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

Kevin Eagles

HEMIS Number: 100256253

Project Supervisor: Dr. Kostas Markantonakis

Chair Project Committee: Professor Peter Wild

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature: Date: 8th September 2006

Word count: 19,646 (Excl. Appendices)

ROYAL HOLLOWAY,

UNIVERSITY OF LONDON

ABSTRACT

A dissertation presented on assessing the similarities and differences of commonly perceived security threats to Smart Card (both contact and contactless) and Wireless Sensor Network Node technologies. A Threat Analysis was undertaken to identify common threats, vulnerabilities, attacks and countermeasures for the technologies at reference with a subsequent Comparative Threat Analysis Assessment to determine any direct and/or indirect commonality or applicability of the security threats from one technology type relative to the other.

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

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKLOWLEDGMENTS

The author would like to give thanks to Dr. Phil Levis (Stanford) and Mr. Chris Karlof (Berkeley) for offering up their time to give pointers on this course of study, and to Dr. D. K. Arvind (Edinburgh) for a discussion that led to further pointers.

Special thanks go to Mr. Harry Cassar (BP) and Dr. Phil Buonadonna (Arch Rock) for very lengthy and helpful discussions that helped the author understand wireless sensor networks in greater depth and firm up areas of interest for this dissertation.

The author would also like to express his gratitude to his Project Supervisor, Dr. Kostas Markantonakis, who has helpfully encouraged the author in the evolution and development of this project.

EXECUTIVE SUMMARY

Ross Anderson articulately states in the Foreword to Frank Stajano's book, "*Security for Ubiquitous Computing"* [1]:-

"Security in the twenty-first century is going to be a much more complex business. It will include a lot more technical issues and will touch the everyday world at many more points. Developers and policy people are going to have to learn to think in new ways."

This dissertation has tried to hold true to this philosophy.

A smart card is a secure token which can store, utilise and protect credentials.

Wireless Sensor Network Nodes or Motes are low-cost, low-power, multifunctional, miniature sensor devices. They collaborate to form Wireless Sensor Networks.

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

The following Objectives were established 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.

A Threat Analysis framework was created to catalogue common security threats within each of the technologies – this was in the

form of a Threat, Vulnerability, Attacker and Countermeasure (TVAC) table; subsequent to this a comparative assessment was undertaken to determine commonalities.

The findings from this study imply that common threats on smart cards that are shared with Wireless Sensor Network Nodes are within the Integrated Circuit space; effective countermeasures to these threats that are currently applied to smart cards may be able to be possibly modified and adapted to become effective countermeasures for Wireless Sensor Network Nodes.

Common threats on Wireless Sensor Network Nodes that are shared with smart cards tend to be in the Radio Frequency space that relate to contactless smart cards, but they only share a slight relation.

This research has concluded that it is necessary to apply tamper resistance to Wireless Sensor Network Node chips to make them more secure; consideration should also be given to writing Protection Profiles for these chips and their operating systems and perhaps pursue a route of formally internationally recognised evaluation, such as Common Criteria. This has helped mature smart cards and may do the same for Wireless Sensor Network Nodes

Most attacks on smart cards and Wireless Sensor Network Nodes still require high levels of expertise and access to specialist equipment, which makes them unlikely to move into the realm of the 'script-kiddie' for some time yet.

Recommendations

i. The author feels that there might be similarities to explore with threats and countermeasures within the functioning of Mobile Cell Phone compared against Wireless Sensor Network Nodes. Also, could SIMs be used within some Wireless Sensor Network Nodes out of interest too?

ii. An assessment of the applicability of Global Platform and its Card Manager, Java Card Runtime Environment (JCRE) and various existing smart card APIs compared

to Wireless Sensor Network Nodes may prove of interest.

iii. There might also be scope to explore network mapping tools such as those used in the TCP/IP world like Eracent Network Probe (ENP), to see if they can be adapted to work in the Wireless Sensor Network Node world to produce a similar mapping capability for Wireless Sensor Networks. The same can be said of things like SNMP, and there may also be some overlap with projects like AVISPA.

iv. The exploration of Attribute Certificates [27] and/or Kerberos tickets for Authentication requirements that may be applied to both smart cards and Wireless Sensor Network Nodes may produce some interesting areas of study.

v. The author would be interested to develop an authentication and routing protocol which he has labelled KAFKA (Know Allies & Family, Know Adversaries) to suit the adaptive nature of Wireless Sensor Networks.

1. INTRODUCTION

1.1 Project Background

A little over a year ago, the author was involved with research and planning for a Ministry of Defence (MOD) investigation into a smart card implementation programme, inspired by the US Department of Defense Common Access Card programme. A substantial part of this MOD research related to aspects of security within smart cards. Through this work the author became actively involved in the CESG Smart Card Security User Group and HMG e-GIF Smart Card Forums from 2003 to 2005.

Being a technologist, the author is interested in cutting edge technology and through trade journals read articles about 'smartdust' (see 1.2.3 for definition). Interest in smartdust led the author to Wireless Sensor Networks, Motes and Ubiquitous computing – all of these areas being inter-related to some degree.

Initially this project was going to focus solely on wireless sensor networks, investigating attacks and countermeasures within this type of technology. On reflection, it became apparent that this topic was too vast for an MSc dissertation.

Upon deliberation with the Project Supervisor, Dr. Kostas Markantonakis, it became apparent that smart cards and wireless sensor network devices seemed to share some similarities in their designs and hence possibly could both have common susceptibilities to the same kinds of threats and attacks. This in turn became the basis for this dissertation.

1.2 High Level Definitions of the Technology Discussed in this Project

Section 3 (Smart Cards) and Section 4 (Wireless Sensor Network Nodes) of this dissertation contain detailed descriptions of both technologies respectively.

However, it is important from the outset that the reader is able to have a high level definitive understanding of the technologies under discussion, and this is given below: -

1.2.1 What is a Smart Card?

There are many different types of smart card in the market place and hereafter the term Smart Card Technologies will be used for either and/or both contact and contactless smart cards. Where any distinction is required, it will be made. This dissertation will not focus on any particular vendors' products, seeking instead a wider applicability to smart cards at large.

"Smart card […] means an integrated circuit containing a microprocessor, volatile and non-volatile memory, and associated software, packaged and embedded in a carrier. The integrated circuit is a single chip incorporating CPU and memory which may include RAM, ROM, and/or programmable non-volatile memory (typically EEPROM or Flash memory). The carrier is typically made of plastic and usually conforms to ISO 7810 and 7813 – Identification Cards, but may have the smaller size of a GSM (global system for mobile communications) subscriber identification module (SIM). The chip is embedded in a module which provides the capability for standardised connection to systems separate from the chip (typically through contact in accordance with ISO 7816 or contactless in accordance with ISO 14443)." [2]

1.2.2 What is Radio Frequency Identification (RFID)?

This definition is included, because contactless smart cards utilise RFID for their communications requirements and in some cases their power supply.

"RFID refers to procedures to automatically identify objects using radio waves […] each RFID system is defined by the following three features:

1. *Electronic identification […]*

2. *Contactless data transmission […]*

3. *Transmit when requested (on call) […]*

• *The transponder – also known as a tag – acts as the actual data carrier. […] Basically the transponder consists of an integrated circuit and a radio-frequency module.*

• *The reading unit […] reads data from the transponder and in some cases instructs the transponder to store further data."* [3]

1.2.3 What is a Wireless Sensor Network Node?

In many published works on Wireless Sensor Networks, it is very common to see the term 'Mote' used. This term is often interchangeable with the notion of a sensor node or wireless network node; however, the term 'Mote' has a specific meaning that shall be covered in Section 4. Smartdust is a mote device that is only a few millimetres in size.

For the purposes of this dissertation the term Wireless Sensor Network Node (hereafter referred to interchangeably as WSN Nodes) shall refer to a device that consists of an integrated circuit with a microprocessor and memory which has a data link to a sensor and is able to function as an element within a network, passing data onto other devices utilising wireless technology as the communications bearer.

"We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general-purpose computing elements. Sensor networks may consist of hundreds or thousands of low-power, low-cost nodes, possibly mobile but more likely at fixed locations, deployed en masse to monitor and affect the environment." [4]

"A wireless sensor network is a collection of sensor nodes, tiny devices, usually battery powered, that acts as nodes in a larger network." [5]

1.3 Project Aim

The overall aim of this project is to assess, within a security context, the similarities and differences between 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 WSN Nodes and reciprocally from the more fledgling WSN Node technology to the world of Smart Cards.

1.4 Project Objectives

The following Objectives have been 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.

1.5 Project Approach

The scope of this project is potentially vast and to make it both manageable and hopefully a worthwhile piece of research it has been necessary to conduct a strict approach due to the risks of 'scope creep'. In this vain, the author has endeavoured to initially determine and subsequently focus on common principal threats, vulnerabilities, attacks and countermeasures only.

To meet the objectives in 1.4, the author has devised a threat analysis framework and methodology to establish, record, analyse and assess common actual and/or perceived threats to Smart Cards and where possible map these threats to comparable areas within WSN Nodes and vice versa for reciprocity.

In addition, the author has conducted many months of intense research refreshing his knowledge on smart cards and learning about Wireless Sensor Networks from scratch – this latter piece of research was extremely difficult due to the lack of most people approached (both academic and commercial at the cutting edge of Wireless Sensornet development) to share their thoughts or views on this technology. Those that did offer guidance are listed in the Acknowledgement section of this dissertation.

The following areas are covered in subsequent sections of this dissertation: -

- Section 2 - Evolution of Computing Technologies
- Section 3 - Smart Cards (detailed description)
- Section 4 - Wireless Sensor Network Nodes (detailed description)
- Section 5 - Threat Analysis Methodology
- Section 6 - Threat Analysis Assessments and Comparisons
- Section 7- Conclusion and Recommendations

2. EVOLTION OF COMPUTING TECHNIOLOGIES

2.1 Section Background

The purpose of this section is to summarise the historical development and evolution of computing technologies, to determine and contextualise how we have arrived at the existence of miniature computing devices such as Smart Cards and WSN Node devices.

This summary is not definitive, it is meant to give a snapshot of what the author perceives to be significant evolutionary milestones that have shaped today's technology. Upon researching this section, the author found many different views on the number of significant computer generations - varying from three through to six. In the author's judgment, there are five significant computing technology eras, as follows: -

2.2 First Generation - c1940-c1955: Vacuum Tubes

In 1946, ENIAC (Electronic Numerical Integrator & Computer) was unveiled to the world in the USA. Although preceded by a few other 'computers' (e.g. 1944 Colossus Computer - UK), ENIAC is widely regarded as the first modern computer machine because it was reprogrammable and capable of solving a full range of computing problems (it was Turing Complete).

It cost c$500,000, weighed 27 metric tonnes and was staffed by an army of technicians.

Vacuum tubes were unreliable and Input/Output was via punched cards. Computational problems could only be worked upon one at a time and compatibility and interoperability with other machines was not a design or business consideration.

2.3 Second Generation - c1956-c1963: Transistors

The smaller, cheaper and faster transistor replaced vacuum tubes, but Input/Output still undertaken via punched cards.

This era was characterised by Mainframe computing although compatibility and interoperability were still virtually non-existent.

