RFID Viruses and Security Threats

By Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum

Monday, 20 March 2006 08:27 EST

RFID systems as a whole are often treated with suspicion, but the input data received from individual RFID tags is implicitly trusted. RFID attacks are currently conceive as properly formatted but fake RFID data; however no one expects an RFID tag to send a SQL injection attack or a buffer overflow.

RFID malware is a Pandora's box that has been gathering dust in the corner of our "smart" warehouses and homes. While the idea of RFID viruses has surely crossed people's minds, the desire to see RFID technology succeed has suppressed any serious consideration of the concept. Furthermore, RFID exploits have not yet appeared "in the wild" so people conveniently figure that the power constraints faced by RFID tags make RFID installations invulnerable to such attacks.

This paper is meant to serve as a warning that data from RFID tags can be used to exploit back-end software systems. RFID middleware writers must therefore build appropriate checks, to prevent RFID middleware from suffering all of the well-known vulnerabilities experienced by the Internet.

Furthermore, as a proof of concept, this paper presents the first self-replicating RFID virus. This virus uses RFID tags as a vector to compromise backend RFID middleware systems, via a SQL injection attack.

Download