

Releases by AP 1/30/05 and commentary

*** The full text Johns Hopkins Research paper is posted on line at <http://rfid-analysis.org/>

RESEARCHERS CRACK CAR SECURITY CODE

BALTIMORE - Researchers said yesterday that they have found a way to crack the code used in millions of car keys, a development they said could allow thieves to bypass the security systems on newer car models. The research team at Johns Hopkins University said it discovered that the "Immobilizer" security system developed by Texas Instruments could be cracked using a "relatively inexpensive electronic device" that acquires information hidden in the microchips that make the system work. (AP)

RESEARCHERS CRACK CAR SECURITY CODE

By BRIAN WITTE

BALTIMORE (AP) - Researchers said they have found a way to crack the code used in millions of car keys, a development they said could allow thieves to bypass the security systems on newer car models.

The research team at Johns Hopkins University said Saturday it discovered that the immobilizer security system developed by Texas Instruments could be cracked using a relatively inexpensive electronic device that acquires information hidden in the microchips that make the system work.

The radio-frequency security system being used in more than 150 million new Fords, Toyotas and Nissans involves a transponder chip embedded in the key and a reader inside the car. If the reader does not recognize the transponder, the car will not start, even if the key inserted in the ignition is the correct one.

Its similar to the new gasoline purchase system in which a reader inside the gas pump is able to recognize a small key-chain tag when the tag is waved in front of it. The transaction is then charged to the tag owners credit card.

Researchers said they were able to crack that code, too.

We stole our own car, and we bought gas stealing from our own credit card, said Avi Rubin, a professor of computer science at Johns Hopkins who led the research team.

Texas Instruments was recently given demonstrations of the teams code cracking capabilities, but the company maintains its system is secure.

Tony Sabetti, a business manager with Texas Instruments, said the hardware used to crack the codes is cumbersome, expensive and not

practical for common thieves.

I think the way in which its presented as being inexpensive to do and quick and all the rest of that is an exaggeration, Sabetti said. And because of that, we believe the technology still is extremely secure for the applications that its used in.

But Rubin said the code-breaking demonstrations illustrate that developers did not pay enough attention to security.

I think the implications are that it sets us back about 10 years ago where we were with car security, Rubin said.

In the seven years the technology has been in use, Texas Instruments has never had a reported incident where a car has been stolen or a gasoline-purchasing tag has been duplicated, company spokesman Bill Allen said.

The Johns Hopkins team, which was funded by Bedford, Mass. based RSA Security Inc.*, recommended distributing free metallic sheaths to cover the radio frequency devices when they are not being used.

* A public company with 2003 revenues of \$259.9 million which is located in Bedford, MA. WWW.RSA.com

January 29, 2005 - Spy Blog

Johns Hopkins University and RSA Labs demonstrate RFID token cracking and cloning with cheap FPGA hardware.

A low cost spoofing and cloning attack has been **demonstrated by researchers from Johns Hopkins University and RSA Laboratories** on some Texas Instruments RFID tag based tokens, used for transport road tolling and the purchase of fuel at petrol stations, and as part of a car key vehicle immobiliser system.

The researchers created a cheap code cracking device from off the shelf **Field Programmable Gate Array** hardware, to brute force attack the 40 bit keyspace. They wrote software to simulate the radio protocols of the RFID tokens on a laptop computer connected to radio equipment.

These tokens do **not** use modern **strong** cryptography, such as the AES algorithm, but the attack demonstration (including **online videos**) should be seen as a **dire warning** for the likes of Tesco, WalMart or the US Department of Defense who seem to be set to use billions of far less sophisticated yet still re-programmable RFID tags e.g. EPC Class 1 Generation 1 or Generation 2 tags, which **do not use any encryption at all !**

It also has implications for the **privacy and security** of new **USA Biometric Passport** for which it is also planned to use **unencrypted RFID chips**.

TEXAS INSTRUMENTS SYSTEMS - EMc

Vehicles by Chrysler Corporation, Ford Motor Company, most Infinities and Nissans, Jeep, Toyota & Lexus, most Mazda & most Jaguars are equipped with an Immobilizer manufactured by Texas Instrument.

Systems manufactured by Philips & Megamos utilize different technology than TI.

TRANSPONDER OVERVIEW (posted on this site) identifies the manufacturer of each vehicle's Transponder System.