2.4 Third Generation - c1964-c1970: Integrated Circuits

Transistors became miniaturised and were placed on silicon chips, called semiconductors or an integrated circuit (hereafter known as IC). This dramatically increased the speed and efficiency of computers and brought about the "Minicomputer" (although the Mainframe was still very predominant).

Gordon Moore stated that ‘transistor density on an integrated circuit approximately doubles about every two years’ - over time this is known as ‘Moore’s Law’ and is still valid today.

Keyboards and monitors are used to interface with computers via an Operating System.

In the US, the Advanced Research Project Agency (ARPA) was established in 1958. An early ARPA project was to create a common communication medium between large, federally funded computing centres; communications had thus far being conducted on a point-to-point basis. In 1969 ARPANET, the world’s first distributed computer network came into existence and is the ancestor of the Internet.

In 1968, German inventors Jürgen Dethloff and Helmut Grötrupp filed a patent application for an identification card incorporating an IC. In 1970, a similar application was made by Kunitaka Arimura in Japan.

2.5 Fourth Generation - c1971-Present: Microprocessors

Thousands of integrated circuits can now be built onto a single silicon chip and leads to the birth of the microcomputer, the most famous being the IBM Personal Computer (PC). As PCs became more powerful, they were linked to form networks.

Graphical User Interfaces (windows) becomes widely adopted.

Microcontrollers are scaled down microprocessors, "embedded" inside many devices (often consumer products) to aid product control. They are often dedicated to a specific task and program.

TCP/IP becomes the de facto communications protocol for computer networked infrastructures around the world.

Commercial development of cryptographic algorithms occurs, such as DES (later 3-DES), RSA and AES to compensate for security concerns relating to data.

Roland Moreno registered smart card patents in France 1974. This is regarded as a key milestone for smart cards, guiding the semiconductor industry in producing specific ICs for smart cards.

In 1999, Seth Hollar at the University of California Berkeley built the first Radio Frequency (RF) Mote (aka WSN Node). It had an Atmel AT90LS8535 processor, 916 MHz RF transceiver and five sensors (temperature, light, barometric pressure, 2-axis accelerometer and 2-axis magnetometer). Its communication range was about 5 – 30 metres with a data rate of 5Kbps [6].

In 2003, 'smart dust' was designed and built by a team of researchers at University California Berkeley and JHL Labs. It is a WSN node approximately 2mm by 2.5mm, dubbed 'Spec Mote' or 'COTS Mote'. It has 3KB of memory and can communicate over 12 metres indoors with a data rate of 19.2 Kbps [7].

At the time of writing, IBM's Blue Gene/L is the world's fastest computer and has reached 280.6 TFlop/s (teraflops or trillions of calculations per second) [8].

2.6 Fifth Generation – Partial Present - Near Future & Beyond: Artificial Intelligence, Nanotechnology, Quantum Computing and Ubiquitous Computing

Major technological breakthroughs for this era are still under development. The goal is to develop devices that respond to natural language input and are capable of learning and self-organisation.

This era will see further and deeper integration of computing technology into the fabric of society, toward Pervasive, near Ubiquitous and possibly even Ubiquitous Computing; meaning computing technology is literally everywhere or accessible anywhere and possibly perceived as invisible or near invisible by the user.

Nanotechnology and Quantum Computing are likely factors to influence computer manufacturing and operation respectively.

2.7 What does this all mean today?

The evolution of computers has gone hand in glove with the evolution of integrated circuit (IC) technology. We are now enjoying increased processing power at cheaper prices, with more applications available to exploit the range of technologies now widely available and accessible.

Today there are ever more faster, smaller, cheaper computing devices that can be interconnected via private networks or share space on a public network such as the Internet. Wireless technologies have shaped the development of Smart Phones, PDAs and devices such as Blackberry, severing the need for a tangible digital umbilical chord and enabling a global interconnectedness within the palm of your hand.

Miniaturisation and mass production have enabled many people in both the industrialised and newly industrialising nations to carry smart credit/debit cards and/or mobile cell phones with a SIM or USIM.

The author feels it is possible to represent quantity of people as (Pn) and quantity of computers as (Cn), and illustrate that in the first four Computer Generations there were more people than computers, which can be represented as (Pn) > (Cn). As the fourth computer generation moves into the fifth computer generation the author believes that by following the historical trend there will be a reversal to achieve (Cn) > (Pn), more computer devices than people, serving the needs of individuals.

Related to these developments is Bell's Law (Gordon Bell c1972), [9] which covers different 'Computer Classes' that have developed stating a loose correlation of ten year formation dates for these Classes. Main points of this law as follows: -

- The law's key point is that a new computer 'class' occurs approximately every ten years to serve a new set of requirements. This is due to technological advances with ICs, interfaces, networks and coding.

- A well established 'market class' of computers are introduced at a constant price, and experience increasing performance and functionality due to Moore's Law.

- Each new computer class is usually a lower priced class relative to predecessors and is maintained as a quasi-independent industry and market in its own right.

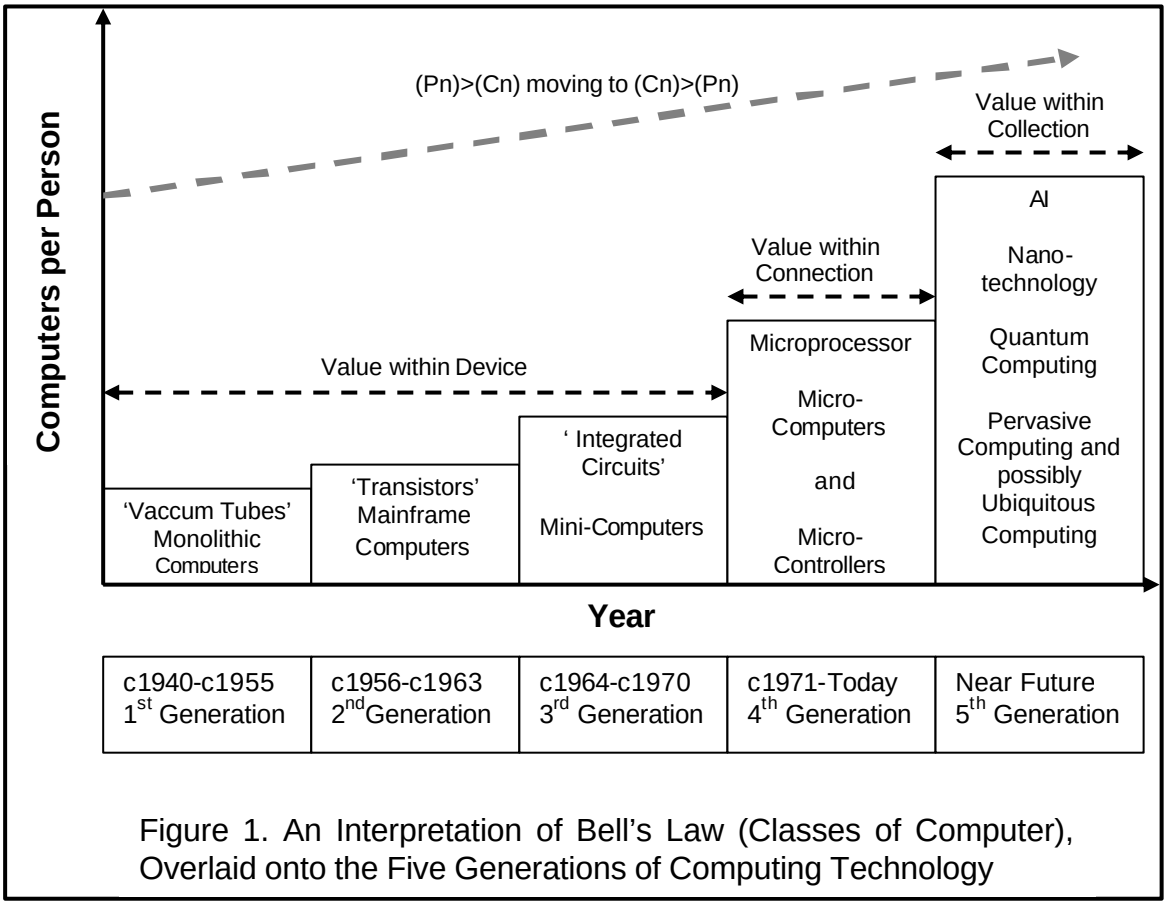

Figure 1. An Interpretation of Bell's Law (Classes of Computer), Overlaid onto the Five Generations of Computing Technology

Figure 1 above illustrates the approximate ten year epochs for Computer Classes which the author has overlaid onto the Five Computer Generations. For this current epoch, Bell feels that the current driver from technology is within 'Collection', indicating the drive for computers to be vast data harvesters – which puts WSN Nodes at the forefront of this class because they harvest data and pass on the information to a base station. Previous value has been and significantly still is within 'Connection' of devices and also within the 'Device' itself.

Bell also draws attention to the fact that with each new class, the amount of computers per person increases. This can be seen in Figure 1 through the increasing height of the bars for each computer generation and is further highlighted by the long grey arrow at the top of the diagram indicating this trend.

One point the author finds quite striking, is that often security seems overlooked and neglected within the historical and technological development of computers.

This is possibly because initially much of the early development that occurs within computer generations is either spearheaded by academic institutions whose drivers are to share information and make their work accessible to others to facilitate progress and security controls might be perceived as a possible hindrance in enabling this. Also, commercial organisations may attempt a dash to market with their product to beat their competitors and hence may compromise certain quality requirements within design and testing to hasten early release. These factors have potentially contributed to vulnerabilities existing within products.

The development of independent commercial cryptographic algorithms has assisted with 'data' and 'system' security, but it mustn't detract from security also being factored into computing products from the outset.

2.8 Section Summary

The following points are the author's views on what has fuelled the evolution of computing technologies: -

1) Historical trends inform us that as a result of continuous innovation, devices become faster, smaller, cheaper and capable of being mass produced.

2) Interconnection and interoperability have been enabled through standardisation (e.g. hardware, software and protocols) thus enabling vendor neutrality.

3) Development of Applications (e.g. word processing and databases) have fuelled widespread adoption creating progressive user dependability on computing technology.

4) Greater accessibility, availability and connectivity – the aim being anyone, anytime and anywhere.

5) Continuous miniaturisation and integration into many specific walks of life assisted by microcontrollers (e.g., PDAs, smart phones and smart cards).

6) Security is often retrofitted as an afterthought, instead of being mandatorily factored into the requirements capture and design phases following a layered approach akin to Defence in Depth. Crime reflects the society we live in – a greater proliferation of computers means a likelihood of more computer related crime. Hacker, spam, virus, worm, trojan, phishing and identity theft are common terms today.

   A lack of preparedness with computer and information security is far from wise in a computer age where a raft of services and information are now digitally available. Coupled with the sheer scale of interconnectivity today, there is the potential to render vast scope to any computer crime that's committed - the amount and range of capability that computers offer legitimate users is mirrored by the scope offered conversely to attackers.

   If (or when) computing is to become ubiquitous it is essential that it is both ubiquity with security and security with ubiquity. As Frank Stajano states [1] "The disappearing computer may disappear so well that users lose not just control but even awareness of what is actually going on."

