Safer swiping while voting and globetrotting

April 15 2010

This is a home-made, extended-range RFID antenna made from cooking gas copper pipes in Professor Wool's lab. Credit: AFTAU

Since 2007, every new U.S. passport has been outfitted with a computer chip. Embedded in the back cover of the passport, the "e-passport" contains biometric data, electronic fingerprints and pictures of the holder, and a wireless radio frequency identification (RFID) transmitter.

Although the system was designed to operate at close range, hackers were able to access it from afar — until research by Prof. Avishai Wool of Tel Aviv University's Blavatnik School of Computer Sciences helped ensure that the computer chip in American e-passports could be read only when the passport is opened. The research has been cited by

organizations including the Electronic Frontier Foundation.

Now, a new study from Prof. Wool finds serious security drawbacks in similar chips that are being embedded in credit, debit and "smart" cards. The vulnerabilities of this electronic approach — and the vulnerability of the private information contained in the chips — are becoming more acute. Using simple devices constructed from $20 disposable cameras and copper cooking-gas pipes, Prof. Wool and his students have demonstrated how easily the cards' radio frequency (RF) signals can be disrupted. The work will be presented at the IEEE RFID conference in Orlando, FL, this month.

More than one way to hack a chip

Prof. Wool's most recent research centers on the new "e-voting" technology being implemented in Israel. "We show how the Israeli government's new system based on the RFID chip is a very risky approach for security reasons. It allows hackers who are not much more than amateurs to break the system," Prof. Wool explains. "One way to catch hackers, criminals and terrorists is by thinking like one."

In his lab, Prof. Wool constructed an attack mechanism -- an RFID "zapper"— from a disposable camera. Replacing the camera's bulb with an RFID antenna, he showed how the EMP (electro-magnetic pulse) signal produced by the camera could destroy the data on nearby RFID chips such as ballots, credit cards or passports. "In a voting system, this would be the equivalent of burning ballots — but without the fire and smoke," he says.

Another attack involves jamming the radio frequencies that read the card. Though the card's transmissions are designed to be read by antennae no more than two feet distant, Prof. Wool and his students demonstrated how the transmissions can be jammed by a battery-

powered transmitter 20 yards away. This means that an attacker can disable an entire voting station from across the street. Similarly, a terror group could "jam" passport systems at U.S. border controls relatively easily, he suggests.

The most insidious type of attack is the "relay attack." In this scenario, the voting station assumes it is communicating with an RFID ballot near it — but it's easy for a hacker or terrorist to make equipment that can trick it. Such an attack can be used to transfer votes from party to party and nullify votes to undesired parties, Prof. Wool demonstrates. A relay attack may also be used to allow a terrorist to cross a border using someone else's e-passport.

How to make "smart cards" smarter

"All the new technologies we have now seem really cool. But when anything like this first comes onto the market, it will be fraught with security holes," Prof. Wool warns. "In America the Federal government poured a lot of money into e-voting, only to discover later that the deployed systems were vulnerable. Over the last few years we've seen a trend back towards systems with paper trails as a result."

But there are some small steps that can be taken to make smart cards smarter, says Prof. Wool. The easiest one is to shield the card with something as simple as aluminium foil to insulate the e-transmission. In the case of e-voting, a ballot box could be made of conductive materials. The State Department has already taken Prof. Wool's advice: since 2007, they've also added conductive fibres to the back of every American passport.

Provided by Tel Aviv University