

## RFID Security Threats: Your Cat is Probably Safe ... for Now

**Adi Tedjasaputra**

RFIDAsia Founder

The recent paper titled "Is Your Cat Infected with a Computer Virus?", published during the Pervasive Computing and Communications Conference 2006 in Italy warns that data from RFID tags can be used to exploit back-end software systems.

One day later, the president of AIM Global, the Association for Automatic Identification and Mobility, published an article on his web site that mitigates this issue and criticises the methodology of the particular research in the paper.

Recognising the two extremely different opinions expressed by two respected representatives from the Computer Science community and the RFID community, it is particularly important for both community members to really understand the essential issues beyond the issue of RFID virus.

### Analysis

The paper published by the researchers from Vrije Universiteit Amsterdam has done a good job summarising the common security and privacy threats, i.e. Sniffing, Tracking, Spoofing, Replay Attacks and Denial of Service and demonstrating the possible malware threat for an RFID system by exploiting several possible security holes.

With the increasing number of IT vendors that jump on the RFID bandwagon and the fiercer competition among the vendors that requires shorter middlewares' time-to-market, there is a realistic chance that the existing RFID middlewares available in the market are delivered with security holes, independent from the critic uttered by the AIM Global's president that the demonstration system mentioned in the paper was intentionally built with a weakness. Instead of pointing fingers to each other, there is a need for verification from security experts to objectively evaluate the current state of RFID middlewares' susceptibility to malware threats.

On the other hand, some organisations that have implemented some RFID system can still currently sleep without worries, because any exploit using the methodology presented in the paper would require a combination of thorough knowledge in malware

production and RFID system design, one or more security holes that match the malware exploit, an opportunity to infect a tag with a proper (relatively expensive) equipment and most important of all an ill intention to sabotage. It is safer to assume that the potential threats coming from internal organisation is more prominent than the external ones.

### Reflection

When I explained the possible security threats of using on-line banking facilities to some people who were not aware of the risks in using an on-line banking system, they usually became alerted with the fact that their asset has been vulnerable to various security threats the second they connect to the Internet.

Explaining some security measures that they could perform, I usually added a joke for the ultimate on-line banking security measure: Unplug all the cables from your computer, turn off all your electronic devices and remove any power source elements from your electronic devices for 100% security guarantee.

In reality, there is no 100% security guarantee in this networked world. When you become part of a "network" voluntarily or involuntarily, there is always a chance that your security is compromised. A sensible action you can take is to assess your security state continuously, take several appropriate security measures and prepare for some recovery plans that may arise from any security breach.

### End-Note

Your cat may be safe for now, because the current RFID animal tags usually have the Read-only (RO) memory attribute and immune from any change of data. However, the recent natural threats from mad cow disease and avian flu have sparked some interests in using RFID animal sensory tags that can integrate some sensing devices to detect, monitor, measure, record and transmit various environmental and host parameters, such as temperature. A future scenario of recording more data into a Read-Write (RW) animal sensory tag is no longer far-fetched. Your cat may no longer be safe in this future scenario.