In the sixty years since ENIAC, there have been startling increases in performance and miniaturisation, with people having wider availability and accessibility to technology – from room sized monoliths that only a few organisations could afford to pocket sized devices with competitive and affordable pricing.

By studying the historical and evolutionary trends of computing technology we can perhaps glimpse future trends and make some informed assumptions considering further developments:

- Computers will become even faster, smaller, cheaper and mass produced.

- Dependability on computing devices will further increase.

- The use of computing devices has already become irrevocable within the functioning of Nations and organisations. Their use will also become irrevocable in some shape or form through the very fabric of every individual's existence within a modern society.

3. SMART CARDS

3.1 Section Background

Smart cards are an example of a hardware token device that can securely store and retrieve credentials and conduct specific functions. Other forms of token are USB tokens with an embedded microprocessor (not to be confused with the commonly available USB data storage fobs) and the Dallas iButton. For reasons of time and scope, this project shall only focus on smart cards.

In the Introduction (Section 1) of this project, there is a fairly high level description of a smart card. This section shall provide a moderately detailed description of smart card technologies and their practical application in today's world.

It is important for the reader to note that in the English speaking world, the term smart card covers a much wider area than is technically accurate. As a term it has been used to describe any 'credit card' sized plastic cards with an embedded chip, generally dependent on an external power supply. This 'wider' perception ends up covering cards that are not 'smart' as such, like the simple and much less sophisticated stored value 'memory cards' (containing simple wired logic and functioning as decrement counters - e.g., phone cards or travel cards).

This dissertation shall treat the term 'smart card' as referring to a credit card sized plastic card with an embedded microprocessor in the form of a microcontroller, making it smart – this definition does not stretch to include 'memory cards'.

The microcontroller was highlighted in Section 2 and it is worth expanding further on its role within smart cards. A microcontroller is often regarded as a highly integrated chip akin to an entire computer on a single chip. It contains a processor (CPU), non-volatile memory for programs (ROM, EEPROM or Flash), volatile memory for Input/Output (RAM), a clock and an Input/Output control unit. It is designed for specific tasks, generally to control a particular system.

The following areas shall be covered in the rest of this section: governing standards, physical characteristics, architecture, operating systems, platforms, applications, management of

smart cards and threats to smart cards; but firstly another history lesson.

3.2 Smart Card History

The use of plastic cards began in the USA with Diners Club issuing the first fully plastic payment card for general use in 1950. All the information stored on the card was held in visual printed form on the card itself, no computing was used.

Over time for reasons of security a magnetic stripe with encoded data was added to the card, as was a PIN (Personal Identification Number).

As we know from Section 2 (Fourth Generation of Computing), Roland Moreno registered smart card patents in France in 1974 – this helped inform the semiconductor industry of what was required to supply integrated circuit technology for smart cards.

Initially, limitations within smart card technology held back progress and widespread adoption; mainly in the areas of capacity, speed, security and interoperability. High production costs were passed onto the customer through high unit costs for the actual cards, further curtailing widespread adoption.

Many users were caught off guard by the requirement for a smart card management system, registering and tracking issuance and managing the card lifecycle.

Early cards also suffered with minimal interoperability capability. Proprietary software limited application development and proprietary designs enabled 'Vendor lock-in'.

Early smart cards had weak security and cards were subject to hacking (e.g., pay per view television services).

These days, performance, interoperability and especially security have improved significantly. Security has been modelled on that found in Hardware Security Modules (HSMs). An HSM is a secure tamper resistant device used for secure key generation and key storage for high assurance cryptographic requirements, such as key generation for a CA within a PKI. HSMs can withstand many forms of attack and if necessary can permanently wipe stored data through a process called zeroising and terminate its functionality, thus having protected any stored

data by rendering both the data and the device unavailable. An example of a commercial HSM is one of the Safenet Luna products, and IBM have a programmable PCI board which is the IBM 4758 PCI Cryptographic Coprocessor - these devices are highly secure and to the author's knowledge have no known forms of successful attack.

Many smart cards now have tamper resistant protection and crypto-coprocessors, and faster chips with greater capacity. As the volume of sales of smart cards has recently and progressively grown in modern times, economies of scale have enabled the purchase price for cards to drop, thus helping to motivate wider adoption of smart cards.

Smart cards started off monolithic, like early mainframe computers, dedicated solely to specific functions and applications, also suffering with interoperability issues. However, smart cards have evolved significantly in their capability and interoperability, now being able to securely store data and run multiple applications efficiently and securely.

3.3 Smart Card Standards

There are a number of standards initiatives to ensure that smart cards from different suppliers are compatible with each other and interoperate with the various reader devices available. Standards fall into two categories, industry specific standards such as those defining the format of the EMV (EuroPay, Mastercard and VISA) card and more generic ISO standards that apply to smart cards in general. This dissertation focuses on the ISO standards, which have wider applicability and are widely adopted.

4.2.1 Contact Smart Cards

- ISO 7816 Contact Cards - Physical electrical connectivity for both power and data via a card reader.

4.2.1 Contactless Smart Cards

- ISO 14443 Proximity Cards - Power and data transferred via inductive coupling over a distance not exceeding 10cm.

- ISO 15693 Vicinity Cards - Power and data transferred via inductive coupling over a distance not exceeding 1.2 metres.

Both Proximity Cards and Vicinity Cards are being treated as the same thing, i.e. a generic contactless smart card, for the purpose of this study. If a distinction is required, it will be made.

4.2.1 Smart Card Interface and Interoperability Standards

- Personal Computer/Smart Card (PC/SC) Workgroup - interoperability in 32 bit Windows environments, the focus is on the card to reader interface with the aim of ensuring that a card from one vendor will function correctly in the reader of another.

- Open Card Framework (OCF) - provides a standard Java interface from a Java Card to a host (terminal or computer) with transparency for application programmers of smart card operating systems, terminals and issuers.

- Global Platform API (formerly Visa Open Platform Terminal API) - targets a much wider range of devices enabling services offered by both PC/SC and Open Card to be utilised in its environment. Smart card and terminal specifications are provided for application loading and management. A Java Card API extension is provided to support downloading of digitally signed applets to a card.

- Government Smart Card Interoperability Specification (GSC-IS) - for US Department of Defense Common Access Card (CAC) and likely to be broadened to cover various US Federal Government smart card initiatives.

It is also important to note that through the internationally recognised evaluation process known as Common Criteria, there are a number of documents required to enable evaluation to proceed. Although not a Standard, a Protection Profile (PP) is an implementation neutral set of security requirements for a specific category of products. Both PPs and products can be evaluated under the Common Criteria scheme and referring to an evaluated PP during a product evaluation accelerates the

evaluation process and helps ensure that all industry standard features are supported.
There are a few Protection Profiles for smart cards, some written specifically for Common Criteria evaluations and others such as the Eurosmart PP which can be used for Common Criteria evaluations but also have a wider scope for assessing security within smart cards.

If a smart card meets the requirements of a PP, a user can have a higher degree of assurance in the use of that card and its ability to meet security requirements compared to a card that does not claim to meet the requirements of a PP.

3.4 Smart Card Hardware

Contact and Contactless cards are separate divisions within smart card technology; however, they may be combined onto a single card.

Dual Interface cards (sometimes referred to as combi-cards) have both contact and contactless interfaces connected to a single chip, transferring data to and from the card. This type of card benefits from being all things to all people in the smart card world, offering users applications in a contact or contactless medium and the need for only one enrolment and personalisation exercise. The drawback of this card, is that from a security perspective there is now an additional interface to the microcontroller which an attacker could try to exploit.

Hybrid cards tend to have two onboard chips, one with a contact interface and the other with a wireless contactless interface for the other chip. The drawback of this type of card, is that you have to undertake two separate personalisation activities and the contact chip can only be read by a card reader as there is no contactless interface to this chip, this causes an extra overhead in time and cost with regard to use.

The interconnection and physical interface between a contact smart card and its host device (generally a PC) is often made via an ISO 7816 card reader.

Both contact and contactless smart cards do not generally have onboard power supplies (e.g., batteries). In the case of a contact

card, the reader allows the smart card to have a source of power enabling it to function and also have a channel to pass data.

Contactless smart cards use an internal inductor to capture some of the incident radio-frequency interrogation signal and uses it to power the card's electronics. A contactless card is read by a host when the close proximity to an antenna completes the transaction. Induction is a magnetic field that produces an electric current in wires passed through the field. It's generally something engineers try to avoid due to the fact it causes interference in standard communications and electronic devices. However, for contactless smart cards induction is harnessed as a useful way to establish power and communications and enables Radio Frequency Identification (RFID).

Active RFID is not that common and uses an internal power source (a battery) to continuously power the device and its Radio Frequency (RF) communication circuitry. It is continuously powered, whether within the reader field or not, and they is normally used when a longer read distance is required.

Passive RFID is very common and relies on RF energy transferred from the reader to the device to power it. Passive RFID tags reflect energy from the reader or receive and temporarily store a small amount of energy from the reader signal in order to generate responses. Passive RFID requires strong RF signals from the reader & the RF signal strength returned from the tag is constrained to very low levels by the limited energy. Passive RFID tags are best used when the tag and reader are close together and are commonly seen as RFID tags attached to merchandise in shops.

Semi-passive RFID uses an internal power source to monitor its own environmental/state conditions, but requires RF energy transferred from a reader similar to passive devices to power a response.

3.4.1 Contact Smart Cards with Microcontrollers

Market sectors for this type of card are: Telecoms (SIM/USIM), ID/Health Cards, Subscription TV, Banking cards (EMV).

They may consist of the following features and specifications: -

- **CPU:** 8Bit, 16Bit or 32Bit (+Crypto processor)
- **Memory:** (ROM /EEPROM/Flash) From 2KB to 2MB
- **Security:** up to Common Criteria EAL 5+
- **Trend:** Memory size increasing, faster performance & multi-applications

3.4.2 Contactless Smart Cards with Microcontrollers

Market sectors for this type of card are: Electronic Ticketing, ID Cards, City Cards, some types of Banking Cards.

