individual privacy? Kang said that tackling issues like RFID privacy requires us to look closely at our society's entitlements and embodiments of power.

During a town-hall meeting at the closing of the workshop, attendees appeared to reach consensus on several issues. Privacy advocates and RFID makers agreed that full disclosure to consumers is essential; that consumers should be notified of the presence of an RFID tag in their purchases. Most parties agreed that consumers also should have the right to kill or disable any RFID tags on items they purchase. Finally, there was little concern over using RFID tags at the pallet level; concern only arose regarding tagging individual items with unique identifiers.

Most participants viewed the RFID Privacy Workshop as a first step in an ongoing dialogue about balancing consumer rights and the RFID system's benefits. While RFID adoption continues to gain momentum, manufacturers are aware that sufficient consumer fear and outrage could stop the technology in its tracks. Despite exaggerations of some privacy concerns, many legitimate issues, such as protecting consumers from tracking, still need to be addressed by both researchers and policy makers. □

Stephen A. Weis *is a graduate student at MIT's Computer Science and Artificial Intelligence Laboratory. His research interests include cryptography and information security. He has an MSc in computer science from MIT and is a member of MIT's Cryptography and Information Security Group. Contact him at sweis@csail.mit.edu.*