

**Prepared testimony of Lee Tien
Senior Staff Attorney
Electronic Frontier Foundation**

before the

**Senate Judiciary Committee
Senator Joseph L. Dunn, Chair**

of the

California Legislature

**In support of the Identity Information Protection Act (S.B. 682)
April 26, 2005**

Introduction

Mr. Chairman, I thank you and the Committee for the opportunity to testify today in support of Senate Bill 682 and to discuss some technical issues that militate strongly against the use of radio-frequency identification (RFID) technology in widely used, necessary credentials like driver's licenses, student ID cards, and medical or health benefits cards. This prepared testimony gives my relevant background.

Background

I am a senior staff attorney with the Electronic Frontier Foundation, a non-profit San Francisco based group that focuses on civil liberties issues associated with computers and other advanced technologies. I specialize in free speech and privacy issues, both as a public policy advocate and as a litigator.

I am one of the nation's most active privacy advocates on the subject of RFID technology. In 2003, I testified on library RFID privacy issues before Senator Debra Bowen's committee and helped write a major policy statement on RFID and consumer privacy. Over the past few years, groups such as the American Library Association, the National Academy of Sciences, and the Federal Trade Commission have invited me to speak about the privacy dangers of RFID.

I am also well known in the legal community for my work in the area of encryption. I successfully sued the National Security Agency for access to classified records about cryptography. I have represented people who write encryption software, and people who

attack encryption. Most recently, I advised Prof. Avi Rubin and his team of information security researchers at Johns Hopkins University about legal issues surrounding their successful attack on the encryption scheme of the Exxon/Mobil SpeedPass RFID card. <<http://rfidanalysis.org>>

Discussion

I will cover three topics today. First, why are RFID devices problematic from a privacy and security perspective? Second, why is their use in driver's licenses and other widely used ID cards especially dangerous? And third, why are common information security techniques like encryption unlikely to work for RFID-enabled ID documents?

A short note on basic security principles

I begin by emphasizing some important points about information security. First and most important, information security is hard. There is no set recipe for information security and no simple yardstick for measuring whether a system is secure. The basic problem is that security is adversarial: you must protect against smart, resourceful attackers – including “insiders” with knowledge of and access to the system.

Bigger, more complex systems are even harder to secure. Not only are there more points to attack, it is harder for the system's guardians to keep track of all the system components. Often, the system components do not work together as well as they should, introducing weaknesses that are unknown to the system administrators until they are exploited. This problem plagues all complex computer systems, from personal computer operating systems like Microsoft Windows to the software and protocols that underlie the Internet itself.

A recent incident illustrates the problem. Early on the morning of March 7, burglars rammed a vehicle through a back wall at a North Las Vegas DMV office, driving off with 1700 blank Nevada licenses, the equipment needed to make licenses, and a hard drive containing the Social Security numbers and other personal information of 8,738 people who had gotten licenses there since November 2004.

Note that the Nevada DMV initially believed that the stolen information was encrypted. That turned out to be false; the government did not know what its outside contractor was doing with the data. Second, the head DMV official said afterward, “who would've thought someone would take a truck and drive it in the back of an alarmed building?” Unfortunately, good security is supposed to anticipate “low-tech” as well as high-tech threats.

Second, in evaluating information security, it is critical to use multiple, reputable, independent specialist advisors. Manufacturers and sellers of all high-technology equipment, including RFID tags, are naturally self-interested and prone to give

questionable assurances. Often, they lack the expertise in overall system security to actually understand all of the security issues. Many manufacturers, even of specialist security products, have been surprised when their systems fell to relatively common, standard attacks.

Finally, any good security analysis anticipates future, unknown threats, not just the current, known threats. Attack and defense techniques improve over time, but the choices we make today may last for the foreseeable life of the system. More important, we must protect this data for the sake of the people whose lives could be harmed by privacy and security failures. The government has a fiduciary duty to protect the information it collects from them against potentially harmful disclosure. Accordingly, security must be thought of as a continual, evolving process, not as a state that can be established once and for all.