They may consist of the following features and specifications: -

- **CPU:** 8Bit, 16Bit (Basic Cryptographic function)
- **Memory:** (ROM/EEPROM/Flash) From 4KB to 64KB
- **Options**: Contact & Contactless I/O or Dual Interface
- **Trend:** Memory size increasing, faster performance & multi-applications

3.5 Smart Card Architectures

A typical smart card microprocessor can be composed of the following elements: a processing unit, security components, Input/Output ports and both volatile and non-volatile memories. This can be depicted in Figure 2 below: -

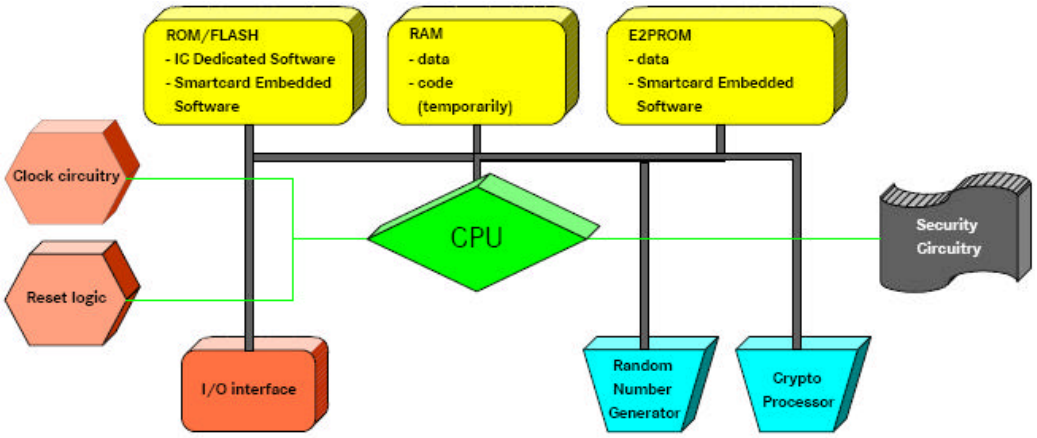

Figure 2 Smart Card Microprocessor Composition [10]

As we can see from Figure 2, a smart card is a mini-computer with a vast amount of functionality, albeit with restrictions due to the amount of space available.

We shall now look further at types of card architecture.

3.5.1 Dedicated Microprocessor Cards (or File System Cards)

This type of smart card has functionality not dissimilar to that found on a PC, this includes a CPU, volatile and non-volatile data storage and an operating system.

Proprietary Operating Systems and Applications are loaded onto the card during the manufacturing stage and generally stored in Read Only Memory (ROM) – they also tend to be written in a low-level processor dependent assembly language. The chip has a small amount of Random Access Memory (RAM) for temporary data storage (the stack) and User data is stored in reusable Electrically Erasable Programmable Read Only Memory (EEPROM) or Flash memory which is seen by many manufacturers as an alternative to EEPROM because it is cheaper but doesn't last as long as EEPROM.

A dedicated hardware co-processor may be included to speed up certain application specific processes (e.g. cryptographic co-processor for key generation or encryption/decryption). Typical uses of this type of card are mobile cell phone Subscriber Identity Module (SIM), banking and Digital Rights Management with subscription TV.

3.5.2 Programmable Microprocessor Cards (Virtual Machine Cards)

These cards have a similar architecture to the dedicated microprocessor cards above and are based on a dedicated smart card operating system which is able to run applications written in a high-level language. It is now possible to utilise the skills of the wider group of Java and C++ programmers to produce applications written in these languages for this type of card. This means that there is wider scope for multi-application development and updates

3.6 Smart Card Operating Systems

Before Multi-application smart cards, there were various smart card operating systems that were proprietary and had constraints in the sense they were very limited and inflexible to work with.

In the sphere of Multi-Application Card Operating Systems (MACOS), there are two vendor neutral Operating Systems that may be used on a wide range of vendors' smart cards. One is MULTOS (Multiple Operating System) and the other was Microsoft's Windows for Smartcards which was subsequently withdrawn from the market place. However, Microsoft has fairly recently brought out a streamlined version of the .NET Framework for smart cards and Embedded Windows NT and Windows CE have had success and both have a small footprint, so Microsoft are not complete strangers to this mini OS space.

MULTOS is an operating system enabling multiple application programs to co-exist independently and securely on a smart card. The applications are isolated by the operating system preventing any inter-application interference.

3.7 Smart Card Platforms

Java Card which is a virtual machine with APIs that plug into any smart card operating system be it a proprietary one, MULTOS or a Microsoft option.

Java Card technology provides a vendor-independent platform for smart cards. Java Card defines a runtime environment on top of the native hardware and smart card operating system. The Java Card runtime environment (JCRE) provides a high-level, standard interface to smart card applications. Security is similar to the web browser and java applet model.

Global Platform which is an operating system independent security function that is portable across any Java Card or Windows for Smartcards. The Card Manager function is the heart of the security scheme and polices the applications and functions on the card.

3.8 Smart Card Applications

MULTOS - Applications are platform-independent and run on a virtual machine. Applications written in languages such as C, Java or even Basic can be compiled into MULTOS Executable Language (MEL) byte code. Security for MULTOS smart cards is enabled by the MULTOS CA, which issues cryptographic keys for each MULTOS smart card and all MULTOS applications. The keys prevent the loading of unauthorised applications without the card issuer's permission.

Java Card-enabled smart cards can run applets downloaded dynamically from servers. Applets can be cryptographically signed and are executed in a sandbox. Due to this flexibility, Java Card is considered less secure than MULTOS

3.9 Smart Card Management

Table 1 below looks in more detail at the steps within each stage of the card manufacturing phase. The supplier is generally responsible for ensuring that the creation and initialisation of the smart card is conducted in a secure and controlled environment. The manufacturing and initial personalisation processes are composed of many individual stages, including: -

Stage	Description	Steps within Stage
Stage 1	Chip fabrication	This stage comprises the following steps: - • fabrication of the wafer • testing of the wafer • loading of initial data onto the wafer.
Stage 2	IC module fabrication	This stage comprises the following steps: - • mounting of Integrated Circuit (IC) into module • wire bonding • encapsulation processes • testing of the IC module
Stage 3	IC card manufacture	This stage comprises the following steps: - • module embedding • initialisation • loading IC card manufacturing data & testing
Stage 4	IC Initial Personal-isation	This stage comprises the following steps: - • loading initial personalisation data • testing • Further personalisation by organisation

Table 1 - Smart Card Manufacturing Life Cycle

Initialisation (sometimes referred to as Pre-Personalisation) is the process by which the fixed person-independent data for an application is loaded into the EEPROM of a smart card.

Personalisation is the process by which the card is assigned to an actual person. This can be physical (embossing and/or laser engraving) and/or electronic (loading personal data in the memory of the card – e.g. Name and PIN).

It is necessary to manage a smart card, just like any other computer asset, and all stages within the smart card life cycle must implement adequate security controls that ensure the integrity of the smart card. This assists in ensuring the security of the information stored upon the card, and it is essential that all phases of the manufacture, issuance and retrieval/destruction of the smart card are performed in a secure and controlled manner.

The overall life cycle for a smart card may be divided in a number of related phases for the manufacture, issuance, usage, retrieval (if required) and destruction of the card.

These phases are illustrated in Figure 3 below: -

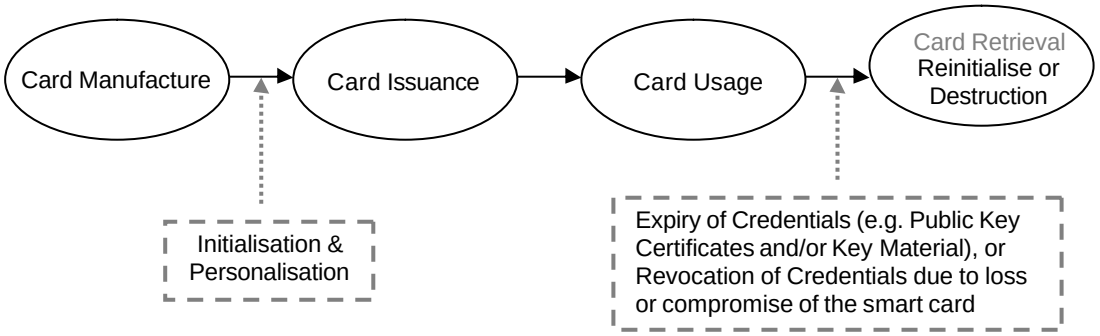

Figure 3 – Smart Card Life Cycle Phases

A key point that procurers of smart cards must grasp is that purchasing smart cards is not the end of the matter. Firstly a consumer needs to determine what their requirements are and how they can be fulfilled with smart cards and if so by what type of spec smart card. Once procured, the smart cards have to be managed within a smart card management system. The workforce need to be educated in the use of the smart card (as new business processes will follow) and the card has to be managed during its lifetime and then securely re-initialised or destroyed.

The following policies would prove of benefit: -

- CONOPS: Concept of Operations – a description of a problem or capability gap that the concept seeks to address and the associated provenance and authority

- CONEMP: Concept of employment for a specific capability within a range of operations or scenarios.

- CONUSE: Concept of Use describes the way in which specific equipment is to be used in a range of operations or scenarios. It represents a developed CONEMP and may have an Acceptable Use Policy as a subsection for users to sign up to.

3.10 Threat/Attack Model

The following Threat/Attack groups have been selected from the following papers [20], [21].

The author deems them to be the most applicable range of articulated attackers for smart cards: -

Class I (= clever outsiders): Smart but lack sufficient knowledge of the system and may have access to only moderately sophisticated equipment. They take advantage of an existing weakness in the system, rather than try to create one.

Class II (= knowledgeable insiders): Substantial and specialised technical education and experience with understanding of parts of the system and potential access to most of it. They have highly sophisticated tools and instruments for analysis.

Class III (= funded organisations): Can assemble teams of specialists with related and complementary skills backed up with significant resources. Capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools available. They may use Class II adversaries as part of the attack team.

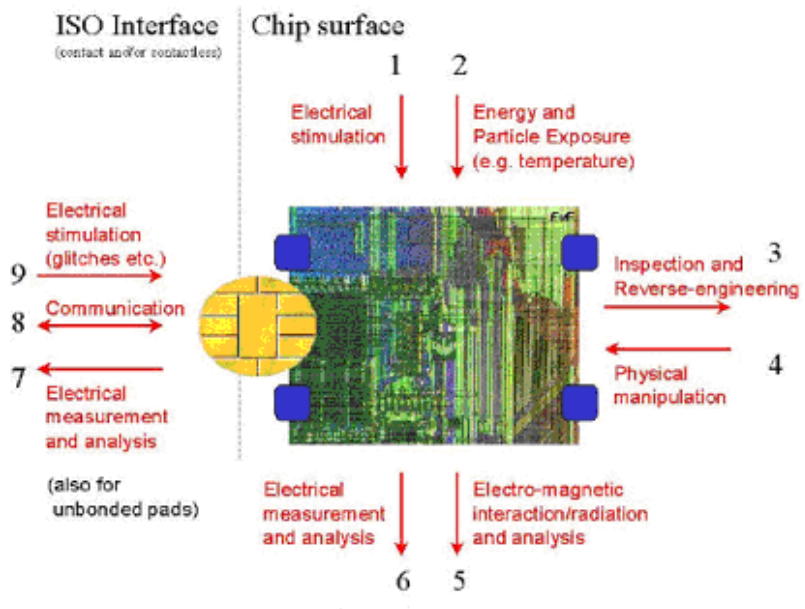

Figure 4. Attack Model for a Contact or Contactless Smart Card Integrated Circuit [10]

Figure 4 above lists nine named potential targeted attacks for a smart card IC. The following high level descriptions of common attacks will be mapped onto Figure 4 as appropriate.

3.10.1 Reverse engineering

The main objective is to identify the structure of the chip as well as detailed information on its internal operations (Attack Number 3 in Figure 4 above).

3.10.2 Physical Probing and/or Modification

Invasive attack to gain unauthorised disclosure or modification of security features/functions, user data, software operation, other operational information and/or change the behaviour of the chip. Affected areas are Attack Numbers 3, 5 and 6 in Figure 4 above.

