Attack on a Cryptographic RFID Device

A team of researchers at Johns Hopkins University Information Security Institute and RSA Laboratories recently announced the discovery and study of a security weakness in a widely deployed, cryptographically enabled RFID tag manufactured by Texas Instruments. The Digital Signature Transponder (DST), as

TI calls this tag, helps secure millions of automobiles against theft and millions of payment transactions in Speedpass tokens against fraud. The JHU-RSA team consisted of six academic and industrial researchers, of which I was one.

The mechanism for digital security in the DST is an encryption algorithm, also known as a cipher. Every DST contains a secret, cryptographic key that it shares with trusted RFID readers. For example, a DST-equipped automobile ignition key shares a cryptographic key with an RFID reader in the automobile. (To clarify: The ignition key is physical, of course. The cryptographic key is digital, i.e., a secret string of bits.) To authenticate a DST—that is, to verify that an ignition key is legitimate—the reader in an automobile transmits a random string of bits to the DST in the ignition key. The DST encrypts this bit-string using its secret, cryptographic key and transmits a portion of the result as its response to the reader. Because the reader possesses the secret key too, it can verify the correctness of the response. In this way, the automobile distinguishes a valid ignition key from a bogus one.

The Texas Instruments DST encryption algorithm is secret and proprietary. One scientific result of the JHU-RSA team was a successful reverse-engineering (unraveling) of the DST encryption algorithm. We did not accomplish this by examining the internal workings of a DST. Rather, we obtained a rough schematic of the cipher from a published Texas Instruments presentation, and purchased several DST tags. Using a normal

TI RFID reader, we interrogated the DSTs in a carefully devised, mathematically structured way.

Having reverse-engineered the cipher, we demonstrated that the 40-bit length of its cryptographic keys is inadequate—not just vulnerable to brute-force attack, as the cryptographic community knows, but inadequate in the face of practical attacks against the DST system. We implemented a system of attack that operates in three phases against a target DST:

1. "Skimming": We use an RFID reader in our possession to establish brief radio contact with the DST. The reader interrogates the DST twice over the course of a fraction of second.

2. Key cracking: Employing the "skimmed" data, we use a specially programmed hardware "key cracker" to recover the unique cryptographic key of the DST. With a few hundred dollars worth of equipment, this takes about 10 hours on average. We are working on a software system that uses standard cryptographic techniques to crack a key in minutes.

3. Simulation: We program a hardware device with the cryptographic key recovered from the DST. This device can then impersonate the original DST; while our device is dissimilar in shape and size to a DST, it is digitally indistinguishable.

Loosely speaking, we demonstrated the digital cloning of DSTs. We believe that an attacker with the right expertise could manufacture a self-contained apparatus about the size of Apple iPod that implements all three phases of the attack. Such a device might cost as little as several hundred dollars.

Anyone capable of the attack we have demonstrated can effectively roll back automobile security by 10 years, contravening a mechanism that has been responsible, by some accounts, for a 90 percent reduction in automobile theft. Alternatively, such an attacker could charge gasoline purchases to a victim's Speedpass account. We have not created

a weakness in the DST: We have uncovered one with serious implications.

To validate the correctness and practical implications of our research, we purchased gasoline using a device that simulated a Speedpass tag that belonged to us. We likewise started an automobile in our possession with an ignition key that lacked its companion DST. Of course, in a real attack, additional security mechanisms like the fraud-protection mechanisms of the Speedpass network and the mechanical steering-column lock system in automobiles would pose additional impediments.

Setting aside the technical legwork to create the system, the difficulty of our attack (and thus debate about its impact) hinges on the difficulty of skimming. Using one of TI's standard RFID antennas, we have achieved an experimental skimming range of several inches. An attacker that brushes up near a victim's pocket or a parking valet handling a victim's car keys could easily skim a DST. In contrast to picking a pocket, an attacker can perpetrate skimming with relative ease and impunity.

