Talk on "Credential Security and Physical Access Control System" on 9 July 2016

by Dr Siow Chun Lim, Grad. IEM

Dr Siow Chun Lim, Grad. IEM is currently the Associate Editor of Journal of Engineering Science and Technology and is also an active reviewer for several conferences and journals.

Token of appreciation

Participants during the course

On 9th July 2016, Mr. Tai Keang Seng delivered the talk on "Credential Security and Physical Access Control System" at Wisma IEM. The awareness on credential security is still not good enough in Malaysia hence the need of this talk to outline the general information on credential security and physical access control system.

Integrated Security Management System (ISMS) is a security system which may be of the form of perimeter detection, barrier gate vehicle access, basement help point, lift integration, visitor registration, access biometrics, ICT integration, intrusion sensor integration, CCTV & Fire integration or integrated control room. There are three main components of ISMS which includes input, process and output. Sensor and camera access reader are categorized as the input, host SW controller is part of the process while locking device and speaker are considered as the output.

ISMS have to perform several functions which include:

1. Detection (done by using exterior/interior sensors, video camera with Intelligent Video Analysis (IVA))
   Detection is defined as the discovery of intrude action followed by an assessment of the alarm to verify whether there is an actual intrusion
2. Deterrence (done using signage, security lightning, electronic security system)
   Deterrence is done to create an environment that discourages trespassers
3. Delay (done using access control)
4. Deny (done using access control) which is an action to be coordinated with the Public Announcement (PA) system
5. Response (Public Announcement system, CCTV, intrusion alarm)

An ISMS typically comprises of fire alarm systems, intrusion detection system, video surveillance systems, access control systems, PA and emergency evacuation systems, 3rd party integration.

Radio frequency identification (RFID) is a method for uniquely identifying an object using a tag or module. Every card has a card serial number. When it nears the reader, the reader will emit a radio frequency wave and power up the card. The card will generate a random number and send back to reader together with the card serial number. The reader will create a diversified key and generate another set of random number and through certain algorithm will perform mutual authentication and the card will generate a response to authenticate it.

There are mainly three referred bands of frequency namely Low Frequency (approximately 125kHz), High Frequency (approximately 13.56MHz) and Ultra High Frequency (approximately 900MHz). The advantage of High Frequency RFID includes extra memory storage, greater functionality, higher level of security, faster communication rate and encryption. On the other hand, the advantages of Ultra High Frequency (UHF) RFID includes allowance for much longer read ranges, without the need for active (powered) credentials, and is often used in asset or inventory tracking and vehicle access. It has also been used for a number of years in access control system. UHF is region dependent and standardization is always a challenge.

Card and credential are always confused with each other. A credential is something that is generated by a trusted authority and identifies the bearer. A PACS credential is digital data that is typically stored in a device, be it a card, key forb or mobile phone. Invariably, the credential is protected by one or more cryptographic methods. Some cards will also have contact chips. Credential data predominantly resides on plastic cards.

Card technologies started with the development of Magnetic Stripe and Prox card. Existing card technologies include contact smart card which has an integrated circuit (memory, stored logic or microprocessor) with electrical contacts embedded in a plastic card using 13.56 MHz carrier. This technology is inconvenient for access control as compared to Prox and Contactless Smart Cards as

insertion reader tends to being subjected to vandalism and weather effects. However it generally supports read and write function, is ISO standardized and has higher security level. A Prox technology on the other hand operates at 125kHz with read-only function and is not ISO standardized.

ISO standardization helps to drive costs down, encourage broad supplier support and customer acceptance, facilitates interoperability between vendors and applications and eliminate obsolence.

Expansion of technologies and applications means more smart card technologies, introduction of smart phones and converged applications. Increase in security means multi-layered protection and breach resistant are increasingly needed. Smart card with long crypto key is generally more secure. The demand for high security and long reading distance would continue to grow.

It is highly recommended to consider hardware cost (readers and cards), setup costs (readers and cards), data management costs, lifetime cost when selecting RFID technology.