Modification may be achieved through techniques commonly employed in IC failure analysis (Attack Numbers 1, 2 and 4 in Figure 4).

3.10.3 Observation Attacks: Information Leakage and/or Cryptanalysis (SPA, DPA, DEMA, DFA)

Non-invasive attack is aimed at retrieving sensitive data (e.g. keys) while observing smartcard under operation or stress. Leakage may occur through emanations, variations in power consumption, Input/Output characteristics, clock frequency, or by changes in processing time requirements.

With the exception of DFA, these attacks are sometimes referred to as Side Channel attacks.

Simple Power Analysis (SPA) - corresponds to a direct analysis of the power consumption of the smartcard. The objective of this attack is to determine information from the power consumption levels of the card and determine which set of CPU instructions are being processed and under which parameters (input/output). This corresponds to Attack Numbers 6 and 7 in Figure 4.

Differential Power Analysis (DPA) - is similar to SPA, but differs in that power consumption is measured when known data is processed and subsequently measured again when processing unknown data. DPA is non-invasive and results are statistically analysed. The attack may be derived either from direct contact measurements (Numbers 6 and 7 in Figure 4)

Differential Electro-Magnetic (Radiation) Analysis (DEMA) – is non-invasive and looks at the electromagnetic emanation of the smartcard to retrieve sensitive data (Number 5 in Figure 4) which may then be related to the specific operation being performed at the time possibly using statistical analysis.

Differential Fault Analysis (DFA) - is a method that aims to retrieve secret information from the smartcard by inducing an error while the smartcard is performing a cryptographic calculation. Thus, two kinds of cryptograms are obtained: wrong cryptograms (cryptograms resulting from a disturbed cryptographic operation) and correct cryptograms. Comparison of both types of cryptograms may reveal information about cryptographic keys. Numbers 1, 2 and 9 in Figure 4.

3.10.4 Protocol and/or Functionality attacks

This type of attack looks for flaws in the protocol implementation to find functionality flaws of the smartcard not conforming to the protocols. Techniques can be replay attacks, interrupting the smartcard while it is executing a command undocumented commands and file scanning (Number 8 in Figure 4).

3.10.5 Perturbation, Malfunction, State, Environmental Stress

Operate smart card outside of normal operating conditions to attempt to deactivate security features (Numbers 1, 2 and 9 in Figure 4), or disclose information e.g., increasing or decreasing operational temperatures. By putting the IC in stress conditions (e.g. on the power supply or by illuminating it) the normal behaviour of the software can be changed. The effects could be inverting a test, generating a jump, modifying read values from memory, etc. These modifications could enable an attacker to for example gain access to protected memories or gain rights to perform protected operations.

The generic method in applying perturbation is the same as the DFA attacks. Various methods for perturbing the IC are available such as glitches, light, laser and heating up or cooling down the smartcard.

3.10.6 Software Attacks

This type of attack is looking into software malfunctions of the smartcard. There are various techniques to execute these attacks, among them malicious software loading, bad formatted commands, all of them exploiting security flaws of the smartcard. The main objective is trying to circumvent smartcard security mechanisms and exploit software security flaws (via Number 8 in Figure 4).

3.10.7 Deficiency of Random Numbers

An attacker may predict or obtain information about random numbers generated by the microcontroller for instance because of a lack of entropy of the random numbers provided. The attacker attempts to take advantage of statistical properties of the random numbers generated by the microcontroller without specific knowledge about the microcontroller's generator.

3.11 Section Summary

Smart cards have been seen to adhere to the 'historical' trend outlined earlier in Section 2, benefiting from further miniaturisation enabling greater capacity and also faster operating speeds. Although early adoption of security was weak, smart cards have learned security lessons from devices such as Hardware Security Modules and now many smart cards have high levels of tamper resistance.

Historically smart cards have endured many threats and attacks exposing vulnerabilities (e.g. pay per view TV, travel cards and EMV cards), however in today's world a substantial amount of threats now have countermeasures.

Smart cards have benefited from an amalgamation of different services or elements within a smart card system. By utilising different 'platforms' in a smart card system a stronger defence against vulnerabilities may be achieved - almost like a layering of security and defence-in-depth. An example of this may be using MULTOS with Global Platform or having cards with the same operating system but sourced from different suppliers.

Smart cards started off as monolithic devices with interoperability issues that are now much richer through being able to run multiple applications with governance and adherence to standards improving interoperability.

Due to the increasing attractiveness of smart cards, volumes have increased and through economies of scale production costs and purchase price of cards has dropped – creating a virtuous circle.

With regard to formal internationally recognised evaluation schemes like Common Criteria, chip manufacturers generally focus on threats to their products during the manufacturing and personalisation stages, whereas card issuers tend to focus more on the usage stages.

Manufacturers of smart card chips often have the IC evaluated to relatively high levels. Card manufacturers may then make claims about evaluation level for their products when in reality only the chip has been evaluated. Coprocessors, firmware, the operating system or applications may be untested and unproven.

Protection profiles have been developed to cover the chip, firmware, operating system and Application Programming Interface (API) but not the on-board applications. These profiles usually include a proviso that they should be used in combination with a separate PP to cover applications. However, it is important to stress the important value that formally recognised evaluation schemes provide in that they help to mature the technology and establish whether it is fit for purpose.

Lastly, smart cards need to have a management system applied to them, this is essential for a successful smart card implementation and continuous management and updates to the cards once in use.

4. WIRELESS SENSOR NETWORK NODES

4.1 Section Background and Brief History of WSN Nodes

In the Introduction of this project, there is a fairly high level description of a WSN Node. This section shall provide a more detailed description and explain their practical application in today's world.

When trying to glean information on the topic of WSN Nodes, the author found it very difficult to get anyone to really 'open-up' on this technology. As this is an up and coming area, all the commercial suppliers contacted were focused on selling their products and most didn't return my emails or calls and most academic groups approached clammed up and were not keen have discussions. The notable exceptions are listed in the Acknowledgments of this dissertation.

The primary distinction between a smart card and a WSN Node is that a smart card is not a networked device and does not form part of a network, a WSN Node does. A smart card may connect to a network (e.g., mobile cell phone SIM/USIM) but a smart card is not within itself an integral functioning element within and thereof a network; a WSN Node however is.

Another immediate distinction between smart cards and WSN nodes, is that tamper resistance is not incorporated to any significant level (if at all) in WSN Nodes compared to smart cards where it is deemed essential for security requirements. The lack of tamper resistance in WSN Nodes is due to the sensitive issue of pricing per node – even if a few dollars can be shaved off the cost per node, this can have a substantial effect on bulk volume purchases of WSN nodes, and these nodes are generally heavily bulk purchased.

In many publications, it is very common to see the term 'Mote' used as an interchangeable term for a sensor node and/or wireless network node. The term 'Mote' seems to actually refer to a design specification for a Wireless Sensor Network device known as a 'Berkeley Mote' (which many commercial WSN node builds are still derived from). The University of California Berkeley spearheaded a lot of the work on hardware specs for 'Motes', and also much of the work around protocols and operating systems for these devices too. Mr. Seth Holler was the

original designer of the Mote at Berkeley and has overseen the design of many subsequent Mote designs [6].

A Mote is the actual device that receives information from a sensor and through clusters of similar mote devices forms a wireless sensor network for the distribution of sensor data via motes to a Base Station that collates this information.

Sensors can be plugged directly into the mote printed circuit board or indirectly connected via a link. Sensor types can be anything, but are mainly location, light, sound, temperature, humidity, pressure, motion detection, acceleration.

For the purposes of this dissertation the term Wireless Sensor Network Node shall refer to a device that is a mote with sensor capability that is able to pass its received data onto other devices in kind utilising wireless signals as the communications bearer.

A point to note that due to costs being driven down relative to Moore's Law and advances in wireless communications, it is now possible to produce WSN Nodes at a competitive price, these economies of scale are similar to the developments that have occurred with smart card manufacturing too.

In order to manage the scope of this project, this study will not cover any attacks on sensors themselves and it will not distinguish between Wireless Sensor Network architectures, network topologies or comment on attacks conducted on specific vendors' products. To do so, would broaden the scope of the project to unmanageable levels and fall out of the remit of an MSc project.

4.2 WSN Node Standards

Unique operating characteristics of WSN Nodes such as their small chip low power capability, radio frequency constraints, the fact they work within a hive mentality with an aim to achieving self-organisation whilst being linked into a vast array of sensor data harvesters presents unique challenges for networking these devices. New methods are required to maintain and support these devices to keep them operational. Specific standards are required that support communication both between these devices themselves and WSN Nodes with established forms of computer technology.

4.2.1 TEDS or IEEE 1451 [11]

Sensors are beginning to incorporate a standard communications interface (called TEDS or IEEE 1451) that enables them to automatically identify themselves and describe their functions as soon as they are plugged into a network.

4.2.2 IEEE 802.15.4 & ZigBee [12] [13]

The IEEE 802.15.4 is a standard developed for Wireless Personal Area Networks (WPANs). WPANS convey information over short distances among devices in a network. They enable small, power-efficient, inexpensive solutions to be implemented for a wide range of applications and types of devices.

Wireless Sensor Networks follow the 802.15.4 IEEE Standard and ZigBee is a set of specifications of high level communication protocols designed to use small, low power digital radios based on 802.15.4 and has been developed to meet the growing demand for capable wireless networking between numerous low-power devices and to provide highly efficient connectivity between small packet devices

The relationship between IEEE 802.15.4 and ZigBee is comparable to relationship between IEEE 802.11 and the Wi-Fi Alliance

Bluetooth is suitable for devices that have low power consumption and low radio frequency range, however ZigBee is similar but has been designed solely for use with WSN Nodes. Devices utilising ZigBee can sustain themselves on a small battery for many months, or even years, making them ideal for install-and-forget purposes.

One emerging problem however, is that many companies weave proprietary extensions within ZigBee in order to enhance its performance. Whilst this is slight proprietary flavour is quite common within computer technologies, it is always imperative that development is open and adheres to standards, proprietarisation can often stymie adoption and can lead to technological cul-de-sacs.

Some key characteristics of an IEEE 802.15.4 network are: -

- Can support large networks, up to 65534 devices.
- 16 independent communication channels in the 2.4 GHz band
- Devices use Energy Detection (ED) for channel selection.
- An over the air data rate of 250 kbit/s in the 2.4 GHz band.
- Devices use carrier sense multiple access with collision avoidance (CSMA-CA) to access the medium.
- Devices inform the application about the quality of the wireless link - Link Quality Indication (LQI).

4.3 WSN Node Characteristics

Tubaishat and Madria (2003) [14] have an overview of WSN Node devices as follows: -

"Advances in hardware and wireless network technologies have created low-cost, low-power, multifunctional, miniature sensor devices. These devices make up hundreds or thousands of ad hoc tiny sensor nodes spread across a geographical area. These sensor nodes collaborate among themselves to establish a sensing network. A sensor network that can provide access to information anytime, anywhere by collecting, processing, analysing and disseminating data. Thus, the network actively participates in creating a smart environment."

In essence, Wireless Sensor Networks have the following characteristics: -

- Can consist of any number of WSN nodes, typically comprising hundreds of nodes, possibly compromising thousands of small WSN nodes wirelessly communicating with each other.

