The Outer Limits of RFID Security

Ari Juels

RSA Laboratories
Bedford, MA 01730, USA
ajuels@rsasecurity.com

It is tempting to regard RFID security and privacy primarily as questions of cryptographic protocol design. We would like RFID tags to authenticate themselves in a trustworthy manner. We would also like them to protect the identities and personal data of their bearers. We might imagine that our aims should be to squeeze cryptographic primitives down to the constrained environments of RFID tags and to craft protocols that scale up to populations of millions or billions of devices. By adapting existing tools, it might seem that we can readily fulfill the majority of our needs with some more circuitry in tags, a greater abundance of cycles and memory on application servers, and a bit of clever economizing.

Ultimately, however, the issues of RFID security and privacy extend well beyond the confines of this neat, conventional picture. At the outer limits of research on RFID security today is a great variety of topics, including:

- *Side channels:* The best logical-layer protocols are in vain if RFID tags are insecure at other layers. For example, as a surprising challenge to RFID privacy, recent research has shown that "dead" tags may be detectable and even classifiable based on their RF signatures. What is the impact (negative and positive) of such information channels?
- *Covert channels:* RFID tags may be viewed loosely as sensors. They will increasingly act as such, gathering and transmitting data about their ambient environment. What can we say about the risk that they are covertly transmitting more?
- *Human-implantable RFID:* Surgically implantable RFID tags for medical identification and access control are commercially available today. What are the security and privacy implications of such "prosthetic biometrics?"
- *Ramping up security:* Moore's Law—or pressing security needs—may someday democratize cryptography among RFID devices. This is likely to happen when there exists a legacy RFID infrastructure with limited support for security. How can we accommodate growing RFID-security needs more gracefully than we have for the Internet?
- *Cooperative architectures:* A spectrum of devices with varying capabilities will operate in the RFID domain. How can high-resource devices assist low-resource ones through simulation and audit?

It is evident that RFID devices are not mere propagators of information, but devices whose physical characteristics and operating environments give rise to rich medley of security challenges and tools.

L. Goubin and M. Matsui (Eds.): CHES 2006, LNCS 4249, p. 231, 2006.