We believe that longer skimming ranges—perhaps 1 or 2 feet—are possible, but have not yet tried to achieve these. A special form of skimming is possible in which an attacker *eavesdrops* on communications between a legitimate reader and DST. This type of attack could be viable at a distance of tens of feet or more. We have not yet experimented with such attacks.

It is easy to dismiss the seriousness of the practical threat posed by our attack. One might argue that the DST's encryption algorithm offers just one layer of protection in a larger security system. But automobile ignition keys and Speedpass fraud detection have obviously been insufficient to achieve good security by themselves. If encryption algorithms weren't needed, car keys and Speedpass devices wouldn't have them.

Similarly, some have noted that the JHU-RSA team of

researchers invested several months of effort and several thousand dollars of equipment in the project, as well as its professional expertise in cryptology (but not RF design)—resources beyond the reach of most lawbreakers. DST cloning is beyond the reach of petty criminals, but not organized ones, particularly given the stakes. Automobile theft is a multibillion industry; the FBI Uniform Crime Report estimates its total impact at $8.6 billion in 2003. As regards the practicality of skimming, we believe we have only scratched the surface. Speedpass, for example, comes in windshield-mounted form with significantly longer read range (and therefore, significantly longer skimming range) than the keychain variety—for good or ill.

Still, our work highlights a lesson far more important than the presence of flaws in the TI system. It is a warning for designers of future RFID systems. RFID devices of one sort or another are already present in building access cards and toll-payment transponders. They will soon proliferate into shipping crates and containers, wireless credit cards, library books, pharmaceuticals, aircraft parts, passports and eventually into consumer products. We will depend on RFID for security in ever more facets of our daily lives. Once RFID infrastructure becomes truly pervasive, strong security will be indispensable.

What now threatens to result in a little stolen gasoline could, in the absence of responsible security design, eventually pose a threat to individual safety and national security. Our hope is to stimulate responsible security design in the RFID community before this happens.

The Impact of Our Research

The data-security community has largely endorsed our research. We underscored the lessons of previous work by our scientific colleagues and shed light on the state of a widely fielded

system. In the RFID community at large, though, our research has produced a mixture of feelings. Some opine that the effect of our work was simply to weaken security in fielded DST-equipped systems.

Security experts and RFID users have the same interest at heart: They both want systems that are more secure. So why the disparities in perspective on our work? The science of cryptology has a long history of them.

In the worlds of cryptology and data security, there is a belief so fundamental that its practitioners often forget how far from self-evident it is. This belief has deep and venerable scientific roots. Roughly stated, it is the seemingly paradoxical tenet: *Greater openness means greater security.*

The 19th-century military cryptologist Auguste Kerckhoffs first set forth the idea as part of a treatise on encryption. He noted that the security of an encryption algorithm should depend not on the secrecy of its workings (i.e., the process of encryption), but instead on secret keys alone. His reasoning was that when an *encryption system* sees widespread use, it is prone to falling into hostile hands. A *key,* on the other hand, can be device- or communication-specific, and therefore hidden more effectively.

There is a second justification of Kerckhoffs' ideas. A publicly known cryptographic algorithm (or security system of any type) is open to the scrutiny of the scientific community, which can refine it and bolster confidence in its strength. All of contemporary cryptography depends on these ideas. Indeed, you yourself probably depend on these ideas. The RC4 and RSA encryption algorithms that secure credit-card transactions in your Web browser, for example, have benefited from public knowledge and refinement by the scientific community for years. The popular DES encryption algorithm saw successful brute-force attack by research teams in 1997 and

1998, illuminating its practical security level for the computer science community. By extension, openness about the design of widely fielded data-security systems—not just cryptographic ones—plays a pivotal role in computer security. That is why public advisories regarding operating system weaknesses and viruses, such as those issued by the CERT coordination center, are vital to computer security today.

For these reasons, the data-security community is often critical of "security by obscurity," i.e., securing systems by hoping that no one will probe them sufficiently. You may be happy to leave the key to your front door under the doormat, but you probably don't want industrial security systems doing the equivalent.