- Generally homogenous but may be heterogeneous devices that are measuring something (be it event, incident or any observable and measurable fact).

- A way to pass on this locally ‘harvested data’ which can be passed along through a network, ultimately to be passed to a Base Station where the data can be

aggregated to form a complete picture of what is occurring to inform a user on events.

And WSN Nodes have the following characteristics: -

- A cheap, tiny, low-power, low clock rate processor, small memory, computing device
- A device that monitors one or more sensor and combines sensing, computation and communication into its functionality.

- A device that transmits and receives sensor data via a radio link.

- Collectively they are capable of forming ad-hoc wireless networks to facilitate the distribution of sensor data via the network.

- Capable of running a networking stack and an operating system which provides low-level event and task management.

- Capable of receiving Over The Air (OTA) updates to their code. There is a small boot loader in some types of WSN Node that is capable of rebooting itself on command and utilise a newly downloaded code image.

- Able to go into a sleep mode to conserve power

There are many different vendors of WSN Nodes and WSN technologies and different types of network topology. Sometimes topology or implementation is linked to a specific vendors product, again emphasising the proprietary behaviour that can happen with computer products, especially in the 'gold-rush' moments of a new product when a specific vendor is always hoping that the adaptation within their product ends up being the mainstay in the market meaning that their product is likely to be the one with widespread adoption.

There are also many references the author has found to Self-Organising and Self-Configuring WSNs, whereby nodes can spontaneously create temporary impromptu networks by assembling themselves into an ordered topology establishing

communication patterns and dynamically adapting to device failure and degradation. Self-Healing is sometimes also placed into this bracket. Suffice it to say, there is a lot going on in this field and because it is still a dynamically rapidly changing environment sometimes it feels like trying to catch water keeping up with developments.

Tubaishat and Madria (2003) [14] assessed the characteristics of Wireless Sensor Networks and stated that there are a number of distinct requirements: -

- "Efficient use of limited resources on the node are required: -
    - Routing-tables, data replication, security must work within the confines of the small size of memory in the sensor nodes.
    - Minimal energy use required. Nodes may be deployed in environments that make servicing impossible, so the lifetime of a node may be determined by battery life.
- Large number of sensors are required to undertake the task, which leads to scalability and management issues.
- Self-organisation of the Network. Given the vast quantity of nodes and the possibility of harsh or hostile locations, self-organisation of the modes into a network is a useful requirement (this is related to a self-healing requirement if nodes fail or are damaged and also if new nodes enter the network there is a requirement for consistent connectivity
- Aggregation of data. The vast number of nodes relaying data may end up causing a congestion of the network. To alleviate this issue, some sensors such as cluster heads may aggregate the data and broadcast the new summary/delta information.
- Collaborative signal processing. It is beneficial to fuse data from many sensors. This fusion requires the transmission of data and control messages. This need may put constraints on the network architecture."

Although it has only been three years since Tubaishat and Madria made these comments, and a lot of the issues outlined have had much global research and proposed solutions, there are still many of these challenging aspects remaining, especially with regard to large scale deployments.

Many trade journals and articles portray WSN nodes as the means to surround the Earth in an electronic skin or digital nervous system, which is associated as a notion with Ubiquitous or Pervasive Computing. Ubiquitous Computing was first articulated by Dr. Mark Weiser in 1988 at the Computer Science Lab at Xerox PARC. Dr. Weiser articulates Ubiquitous Computing as being “one person and many computers.”

It is quite possible that WSN Nodes or devices akin to them may become a framework or glue for developments such as Ubiquitous computing, but such thoughts are outside the scope of this project.

Another term that is used a lot in the arena of WSN nodes is Embedded Systems. The Director of the Center for Embedded Networked Sensing (CENS) at the University of the City of Los Angeles (UCLA), Ms. Deborah Estrin, has a concise Venn diagram illustrating the relationships of similar technologies relative to WSN Nodes, see Figure 5 below: -

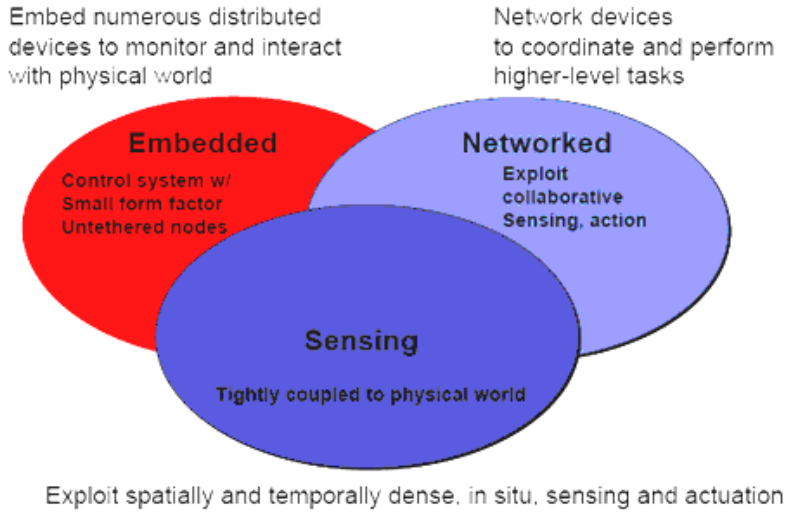

Figure 5. Ms. Estrin’s Venn Diagram Illustrating the Relationships with Mote Based Microcontroller Technologies.

4.4 WSN Node Physical and Architectural Characteristics

The IC on a standard WSN Node tends to consist of the following aspects of real estate: CPU, ROM, RAM, EEPROM and/or Flash Memory, Input/Output ports for sensors, Radio Transmitter/Receiver & Frequency Settings, and an onboard Power Source which is usually a battery with limited power.

To get an appreciation of the scale, resource constraints and architecture of WSN Nodes themselves, a breakdown of the some of the most popular and readily available ones follow. The photos used are promotional photos gleaned from the vendors' corporate websites: -

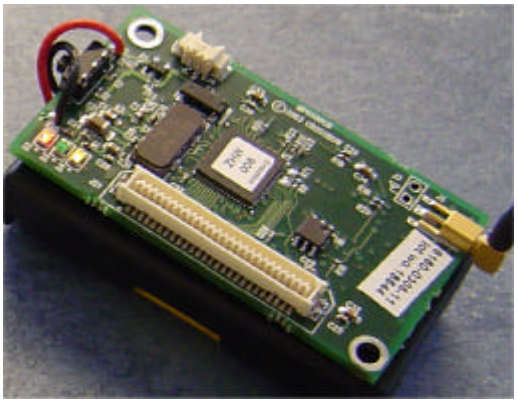

Figure 6. Crossbow Mica2 Mote

Figure 7. Crossbow Mica2 Dot Mote

The Mica2 Mote seen in Figure 6 above is produced by a company called Crossbow Technologies. It consists of an Atmel Atmega 128L processor capable of running up to 4MHz which is common to many of the motes specs derived from the original Berkeley mote specs.

It has a surface mount 51 pin connector for the attachment of sensor boards and power is provided from 2 AA batteries (battery life may last up to a year dependent on the applications utilised)

It has 4Kbytes of SRAM and a 4Kbyte EEPROM and 512Kbytes of serial flash. The radio can function on both the 433 MHz band or the 868/916 MHz bands and its data rate is circa 38.4 Kbps. The outdoor range can go up to 300 metres. This WSN Node utilises Berkeley TinyOS as its underlying operating system to control its functions and any attached sensors. This particular

mote spec allows every mote to function as a routing device and supports remote reprogramming over the network.
The Mica2 Dot Mote (Figure 7 above) is virtually the same as the Mica2. It has a coin sized footprint and using a 3V coin cell battery. It has a temperature sensor and LED on board.

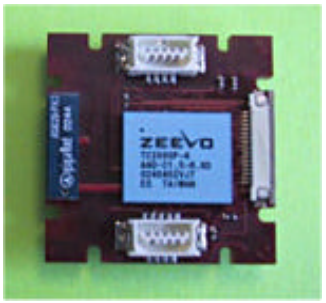

Figure 8. Intel Mote

Figure 8 above is a photo of an Intel Mote that consists of a very powerful ARM processor. It has 64kB RAM and 512 KB flash memory. It is a near coin sized footprint with a 30m range radio and 2.4 GHz antenna. It uses Bluetooth technology and also supports other radio technologies as add on modules. Its mote software is based on TinyOS but has a proprietary specific layer for Bluetooth support, device drivers and topology requirements.


Figure 9. Moteiv TelosB Mote

Figure 9 above shows a photo of Moteiv's TelosB Mote which has an 8 MHz Texas Instruments MSP430 processor, 48 KB Flash memory, 10KB RAM and is out of the box IEEE 802.15.4 compliant.

The Alchemy of WSN Node (Mote) manufacturers is that these devices will eventually disappear from view becoming smartdust and parts of networks known as specknets, with a footprint of $1mm^3$ or less.

In 2003, ‘smart dust’ was designed and built by a team of researchers at University California Berkeley and JHL Labs. It is a WSN node (mote) approximately 2mm by 2.5mm, dubbed 'Spec Mote' or 'COTS Mote'. It has 3KB of memory and can communicate over 12 metres indoors with a data rate of 19.2 Kbps.

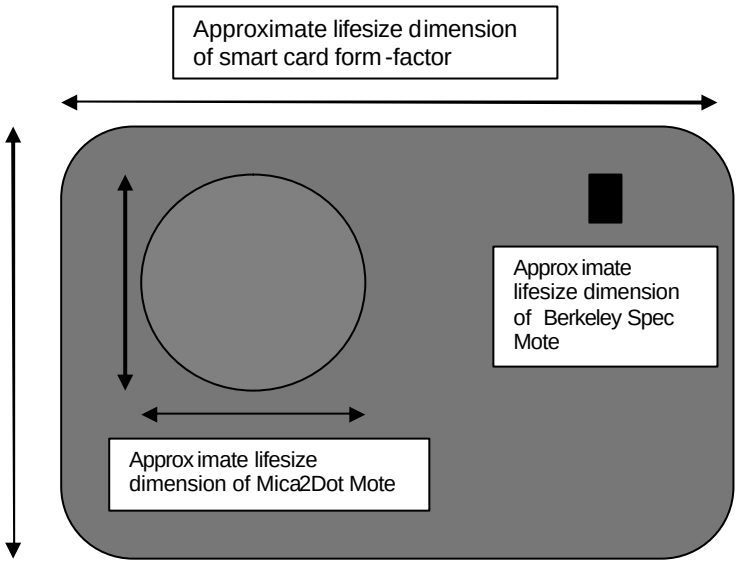

Figure 10. Form-Factor Comparison

In Figure 10, we can see a comparison of the approximate physical form-factors for the technologies discussed so far in this dissertation, this does not include the chip real-estate of the respective microcontrollers as the author was unable to obtain that data.

4.5 Operating Systems and Software

As a point to note, Middleware seems to be a consistent issue. Long established distributed middleware (e.g. CORBA, DCOM) tend to be memory hungry [15].