The privacy and security problems of RFID tags

The fundamental problem with RFID technology is simple: RFID tags and RFID readers communicate using radio waves, and radio-frequency transmissions in general are physically insecure. Exposed or publicly available information channels are harder to secure than wires or cables.

Several factors make RFID tags especially dangerous to privacy.

- RFID tags are *promiscuous*: they are generally designed to be activated, and their transmissions receivable, by any compatible reader/sensor device
- RFID tags are *stealthy*: when RFID tags are being read, the people carrying the tags don't know that it's happening
- RFID tags are *remotely readable*, and can be read *through* many common substances (cloth, leather, paper)

Moreover, RFID reading devices are easy to build, and will be easier to build as RFID technology spreads. Nokia last year unveiled a cell phone that can read RFID tags. RFID Journal, *Nokia unveils RFID phone reader* (March 17, 2004)

<<http://www.rfidjournal.com/article/articleview/834/1/13/>> There already exist SD cards for Palm-compatible handhelds that can convert popular PDAs like the Treo into RFID readers. <<http://www.engadget.com/entry/1234000257034127/>> German hacker Lukas Grunwald used his RFDump software on a PDA equipped with an RFID reader to read and write to RFID tags in a German grocery store. Arik Hesseldahl, *A Hacker's Guide to RFID* (July 29, 2004)

<http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html>.

In short, RFID tags are designed for convenience of reading, but that convenience comes with a high cost to privacy and a high risk of identity theft. EFF believes that in the vast

majority of applications, ID cards that require physical contact with a reader will meet organizational goals with far less harm to privacy.

Privacy threats

1. Unintended or unauthorized disclosure of personal or sensitive information

The most obvious threat is that information might be read from a card for inappropriate use without the holder's knowledge or consent. Any compatible reader within range of the RFID tag could read the stored data. Read range varies depending on the radio frequency being used, the power of the reading device, and many environmental factors.

For instance, communications using the Bluetooth radio protocol, originally designed for a read range of about 30 feet, have been successfully captured from more than a mile away by modifying reading devices. Kim Zetter, *Security Cavities Ail Bluetooth* (Aug. 6, 2004), <<http://www.wired.com/news/print/0,1294,64463,00.html>>. The results of this research have led to the creation of a step-by-step tutorial so well written that virtually anyone can read and replicate these modifications.

<<http://www.tomsnetworking.com/Sections-article106.php>>

But while much public concern about RFID tags and privacy has focused on remote reading over long distances, we should be more concerned about short-range reading. If RFID technology continues to proliferate, the main practical threat to the average person will be RFID readers built into the everyday social environment: gas pumps, shopping malls, office buildings, and “reader gates” of all kinds.

Eavesdropping is a second type of information disclosure threat. In eavesdropping, the attacker does not read the information directly from the RFID tag or card; instead, the attacker listens to the transmission between the RFID tag and an authorized RFID reader. Researchers have described an eavesdropping “relay attack” using two devices: a “leech” that can be as far as 50 centimeters from the RFID device, and a “ghost” that can be up to 50 meters away from the authorized reader. Ziv Kfir and Avishai Wool, *Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems* (2005), Cryptology ePrint Archive, Report 2005/052 <<http://eprint.iacr.org/2005/052>>.

The eavesdropping threat is the main reason why merely shielding RFID devices is inadequate to protect privacy, because the RFID card must be exposed in all legitimate transactions.

2. Clandestine tracking (real-time or forensic/after-the-fact)

An RFID card also enables others to secretly monitor its holder's whereabouts and possibly his or her actions. As the number of RFID readers in the social environment increases, the easier it will be to track RFID tags.

Importantly, the tracking threat exists even if the RFID tag contains no name or other personal information. What matters is that the RFID tag contains a static unique number or pattern that is or can be persistently associated with a person's identity. So long as the RFID tag or chip broadcasts this information, the person carrying that tag can be distinguished from any other person carrying a different RFID tag.

