Hack-proofing RFID-equipped personal devices

December 27 2016, by Sim Shuzhen

Radio-frequency identification (RFID) tags have become almost ubiquitous – look carefully, and you'll notice them in passports, credit cards, library books, office access passes, and even pet cats.

The technology, which allows fast, automated identification of physical objects, is also a staple for many industries – factories and warehouses use it to track inventory and manage supply chains, pharmaceutical companies deploy it to track drugs, and courier services use it to tag deliveries. But what would happen if RFID technology were compromised?

"A security breach in RFID applications would leak valuable information about physical objects to unauthorised parties," says Li Yingjiu, Associate Professor at the Singapore Management University (SMU) School of Information Systems. Professor Li, an expert on RFID security and privacy, as well as other aspects of mobile security, is endeavouring to build better safeguards into the technology.

Improving RFID security protocols

Because RFID tags work by broadcasting information to electronic RFID readers, security breaches can occur if hackers eavesdrop on this conversation, and manage to gain access to or tamper with information.

The consequences of such an attack could be serious, says Professor Li.

"In the context of supply chain management, for example, this means industrial espionage may obtain sensitive information about inventory levels, trading volumes, trading partners, and even business plans," he explains.

To protect communications between tags and readers, Professor Li and his team are designing and testing new RFID protocols with enhanced security features, such as those in 2010 study, "Achieving high security and efficiency in RFID-tagged supply chains", published in the International Journal of Applied Cryptography. These strategies include making the protocol's output unpredictable, making two tags indistinguishable to the hacker, and preventing hackers from obtaining useful information even if they manage to interact with the tags.

In addition, there are many instances where sharing of RFID information – between suppliers and retailers, for example, or between various components of an Internet of Things – would have obvious benefits, says Professor Li. But without appropriate security controls, however, most companies would be reluctant to make valuable data readily available. To address this problem, Professor Li's team is also designing improved access control mechanisms that protect RFID information when it is shared on the internet.

Stress-testing smartphone security

We carry RFID around in our pockets – mobile payment systems such as Apple Pay and Google Wallet use a specialised form of the technology. Given our increasing reliance on smartphones for everyday functions – banking transactions and contactless payments, for example – mobile security has become an area of critical importance.

Professor Li is particularly adept at sniffing out potential vulnerabilities in smartphone operating systems. In 2012, his team identified a number

of attacks which hackers could use to target Apple iPhones. The code to launch these attacks – which included passcode cracking, interference with or control of telephony functionality, and sending tweets without the user's permission – could be embedded within third-party apps that were available in the iTunes store.

The team reported their findings to Apple's security team, and the company plugged these loopholes when its new operating system was released the following year. They also wrote up their findings in the 2013 article, "Launching generic attacks on iOS with approved third-party applications", which was published in the Proceedings of Applied Cryptography and Network Security: 11th International Conference, ACNS 2013.

More recently, Professor Li's team also reported Android framework vulnerabilities and potential attacks to Google, which went on to acknowledge the SMU group's findings in its security bulletins. The team has also developed a set of smartphone vulnerability analysis tools in collaboration with Chinese telco Huawei; two patents arising from this project were evaluated as "potentially high value" by the company.

"We see the opportunities to work with industry in this area because it is important for smartphone manufacturers to make their products better in terms of security," says Professor Li.

Bridging the gap between academia and industry

There are many situations in which data owners may not fully trust service providers – when we store data in cloud services, or exchange it over secure messaging systems, for example. In collaboration with Professor Robert Deng, also at the SMU School of Information Systems, Professor Li is now working to develop new solutions for attribute-based encryption – a form of encryption that gives data owners better control

over who can access their data.

The pair's solutions, says Professor Li, which they shared in an article, "Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption", for ASIA CCS'14: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, have many applications in real-world scenarios.

Despite its promise, however, getting this research out into the market is still proving to be a challenge. "While we can prove in theory and using proof-of-concept prototypes that our solution is better than the existing solutions in terms of security and flexibility, it is still difficult to convince the industry to adopt it without developing it into a final product," Professor Li points out.

Indeed, one of the data security field's biggest challenges is the widening gap between academia and industry, he says. While people in industry are familiar with the market, they are mostly isolated from cutting-edge research; conversely, academics pay too much attention to research and not enough to understanding the market.

"The future of data security, in my vision, is how to narrow the gap and bridge the two communities, which have completely different incentives and evaluation criteria," says Professor Li. On his part, he adds, he is keen to explore ways to increase the industrial impact of his research.

Provided by Singapore Management University