

Table of Contents

United RFID 1

United RFID

By Benjamin Mako Hill

Since their introduction, RFID tags have been the subject of intense debate between privacy, consumer rights, and civil liberties groups and the companies that produce or employ them. Through their near invisibility and the fact that, unlike bar-codes and magnetic strips on credit cards, they can be read silently and imperceptibly from a short distance, RFID tags introduce the potential for violations of privacy in unprecedented ways. Benjamin Mako Hill catches up with the state of the art

Pushing a shopping cart full of food out the supermarket door without stopping – the price of the goods in your cart is tallied and automatically debited from your bank account. Invisible checkpoints where police can identify you and the precise contents of your wallet or purse – down to the amount of cash you're carrying and a log of when and where those notes changed hands. With the use of Radio Frequency Identification (RFID) tags, such scenarios, while still far-fetched, are becoming increasingly possible.

RFID tags are similar to the tags that airports and airplanes use to identify each other. Each 'tag' broadcasts unique identifying information over radio frequencies while receivers listen for these signals. The data stored and broadcasted by the tag is usually a unique number (usually under 40 digits) hard-coded into the chip. This number is associated with data in a computer to establish identity and information about the transmitter.

Over the past decades, RFID tags have quietly made their way into library books, clothing, identification cards and toll road 'Speed Passes.' Retail giant Walmart has required that its suppliers include RFIDs in pallets (although not individual items) by the end of 2004. The most modern tags are tiny transistors and microchips that harness the power of the receiver's radio signal to eliminate the need for batteries and bulk while reducing the cost to only a few pence. The smallest chips to date, 'mu-chips' made by Japanese electronics giant Hitachi, measure only a third of a millimeter across plus a hair-sized antenna. This has allowed the European Central Bank to consider a plan to place tiny RFID tags in each euro note in an attempt to cut down on counterfeiting and money laundering. As the chips become smaller and cheaper, their potential uses – and abuses – rapidly multiply.

The most simple abuse is in the potential for corporations and individuals with tag readers and access to RFID databases to do silent electronic searches without the knowledge or permission of the person being searched. For example, when you buy a shirt with an RFID tag sewn into the fabric, your personal information – through a credit card or loyalty card – may become associated with the unique ID broadcasted by the tag in your shirt. Each time you walk through an RFID scanner with knowledge of your shirt's tag, the history of your shirt – and your own history through association – becomes available to anyone with access to the information in the store database. Realistically, the proprietary nature of most corporate databases will mediate, but not eliminate, the danger of this type of abuse.

The more worrying type of abuse is happening at the hands of governments. State programmes to interconnect existing databases, like the US Department of Defense's proposed 'Total Information Awareness', will be able to bring together vast amounts of personal and identifying data with the physical presence location of individuals. While the presence of chips will not always indicate the presence of an individual, it will be accurate enough to provide impetus for such use.

[IMAGE]

The advocates of RFIDs have already demonstrated its usefulness and desirability. Amidst the hype, they have largely ignored or unfairly dismissed the potential for privacy abuse introduced by the technology. Although RFID is still prohibitively expensive and readers are only reliable within close proximity (2-3 meters) to a tag and rarely capable of reading multiple chips simultaneously, these limitations are only temporary. In this early stage of the technology's life, privacy, civil, and consumer rights groups still have an opportunity to influence the nature of how this technology is and isn't used. It's important that these discussions happen now.

Benjamin Mako Hill <mako AT bork.hampshire.edu> is a Free Software advocate and a member of the Debian Project