RFID Feared as Possible Terrorist Target

March 28 2007

London's Royal Academy of Engineering suggests that someday a terrorist will be able to read personal details from a distance and set a bomb to go off when a particular person gets within range.

As if RFID chips in driver's licenses and passports weren't scary enough already, London's Royal Academy of Engineering is suggesting that someday a terrorist will be able to read personal details from a distance and, given the right antennas and amplification, set a bomb to go off when a particular person gets within range.

It's already widely acknowledged that unencrypted data stored on an RFID chip in a passport can be read covertly by anybody with a pass-by reader.

As the ACLU pointed out at Black Hat earlier in March, you can buy parts on the Internet to make a reader for as little as $20.

With a reader, you can pick up whatever the RFID chip is sending out: passport number; name; where an individual was at, at what time; name; address; Social Security number, etc.

The ability of RFID to be subverted in far more dangerous ways was only one example of how advancing technology can be exploited in the future, according to the Royal Academy.

The Academy on March 26 released a report titled "Dilemmas of Privacy and Surveillance: Challenges of Technological Change," by

Nigel Gilbert, chairman of the Academy's group on Privacy and Surveillance.

Here are some other technology shocks that have already occurred or that may come to pass, according to Gilbert:

Unencrypted data can be forged. The United Kingdom, for one, introduced biometric passports in March 2006.

The e-Passport, as it's called, uses facial recognition to link an individual with a paper passport, with iris and fingerprint data used as backup, and other countries have expressed interest in using biometrics as well.

Because the data will be read at places such as passport control to verify the identity of the holder, the data have to be quickly and reliably transmitted - hence, use of RFID chips have been proposed.

A forged passport could include a passport carrier's biometric information but with forged personal details, including name, date of birth and citizenship.

Of course, passports could be checked against a central database to ensure that the data on a given passport matches the master set. But then, it's unnecessary to store the data on a passport, since it can be retrieved from the central database.

"Encrypting the data on the e-Passports can help to avoid these problems," Gilbert writes, "but even then there is potential for failure. Firstly, if the encryption codes can be broken, then the two vulnerabilities reappear. Secondly, a problem with current plans for e-Passports in the U.K. is that the key for the data on the chip is stored on the passport itself - so the encryption does not in fact lock out eavesdroppers."

The only way to keep RFID passport information truly safe, Gilbert says, is to encrypt with extremely tough algorithms and to disable the access to encrypted data on the passport by using a key stored on the passport itself.

"Otherwise, efforts should be focused on an altogether different way of designing e-Passports," he said.

Plans for more dangerous data leaks than ever are in the works.

It's a pedophile's dream come true: children's data stored in a national database.

The U.K. is reportedly planning to take fingerprints as well as names and addresses from children as young as 11 and store it all in a government database.

The children's data, as a subset of the U.K.'s biometric passport scheme, will be transferred to the country's new national identity database when the children turn 16.

The consequences of data breaches or leaks on such a database could be "extremely serious," Gilbert says. "This information could be used by pedophiles to target those children for abuse," he writes.

Other serious data leaks that have happened or could still happen, Gilbert points out: leaks of credit-card data used to embarrass public figures; leaks of the addresses of staff who work at sensitive sites, such as abortion clinics or research centers that practice animal experimentation; leaks of health records that could doom the employment prospects of patients or even expose them to risk of violence, including HIV status or a record showing that a woman had had a pregnancy terminated (if this was unknown to her partner or parent), or data (such as DNA or blood group) showing that the paternity of a child could not be the presumed father.

The report details other worst-case scenarios, including identity fraud assisted by the Semantic Web and its extensive publicly accessible personal details of individuals as well as the use of fingerprint images to fool a pay-by-touch system.

The future of technology misuse may look dire, but Gilbert offers ways to secure even the scariest technology.

For example, A biometric pay-by-touch system that requires two forms of identification - a PIN and a fingerprint - would be "much more successful" in preventing fraud than one that relies only on a fingerprint, he said.

Regarding RFID-enabled passports and the possibility that they could be linked to bombs or other, less dramatic abuses, one workaround is to forgo RFID chips for a technology such as that now being developed by Ingenia Technology called "Laser Surface Authentication."

LSA technology takes into account the unique surface qualities of a given document. Paper documents and credit card plastics have unique microscopic surface qualities attributable to how paper fibers are arranged or how the plastic has been set.

"These qualities cannot be controlled and cannot be copied, and they are unique in every case - rather like human fingerprints," Gilbert writes.

"Ingenia have devised a way of scanning documents to reveal these surface properties, which they refer to as the 'LSA fingerprint.' The system they have created is 'read-only', the document is passive, it is simply scanned and a record of its surface features is recorded."

Citation: RFID Feared as Possible Terrorist Target (2007, March 28) retrieved 3 May 2024 from https://phys.org/news/2007-03-rfid-terrorist.html