For example, suppose the RFID tag in your ID card always transmits the number 1732. Anyone with a reader within range can read 1732 from your card, and can distinguish you from someone carrying a card that transmits 1414. The reader owners need only know that you carry the card that transmits 1732 in order to track you.

Note also that the tracking threat is not merely a real-time threat. Someone may record 1732 in multiple locations without knowing that you are 1732. But once they associate 1732 with you, then they know where you have been. And there are many ways to associate you with 1732.

3. The "key" problem:

Any unique ID number on the card may be a "key" to personal information stored in a database somewhere. Our society often uses unique ID numbers to index or organize personal information in databases, or as a linking or matching identifier across multiple databases. The worst-case scenario would be a commonly used unique number like a Social Security number, phone number, or a driver's license number, which is already used to index and link personal data.

But even if a new unique ID number were generated for RFID cards, such as driver's licenses, that number would presumably act as a "key" to the individual cardholder's information in the DMV database. Unless strict precautions against "function creep" were taken, any new unique ID number could very well become widely used as a "key" to data about you – not only in government databases, but also in private-sector databases – like the Social Security number, which did not become a "key" to personal data overnight.

Security threats

RFID tags also present security issues, such as "cloning" or duplication and card forgery. If the RFID tag is read, but the card itself is not examined cloning the RFID tag alone might suffice for an illegitimate purpose. This could easily occur in "walk-through" application when the card is read from one's wallet, pocket or purse, or in "self-service," automated contexts when no person actually looks at the card. If the RFID tag is read while the card is presented but not examined closely, cloning the tag or even forging the tag combined with a stolen blank card or a forgery of the actual card might be enough.

Remember that the Nevada burglars mentioned above escaped with 1700 license blanks and laminated covers bearing the embossed state seal.

The special problems of driver's licenses, ID cards, and other mass applications

I noted earlier that information security gets harder as systems get bigger. As a result, *mass applications* – applications with large numbers of devices and users, large number of authorized readers, and large numbers of authorized uses – are especially problematic from a privacy and security perspective.

- More equipment to reverse engineer: If there are millions of RFID tags in circulation, and thousands of official RFID readers, it is highly likely that attackers will figure out how to defeat security.
- More equipment to protect: The sheer quantity of available equipment means that there is more scope for insider abuse, e.g., the misuse of authorized readers by authorized persons, as well as the loss of control of authorized readers to unauthorized persons.
- If there are many authorized uses, there will be more variation in the places or settings to be secured; there will not be one or a few standard, well-understood settings to control.
- Mass systems are more attractive to attackers because the payoff from a successful attack is so great. In the security world, this is called the “Fort Knox” problem.
- Conversely, the potential harm from compromise to a mass application is much greater – as is the cost of recovering from a breach.

This last point is especially important, because it is often neglected. Systems always fail. It is therefore important to design systems to fail well. Consider again the fallout from the Nevada security breach. Nevada is invalidating the driver's license numbers of the 8738 people whose information was in the computer and sending new licenses to each of them via certified mail. The old numbers were entered into a national security database and will be flagged if they come up during traffic stops or in other checks. Also, the three major credit-reporting bureaus were asked to watch for unusual credit activity involving people whose personal information was stolen.

What encryption and “unique identifiers” can and can't do

We often think that encryption, access control, and other techniques provide adequate information security. Properly implemented, strong encryption can protect information against the first-level threat of information disclosure (i.e., simply reading data from the card or eavesdropping on authorized transmissions) and against brute-force attacks on the encryption itself.

Unfortunately, these theoretically powerful techniques can be very difficult to implement properly and are especially unlikely to succeed in the real world of mass applications. The general problem of security for mass applications is relatively simple: when many entities are entitled to decrypt or otherwise access the protected information, it is very

hard to keep that information protected. Ways around some of these problems may be found with more sophisticated cryptography, but the intelligence required for such high-end tags in mass applications will probably be much more expensive than industry and government would be willing to adopt.