4.5.1 nesC

The nesC language is an extension of the C programming language. It was primarily designed for use with embedded

systems such as sensor networks, and is also used for structuring concepts and the execution model of TinyOS.

4.5.2 Tiny OS (Tiny Operating System)

TinyOS is an operating system designed specifically using nesC. Tiny OS is an operating system for WSN Nodes, originally for the Berkeley Mote spec but has since been ported to other platforms based on the Berkeley Mote spec. It is the most commonly used choice for operating system with WSN nodes and has now become an 'open community' driven product not dissimilar to the way Linux has evolved in some quarters

4.5.3 TOSSIM (Tiny OS Simulator)

TOSSIM (Tiny OS Simulator) enables modelling and planning to occur for a deployment and/or research and development. TOSSIM is useful to: -

- Plan deployments (especially large scale)
- Cope with limitations of space to conduct research
- Cater for limitations of Cost to procure sensors
- Create a controlled environment and reproduce sensor data
- Cope with repeated real life concept testing can be monotonous and very labour intensive

4.5.4 Maté - 'Tiny Virtual Machine' [16]

Tiny OS programming is regarded as complex, and Dr. Phil Levis (Stanford) has been working on Maté, a 'Tiny Virtual Machine' for Sensor Networks. Maté consists of: -

- Short Virtual Machine programs, providing a safe program execution environment
- A byte code interpreter that runs on TinyOS
- A single TinyOS component that sits on top of several system components

4.6 Wireless Sensor Network Node Applications

Most new cars have some use of sensors within the vehicle to gauge heat, wear and in some cases parking sensors to detect proximity to other solid objects. These sensors are quite basic in terms of what is being discussed in this section, but their established presence points the way forward to a likely greater and wider use within society.

Within the field of Wireless Sensor Networks, much of the data harvested is of a monitoring and/or tracking nature – an adage that rings true relative to this is "if you can't measure it, you can't manage it".

The following are proposed areas where WSNs may have potential uses: -

- Collection of Environmental Data: -
  - Habitat Monitoring (e.g., Ecosystems)
  - Integrated Biology
  - Structural Monitoring (e.g., Buildings, Roads or Bridges)
  - Heart and Brain Monitoring
  - Industrial

- Interactive & Control data: -
  - Pursuer-Evader (e.g., Military, many roles but a possible replacement for landmines)
  - Building Security (e.g., Intrusion Detection)
  - Automation

- Predictive Maintenance
  - Seismic Structure Response (e.g., Earthquakes, Tsunami)
  - Containment Transport
  - Micro-Organisms (e.g., Marine Monitoring)
  - Ecosystems Bio-complexity

One example of Habitat Monitoring was a UC Berkeley trial at the Great Duck Island Environmental Preserve [17], a small island off the coast of Maine in the US. The trial consisted of monitoring a nesting site for storm petrels (an ocean bird).

WSN node devices operated on a low duty cycle lasting up to a year and the devices would wake up periodically every 8 seconds to read sensors and send data.

This trial enabled analysis of the nesting environment and how the environment affected hatchling health and survival. A project in a similar vain is the Zebranet project at Princeton University.

4.7 Wireless Sensor Network Node Threat Model

A point to note is that historically, many WSN routing protocols were simple and hence vulnerable to targeted attacks, to some degree this is still the case. Although there are many 'open' routing protocols available, there are still many implementations that use proprietary routing protocols and algorithms.

When it comes to WSN Node threats, many papers categorise threat as being network Outsiders or Insiders; further, attackers are categorised as Mote-class attackers or laptop-class attackers [4].

Mote-class attackers are perceived to have access to a few WSN Nodes with similar capabilities to the WSN Nodes they wish to exploit, but there reach is restricted to only affecting a few nodes within a WSN.

Conversely, a laptop-class attacker may be in possession of much more potent devices (e.g., laptops for instance). Use of this type of device or greater can lead to a higher and wider degree of threat to a WSN.

C. Karlof and D. Wagner 2003 [4] state "Insider attacks may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes, and who then use one or more laptop-class devices to attack the network."

Because of the nature of WSN node devices, attacks tend to focus on known vulnerabilities: -

- Denial of Service attacks on the device by running down its power source (battery) through continuous operation
- Radio Frequency jamming so data can not be transmitted or received

- As devices do not seem to have a crypto-coprocessor any encryption carried a massive processing overhead for already constrained processing capabilities.
- As WSN Node ICs are not tamper resistant, any secret information on the chip is susceptible to standard physical and logical attacks that smart cards used to widely suffer.

4.8 Section Summary

WSN Nodes are a relatively new and maturing technology. There are some authoritative sources of information, but published information seems to date very quickly.

Nodes have limited storage, processing and bandwidth capability and power (battery) management is essential.

The author was not able to find any WSN Node Common Criteria evaluated products or Protection Profiles, and due to the maturing nature of the technology this is not surprising.
However, WSN Nodes would clearly benefit from some form of Protection Profile to assist their maturity and produce a bench mark for people to assess the assurance that products may offer.

5. THREAT ANALYSIS METHODOLOGY

5.1 Section Background

5.1.1 Research

It is important to note that the author was not able to obtain funding to purchase any smart cards and/or WSN Nodes to undertake any form of direct 'physical' security analysis. Instead, this dissertation is based on experiences the author has had through his professional work with smart cards and through reading research papers and articles that distinguished people have written on both smart cards and WSN Nodes.

The author had two significant challenges during this project; the first was a vast learning curve on WSN Node technologies, as the author has never worked in this field but had a growing interest in the technology. The second was in designing a framework to undertake the threat analyses for smart cards and WSN nodes.

To meet the first challenge of a knowledge gap, the author read as much as possible on the subject on WSN Nodes and also contacted key players in the field of Wireless Sensor Networks.

The author was able to get very useful email feedback from the following people: -

- Dr. Phil Levis - Stanford University (PhD Berkeley) who has been responsible for many key items of research on Sensor Networks and is currently working on application specific virtual machines for WSN Nodes (e.g. Maté).

- Mr. Chris Karlof - University of California, Berkeley (Graduate Student) who has produced many research papers on Sensor Networks especially in the fields of Routing and Security.

Both Dr. Levis and Mr. Karlof were very helpful, but due to constraints on their time they were only able to offer the author helpful high level guidance pointers.

The author did manage to have very useful discussions with the following people: -

- Dr. D. K. Arvind - University of Edinburgh (Director, Institute for Computing Systems Architecture) currently working on a Specknet project.

- Mr. Harry Cassar – BP (Technology Director CTO Team) who has been responsible for many trials and implementations of WSN Nodes within the oil company's business operations.

- Dr. Phil Buonadonna – Arch Rock Corporation (formerly a senior researcher with Intel). Arch Rock develops products that support wireless sensing and control networks.

These discussions helped the author plug knowledge gaps within the subject of WSN technologies and also helped establish and firm up areas of interest for this project.

Provenance of contacts is supplied in Appendix 1 - Primary Correspondence with Subject Matter Experts.

5.1.2 Why Threat Analysis and not Risk Analysis?

In order to control the scope of this MSc project, and prevent it becoming a vast programme of work, this dissertation covers a Threat Analysis and its constituent parts, and will not cover the following areas: -

- Risk Analysis or Assessment
- Risk Management
- Security Policies

In any form of Risk Management, it is necessary to initially determine and assess the Threats you need to mitigate before you can then subsequently assess the Risks to the particular environment in question. In the case of this project, the contexts of use of the technologies and the environments within which they could be used are not established because this project is a generic threat analysis and it would be necessary to constantly make scenario assumptions which would lead it to be more a work of fantasy rather than grounded in reality.

Incorporating Risk would also widen the scope of this project up further whilst adding very little to the key aim and objectives,

which are to assess the similarities security issues within the two technology types.

However, if required within a 'real-world' scenario, a section for Risk could be added to the Threat Analysis framework produced for this project, thereby adding more value to real world use. Any reader interested in aspects of Risk Analysis or Management should refer to ISO 17799 & 27001 (BS7799 Parts 1 and 2).

It is worth establishing how the bulk of threats can come about. In many situations, the product eventually developed is rarely exactly what the design specification intended as a whole – the end product is ever so slightly different, either by design amendments, product implementation or configuration. This is more pronounced in Software design but Hardware design is not immune to the problem.

The point being that testing evaluations and security assessments are based off the original design specification (this includes how the item will be implemented and configured). In real life designs change as do implementations and configurations. This is one of the main ways that bugs or vulnerabilities enabling exploits can occur.

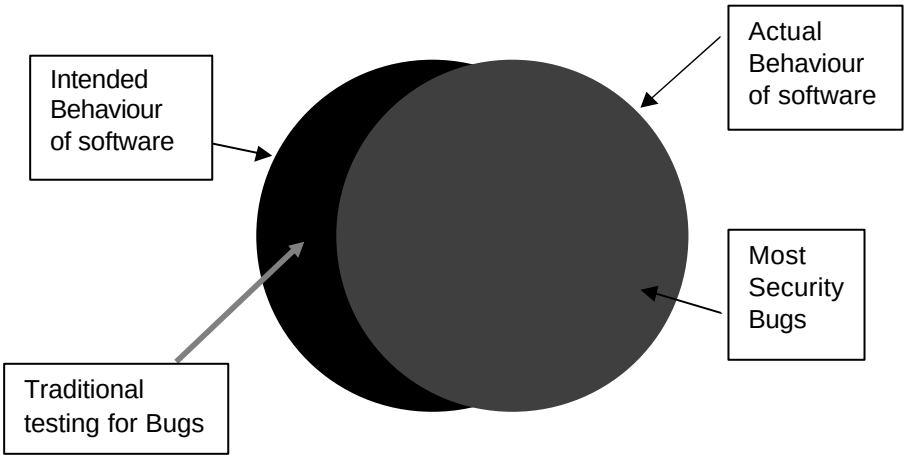

Figure 11. Misalignment of Perceived Vulnerabilities relative to Actual Vulnerabilities [18].

Figure 11 [18] above illustrates how a misalignment can occur within the perceived product and the final actual product, and how this is also reflected in the perceived vulnerabilities within the product and what transpires to be the actual vulnerabilities.

Although this diagram was originally used to reflect issues within the design of Software, the author feels that it has applicability to a much wider area including firmware and hardware, especially for new products that have yet to seasoned by thorough code reviews or open scrutiny.

So, in essence users are expecting a product to undertake a specific role, which invariably it does and meets the user's expectations. However, the way in which the product conducts the execution of this role may be very different than what was intended within its original design and most evaluations and it is quite possible that evaluations and assessments are geared around the original specification and sometimes fail to capture all the design changes and variances in implementation and configuration.

5.2 Threat, Vulnerability, Attacker and Countermeasure (TVAC) Table

As a point to note for the reader, the author discovered many different definitions and interpretations for terms like Threat, Risk, Vulnerability, Attack, Countermeasure, Mitigation and Safeguard in many different publications. Therefore the author has attempted to astutely produce his own definitions for some terms and the author gives clear indication to the reader where this has taken place.

The kernel of this project is to identify the most common critical security issues broken down into constituent elements: threats, vulnerabilities, attacks and countermeasures. This identification will be conducted firstly for Smart Card technologies and then subsequently same exercise for Wireless Sensor Network Node technologies. Once these security issues have been flagged, it is then possible to undertake the next part of the study, which is to compare and contrast the security issues between the two different technologies.