Our research on the DST exemplifies Kerckhoffs' principle and communicates it to a new audience, the RFID community. The DST encryption algorithm is present in devices distributed around the globe and owned by millions of users. There can be no reasonable expectation of "security through obscurity" around it. Someone somewhere was bound to unravel it. Hackers can independently do what we as researchers have done (if they haven't already). We believe that consumers and users of the DST need to be aware of its true level of security.

Openness in security design and disclosure of vulnerabilities has become largely mainstream doctrine in the wired world. They need to see translation and reinterpretation in the wireless world, where security risks are often greater. As we have explained, a thief can potentially duplicate a Speedpass without ever touching it. And he or she can do so without leaving any kind of audit trail—a rarity in the wired world. Moreover, while software can be speedily patched, a hardware device cannot. Thus the RFID transponder in an ignition key needs security that will last for the lifetime of an automobile, perhaps 15 years. This principle holds for many RFID systems. They are often more vulnerable and harder to modify than their wired equivalents, and consequently require

even stronger security.

Johns Hopkins and RSA Laboratories did not create a new vulnerability in Texas Instruments' Digital Signature Transponder. We merely brought an existing flaw to light. One does not weaken a highway bridge by drawing attention to a rust-eaten undergirding—nor does one jeopardize drivers by doing so.

On the contrary, calling attention to problems is the surest way to fix them. The sooner, the better. This is our hope in raising awareness about the weakness in the TI system: To promote consumer knowledge as well as industry education and accountability. For their evolution and ever-improving safety, consumer products—like automobiles—have depended on consumer reports, safety assessments and general communal vigilance. RFID products should too.

The value of openness, of course, has its limits. Prior to disclosing our findings to the public, we honored an ethical obligation to inform Texas Instruments of the weakness we had discovered. We invited the company's comments and questions about our work. We waited, moreover, until we were certain that no private remedy could be deployed in advance of public notice of the weakness. When we did publish our results, we chose to withhold certain details of the DST cipher. We disclosed what we felt was sufficient to offer scientific illumination, but not enough to facilitate abuse. Our technical paper omits a "recipe" for the DST encryption algorithm. (Many colleagues believe that we should divulge such a "recipe" to the scientific community for analysis. We may do so later when the industry has had time to absorb the implications.)

Texas Instruments is to be commended for introducing cryptography into its DST tags. Despite its problems, its DST system in fact offers a higher level of security than many other commercial RFID devices. We trust that TI will not just

address the problem we have identified, but aim at continuous evolution of security in its devices.

Our research on the DST is by no means an indictment of RFID security in general. We insist that good security is attainable in RFID systems. Indeed, we stress that security deserves to be seen not as an impediment to RFID deployment, but as a facilitator. Secure systems pay for themselves in ease of use and maintenance—and as insurance against calamities.

It is incumbent upon the RFID community to embrace good security principles now—especially vigorous scientific oversight and industry accountability. We should tackle security problems in the RFID arena *before* they become costly, pervasive and pernicious. In doing so, we can hope to avoid the historical mistakes of the wired world and the future perils of an automated world, and quickly smooth the way for RFID to deliver its very high pitch of promise.

A technical paper and other details on the DST project are available for interested readers at www.rfidanalysis.org. This project is just one in a broad, ongoing program of research into RFID privacy and security at Johns Hopkins and RSA Laboratories.

Ari Juels is the principal research scientist and manager of applied research at RSA Laboratories, the research center of RSA Security. His primary research area is data security, with emphases on authentication, biometrics, electronic voting and financial cryptography. To comment on this article, click on the link below.

- ADVERTISE
- CONTACT

FOLLOW US ON

- Follow
- Follow
- Follow
- Follow

ABOUTCAREERSAUTHORIZED SERVICE PROVIDERSYour Privacy ChoicesTERMS OF USEPRIVACY POLICY