Royal Holloway University of London

Kevin Eagles
supervised by Dr. K Markantonakis

Smart Card Centre Royal Holloway

"A comparative analysis of common threats, vulnerabilities, attacks and countermeasures within smart card and wireless sensor network node technologies."

PROBLEM AREA

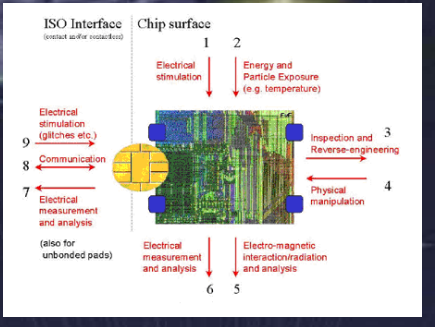
An assessment of the similarities and differences of commonly perceived security threats to Smart Card (both contact and contactless) and Wireless Sensor Network Node technologies - two distinctive technologies that seem to share a close resemblance to one another.

The main aim, is to establish whether there can be 'Security Lessons Learned' from the world of Smart Cards that may be applied to Wireless Sensor Network Nodes and reciprocally from the more fledgling Wireless Sensor Network Node technology to the world of Smart Cards.

The following Objectives were established by the author to progress this research: -

OBJECTIVE 1: Determine if there are any security threats, vulnerabilities, attacks and countermeasures that have been established for Smart Card Technologies (both contact and contactless) that can be directly and/or indirectly applied to Wireless Sensor Network Node Technologies.

OBJECTIVE 2: Determine if there are any existing or emergent security threats, vulnerabilities, attacks and countermeasures that have been established for Wireless Sensor Network Node Technologies that can be directly and/or indirectly applied to Smart Card Technologies.



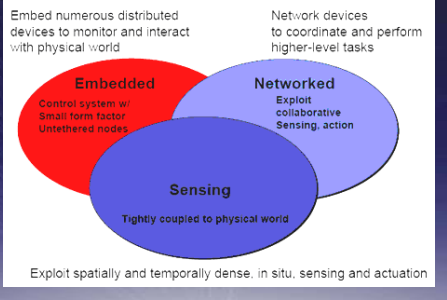
CAPABILITY DEMONSTRATION

A smart card is a secure token which can store, utilise and protect credentials. There are many multi-functional and multi-application cards available today with capabilities such as key generation and with multi-application enable multi-purpose use. Contactless cards have the capability of harnessing Radio Frequency as a communications bearer, bringing its use in the wireless world.

Wireless Sensor Network Nodes or Motes are low-cost, low-power, multifunctional, miniature sensor devices. They collaborate among themselves to establish a Wireless Sensor Network providing access to information anytime, anywhere by collecting, processing, analysing and disseminating data via wireless communications. Thus, the network actively participates in creating a smart environment.

To investigate the security issues with these technologies it was necessary to establish parameters. The principle focus of this project was not one of Risk Analysis but Threat Analysis. The author created a Threat, Vulnerability, Attack and Countermeasure Matrix in which to catalogue common threats to the respective technologies. Once these threats were catalogued, a Comparative Threat Analysis Assessment was undertaken to determine any commonalities.

Both technologies share many common threats at the Chip level and although there are sufficiently high levels of tamper resistance in many smart cards today, many Motes lack any form of tamper resistance. There is partial applicability of communication layer threats to contactless smart cards mapping across to motes and vice versa.



CONCLUSIONS & FURTHER WORK

This research has concluded that it is necessary to apply tamper resistance to mote chips to make them more secure. Also, consideration should be given to writing Protection Profiles for mote chips and operating systems and consider pursuing a route of formally internationally recognised evaluation, such as Common Criteria.

Recommendations are to consider threats to mobile cell phone technology and how they may also have an applicability to motes