Problems with encryption

1. Even if the data stored on the RFID card is encrypted, an enormous number of authorized users (whether state or local officials or commercial users) would be in a position to abuse their authorized access to the data. If the data were read directly from the cards themselves, rather than from a central database, it would be difficult to maintain an audit trail of access to the data, and therefore very difficult to detect abuse.

2. Even if the data stored on the RFID card is encrypted, an attacker could eavesdrop on a legitimate data transmission between the RFID card and the RFID reader. For instance, if the system were designed so that RFID card only transmits after it receives a secret code or PIN from a legitimate RFID reader, an attacker could capture the PIN while it is being sent. Alternatively, if the data on the RFID card is encrypted while stored, but is transmitted in decrypted form, an attacker could capture the decrypted data when it is being sent to the RFID reader.

3. By definition, every authorized RFID reader can decrypt the data stored on RFID card. Thus, many thousands of readers would have access to the keys needed to read the RFID cards. There are two main scenarios here.

a) If every card is protected by the same encryption key or PIN (like ATM cards), then each reader would need to have that PIN or key. It is essentially impossible to maintain the confidentiality of such widely distributed information. Researchers have successfully extracted PINs from supposedly secure smart cards and successfully extracted encryption keys from stolen card readers. Once the system has been compromised, “bootleg” readers could easily be created. One might also steal the PIN or key from inside the system. Storing the key in, say, an attached computer system, rather than in the reader hardware itself, makes this attack easier, not harder. The computer is just as easy as the reader to steal, and generally easier to extract the key from. Over time, the result would be essentially the same as not using a PIN and not encrypting the data.

It is hard to imagine how the system would recover from this sort of breach.

b) If a different PIN or key were used for each card, then readers would need access to the PIN or key for each card read. This creates enormous complexity and logistical problems, as well as a large set of difficult security concerns.

For instance, suppose that each RFID card’s PIN or encryption key is kept in a central database that authorized RFID readers could access. The implications include:

- It would be impossible to use RFID readers without some communication channel to the central database, possibly making the readers unusable in many field applications.
- Any such communications channels would need to be protected against eavesdropping.
- Complicated access control and authentication mechanisms would be needed to ensure that queries to the database truly came from legitimate readers.
- It would still be possible to steal or "borrow" and abuse a legitimate reader.

4. Encryption cannot solve the tracking problem

I earlier discussed how the tracking problem stems from the use of a persistent or static unique identifier. Encryption transforms the original information into different information, but the result will still be unique. Accordingly, encryption cannot solve the tracking problem because encrypting unique information will result in different, but still unique, information.

5. Encryption does not protect against cloning.

To clone the data stored in an RFID tag, it is only necessary to copy the encrypted data verbatim from one chip to another. One need not be able to understand the data. Furthermore, static digital signatures or certificates do not prevent cloning. A digital signature proves only that the data is the same as the data signed by the signing authority. Copying the entire contents of the chip, including the digital signature, will create a card that appears as valid to verifying software as the original, unless additional precautions are taken.

Problems with unique identifiers:

Storing only a unique identifier on the RFID addresses the first-level information disclosure problem, because there would be no personal information to be captured. Unique identifiers do not, however, address tracking and "key" problems. So long as *any* unique identifier is readable without additional safeguards, neither encryption nor PIN-based access control protects against tracking. If an identifying number is available, it can be used to track the card's movements, and then later used to link the card to the holder's identity. Even if the *entire* contents of the chip are encrypted, it remains trackable; the encrypted data block itself provides a unique identifier.

Conclusion

I will end with a simple analogy that may illustrate the problems with trying to use technical measures like encryption to protect information used in mass applications. Imagine that you have a really good lock on your car, but many keys to your lock are floating around, and many people are legitimately allowed to hold those keys. How secure is your car?