'Fingerprinting' RFID Tags: Researchers Develop Anti-Counterfeiting Technology

November 19 2009

(PhysOrg.com) -- Engineering researchers at the University of Arkansas have developed a unique and robust method to prevent cloning of passive radio frequency identification tags. The technology, based on one or more unique physical attributes of individual tags rather than information stored on them, will prevent the production of counterfeit tags and thus greatly enhance both security and privacy for government agencies, businesses and consumers.

“RFID tags embedded in objects will become the standard way to identify objects and link them to the cyberworld,” said Dale R. Thompson, associate professor of computer science and computer engineering. “However, it is easy to clone an RFID tag by copying the contents of its memory and applying them to a new, counterfeit tag, which can then be attached to a counterfeit product - or person, in the case of these new e-passports. What we’ve developed is an electronic fingerprinting system to prevent this from happening.”

Thompson and Jia Di, associate professor of computer science and computer engineering and co-principal investigator on the project, refer to the system as a fingerprint because they discovered that individual tags are unique, not because of the data or memory they contain, but because of radio-frequency and manufacturing differences.

As Thompson mentioned, RFID tags are becoming more prevalent. They have been used in a wide range of applications, including government processes, industry and manufacturing, supply-chain operations,

payment and administration systems, and especially retail.

“In spite of this wide deployment, security and privacy issues have to be addressed to make it a dependable technology,” Thompson said.

A passive RFID tag harvests its power from an RFID reader, which sends radio frequency signals to the tag. The tag, which consists of a microchip connected to a radio antenna, modulates the signal and communicates back to the reader. Working with an Avery Dennison M4E testcube designed for determining the best placement of RFID tags on packages, Thompson, Di and students in the Security, Network, Analysis and Privacy Lab measured tags’ minimum power response at multiple frequencies.

The researchers did this using an algorithm that repeatedly sent reader-to-tag signals starting at a low power value and increasing the power until the tag responded. Radio frequencies ranged from 903 to 927 megahertz and increased by increments of 2.4 megahertz. These measurements revealed that each tag had a unique minimum power response at multiple radio frequencies. Moreover, power responses were significantly different for same-model tags.

“Repeatedly, our experiments demonstrated that the minimum power response at multiple frequencies is unique for each tag,” Thompson said. “These different responses are just one of several unique physical characteristics that allowed us to create an electronic fingerprint to identify the tag with high probability and to detect counterfeit tags.”

Like other electronics equipment, cost and size have driven development of RFID technology. This emphasis means that most tags have limited computational capabilities; they do not include conventional encryption algorithms and security protocols to prevent cloning and counterfeiting. The electronic fingerprinting system addresses these concerns without

increasing the cost or physically modifying the tag, Thompson said. The method can be used along with other security protocols for identification and authentication because it is independent of the computational capabilities and resources of the tag.

Thompson and Di are also developing network circuits that are resistant to side-channel attacks against readers and tags.

Provided by University of Arkansas (news : web)