Commentary - This disclosure is not as bad as it first appears. The Brian Witte release actually contains a little perk from TI - that they know of no instance in 7 years of their system being defeated.

It is my understanding at this point that the equipment is large, not generally available and that it has to be very near an existing key.

Like always, Motive will remain the most important aspect in an analysis of a theft claim involving a vehicle equipped with Immobilizer technology.

Persons who may ultimately have access to this equipment will not be using it to steal a radio - the vehicles would be unrecovered or stripped of valuable components and not vandalized. Don't forget that the most of the vehicles involved also have high security type ignition locks.

I feel that this will prove to be the proverbial tempest in a teapot - to our business.

Fortunately I included identification the the security system's manufacturer for each of the vehicles listed in my Transponder Overview document on my web site. The vehicles equipped with Megamos and Philips systems use different technology and are not affected by the Johns Hopkins research.

None of the German cars use the TI system nor does GM.

I will post new INFO ASAP - EMc

[Article from the July 2002 RFID JOURNAL describing the TI system](#)

Stealing Cars Will Get Tougher

Texas Instruments' new vehicle immobilizers will make it more difficult for owners to conspire to cheat insurance companies.

July 3, 2002 -- Some people think that RFID will one day eliminate, or at least drastically reduce, theft. That day may not be far off ? at least as far as automobiles are concerned.

Texas Instruments has introduced a new version of its RFID vehicle immobilizer, which aims to stop not just theft but also fraud.

Insurers in Europe are finding that fraud is becoming a problem precisely because of the success of vehicle immobilizers, which were introduced in 1993 in response to the rapid rise in auto theft that followed the opening of Eastern Europe.

A study by Allianz AG, one of the world's largest insurers, revealed that between 1993 and 2000, vehicle theft in Europe dropped by 50 percent, largely because of the use of immobilizers. The first units required a unique serial number stored in an RFID tag in the key to match the number stored in a reader in the steering column. If the key didn't match, the car wouldn't start.

The current technology, which was introduced in 1997, uses an electronic signature for additional safety. The unit in the steering column generates a random number, which is transmitted to the key. The key combines the random number with its own unique serial number. The new number is encrypted and sent back to the unit in the steering column. If the numbers don't match, the car doesn't start.

Allianz and other insurers in Europe found that some criminals had figured out a way around the system -- use the key. Instead of hot-wiring cars, the criminals were conspiring with owners. The criminal pays the owner for a copy of the key and takes the car away, perhaps reselling the parts in Eastern Europe. The owner tells the insurance company that the car was stolen and gets reimbursed.

When the insurer asks to see the keys, the owner turns over the original keys and any copies, but doesn't tell the insurer that there was an extra copy, which was given to the co-conspirator.

To prevent this kind of fraud, Texas Instruments worked out an enhancement to its immobilizers, which it calls Digital Signature Transponder Plus, or DST+. The system allows data to be stored on individual keys and in the car, so that both the vehicle and the car know how many new keys have been made and even when they are used.

Here's how it works. A customer buys a new car and is given two keys. He wants to make two copies. Depending on the car manufacturer, he may have to go to the dealer, or he may be able to get them from a qualified locksmith. Each key has a unique serial number.

When the new key is used in the car, the unit in the steering column records the existence of a new key. The next time the original keys are used, the steering column unit writes data to the keys, so all keys have information on the existence of all other keys. The system can also store date stamps, so the insurer can check when each key was last used.

The system doesn't stop conspirators from making a copy and using it to get rid of the car before the existence of a new key can be recorded on the existing keys. But the unit in the car will know a new key has been used, so if the car is recovered, the insurer will uncover the fraud.

DST+ will be available on some 2004 models. "We feel we are first to market with this enhancement," says Tony Sabetti, global business unit manager for Texas Instruments RFID Systems. "The technology is backward compatible, so car companies that have

used our first and second generation systems will find this to be an easy upgrade."

Texas Instruments has also developed the 3D Analog Front-End RF chip, which automakers can use to allow passive entry. A reader in the car senses the presence of a transponder in a key fob or other form factor and automatically unlocks the doors. The car can even be programmed to start the engine and adjust the seats to a specific driver automatically. The feature will be installed on some 2003 vehicles.