In order to capture, analyse and assess security issues the author needed to create a 'tool' to facilitate and enable this activity. There are many different tools or mechanisms that exist to capture and assess threats and risks, but in the author's eyes for this project, they all seemed to have drawbacks, either because they were for designed for software, traditional computing environments, and server rooms or were heavily

weighted to assessing Risk rather than documenting Threats and associated security issues.

Therefore, the author had to create a framework and tool to enable the logging and cataloguing of threats, vulnerabilities, attacks and countermeasures within each technology type. Outside of the significant learning curve the author had in researching and understanding WSN Nodes, the creation of this framework and tool was the biggest challenge during this project.

The author created a Threat, Vulnerability, Attacker and Countermeasure Table; this will hereafter be referred to as a TVAC table. A blank copy of a TVAC Table can be seen at Appendix 2 and populated copies can be seen at Appendix 3.

This table sounds simple enough, however the challenge came in making this table contain relevant subsections to provide sufficient information when logging security issues whilst being of a simple enough layout and construction to make it useable, manageable and easy to understand.

Therefore, the aim with the TVAC Table was to achieve a simple mechanism to log, collate and catalogue relevant and sometimes complex data, which could in turn be easily understood by a wide readership.

The TVAC Table designed for this project has been designed to be a composite of five fundamental blocks that enable data to flow from one block to the next. Each block contains specific elements and subsections that provide the necessary granularity in detailing the security issue.

The blocks are as follows: -

1) THREAT BLOCK
2) VULNERABILITY BLOCK
3) ATTACKER BLOCK
4) COUNTERMEASURE BLOCK
5) APPLICABILITY to WSN NODES/SMARTCARDS

A walkthrough description of the TVAC Table now follows.

Each TVAC table has two columns preceding the five blocks just mentioned, these columns consist of the following: -

5.2.1 Technology Column

This column indicates what technology has been reviewed in the Threat Analysis table, as follows: -

- Contact Smart Card
- Contactless Smart Card
- WSN Node

5.2.2 Threat Unique Identifier (TUID) Column

In this column, each threat is given a Threat Unique ID (TUID) to prevent any confusion and to keep the information in the table specific to that threat. The TUID may also assist when cross-referencing to other threats by acting as a primary key (this could also enable XML tagging of each threat to aid threat classification in a shared or global threat catalogue).

TUID referencing is as follows: -

- A Contact Smart Card – has the prefix SCA and the threat reference to follow – e.g., SCA-T1

- A Contactless Smart Card – has the prefix SCB and the threat reference to follow – e.g., SCB-T1

- A WSN Node – has the prefix WSNN and the threat reference to follow – e.g., WSNN-T1

A breakdown of each block now follows: -

5.2.3 THREAT BLOCK

In the context of this project, the author has defined a threat as being: -

“An objective a foe might try to realise in order to misuse a target or asset”

The Threat Block is made up of the following constituent parts: -

5.2.3.1 Target and/or Asset

This states at ‘what’ the attack is aimed, and the author has chosen the following broad categories: -

- Physical - Chip
- Physical – Other (State the details)
- Logical - Operating System
- Logical - Platform
- Logical – Application
- Logical – Other (State the details)
- Communications Bearer (e.g., Card Reader, RFID, RF)
- Other (State the details)

5.2.3.2 Threat Class

The classification of the threat has been broken down in the following areas: -

- Physical Static (e.g., No Power to Hardware)
- Physical Dynamic (e.g., Power to Hardware)
- Logical Static (e.g., No Power to Software)
- Logical Dynamic (e.g., Power to Software)
- Social (e.g., Social Engineering)
- Policy (e.g., Weakness in Governing Policies)
- Other (State the details)

5.2.3.3 Threat Summary

This includes a brief 'Statement' describing the Threat, followed by an indication of the 'Entry Point', which is then followed by a rating of the 'Impact' of the Threat. The author has categorised impacts as being: -

- H = High
- M = Moderate
- L = Low
- U = Unknown

The use of the letters H, M, L, U respectively indicate the impact. This categorisation was chosen, because the types of technology in question are relatively simplistic on an application and functional level (microcontrollers with small Operating Systems and Applications) which should lead to a clear impact assessment. IT Systems and Operating Systems such as Windows or Linux would require more granular impact ratings or scoring, due to the sophistication of the technology hence requiring more layers of impacts.

5.2.4 VULNERABILITY BLOCK

In the context of this project, the author has defined a vulnerability as being: -

"A specific means by which a threat can be executed via an unmitigated attack path."

5.2.4.1 Vulnerability Summary

This includes a brief 'Statement' describing the Vulnerability, followed by a rating of the 'Probability' of the Vulnerability occurring. The author has followed a categorisation similar to the Threat Summary Impact rating (outlined above): -

- H = High
- M = Moderate
- L = Low
- U = Unknown

5.2.4.2 CRIPAL

CRIPAL is an acronym the author has established to cover the following high level 'primary' security goals (the following definitions are the author's own): -

- C = Confidentiality – The restriction of information and/or assets (both physical and logical) to authorised entities/individuals only.

- R = Reliability – The ability to access and use information and/or assets (both physical and logical) consistently without disruption

- I = Integrity – The maintaining of information and/or assets (both physical and logical) in their complete and intended form.

- P = Privacy – The ability for an entity/individual to choose with whom to share their 'Private' information and/or assets (both physical and logical), without concern of impermissible access and/or use.

- A = Availability – Constant and timely access to information and/or assets (both physical and logical) for authorised entities/individuals.

- L = Legitimate Use – Use of information and/or assets (both physical and logical) is undertaken by authorised entities/individuals who have the legal rights to conduct actions through propriety.

A vulnerability will be characterised by one or more of the letters of this acronym that relate to the specific categories above, e.g., if the vulnerability exposes Confidentiality as a weakness, a "C" will be placed in the CRIPAL column.

5.2.4.3 STRIDE

STRIDE is a method used by Microsoft [19] to help categorise threats during software development. In the context of this project, STRIDE helps to add a low level granularity to the previous 'CRIPAL' column. Similarly to CRIPAL above, any of the letters that make up the STRIDE acronym can be used as an entry within the TVAC table.

The STRIDE acronym is explained in more detail through Table 2 below: -

STRIDE Categories	STRIDE Definition	More Common Interpretations
(**S**)poofing	Using another person's authentication information, such as User ID & Password.	Authentication, Masquerade, Man in the Middle.
(**T**)ampering	Malicious modification of data.	Integrity Violations.
(**R**)epudiation	Users who deny performing an action. Non-repudiation refers to the ability of a system to counter repudiation threats.	Non-Repudiation.
(**I**)nformation Disclosure	Information/data exposure to individuals who are not supposed to have access to it.	Confidentiality and/or Privacy Violation.
(**D**)enial of Service	Deliberate attempt to prevent legitimate users from using a service or system.	DOS (Denial or Disruption of service), DDOS. Reliability & Availability Violation.
(**E**)levation of Privilege	Where an unprivileged user gains privileged access. An	Access Control.

	example of privilege elevation would be an unprivileged user who contrives a way to be added to the Administrators group.	Permissions and Rights Violation.

Table 2. STRIDE Table.

5.2.5 ATTACKER BLOCK

In the context of this project, the author has defined an attacker as being: -

"The entity that is exploiting a Vulnerability to establish a Threat."

The author has made the assumption that all attacks are deliberate. Non-deliberate accidents or Acts of God/Natural Disasters are not covered and are out of scope. This project is dealing with deliberate attempts to tamper with information and/or assets (both physical and logical).

5.2.5.1 Attacker Group

The following Attacker Groups have been selected and derived from [20], [21].

"Class I (= clever outsiders): They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

Class II (= knowledgeable insiders): They have substantial specialised technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis.

Class III (= funded organisations): They are able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team."

This maps quite well to other standard views on grouping attackers, a generic mapping follows: -

“Class I” (= clever outsiders) → “Opportunist Attacker” (Hobbyist and/or Vandal possibly seeking personal fame using basic widely available tools)

Class II (= knowledgeable insiders) → “Expert/Professional Attacker” (Personal Gain generally financially motivated and using tools adapted specifically for the purpose)

Class III (= funded organisations) → “Sophisticated Attacker” (Intelligence Services or very highly skilled Organised Crime. A long term and sustained attack using specially created tools and long standing highly trained operatives for specific operational gains).

5.2.5.2 Attack Class

These are tied to Threat section: -

- Invasive Active (e.g., Cutting new tracks)
- Invasive Passive (e.g., Microprobing just to observe not to alter what is happening)
- Non-Invasive Active (e.g., Power Surge or glitch attacks)
- Non-Invasive Passive (e.g., DPA and Timing Attacks)
- Semi Invasive techniques (e.g., Light attacks)

An ‘invasive attack’ involves physical penetration and alteration to the IC, and a ‘non-invasive attack’ involves no physical harm or alteration to the IC on the card.

Attacks can be either passive or active:-

Active attacks, like brute force and glitch attacks, involve interfering with the signals applied to the device including the power supply line.

Passive attacks, also called side-channel attacks, do not involve any interaction with the attacked device but, usually, observation of its signals and electromagnetic emissions.

Semi-invasive attacks [22] involve some depackaging to reach the chip’s surface, however it is not necessary to break through the passivation layer to gain physical access to the chip’s interior.

Many attacks can be blended, i.e. which means that there is a potential for mixed threats which are potentially more effective – especially if it is a form of avalanche attack.

5.2.6 COUNTERMEASURE BLOCK

In the context of this project, the author has defined a countermeasure as being: -

"A mitigation measure that prevents, detects or significantly reduces a misdeed associated with a specific threat or group of threats."

For the purposes of this study a Safeguard and a Countermeasure are treated as the same thing as classed as a Countermeasure, the key point being that it is a way to mitigate the threat.

5.2.6.1 Countermeasure Summary

This includes a brief 'Statement' describing the Countermeasure, followed by a categorisation of the 'Effectiveness' of the countermeasure, defined as follows: -

- Total – Complete Effectiveness
- Partial – Some Effectiveness
- None – No Effectiveness

5.2.6.2 Overhead of Countermeasure on Time, Performance & Cost

When implemented, most countermeasures tend to have an impact on Time, Performance and Cost to some degree. Within this part of the block the author has tried to assess what this might be.

5.2.7 APPLICABILITY to WSN NODES/SMARTCARDS

This section deals with whether the Threat, Vulnerability, Attacker and Countermeasure data can be applied to the other technology, e.g., from Smart Cards to WSN Nodes and vice versa.

This follows a similar categorisation used within the Countermeasure Summary: -

- Total – Complete Applicability
- Partial – Some Applicability
- None – No Applicability

5.3 Section Summary

This has been rather a lengthy chapter, but the detail therein is necessary to explain the TVAC Table, the vital tool required to conduct the respective threat analyses. The threat analyses can now be seen in the populated TVAC tables that are in Appendix 3.

Section 6 contains a Threat Analysis Assessment Comparison to see what threats can be mapped from one technology to the other.

6. THREAT ANALYSIS ASSESSMENTS & COMPARISONS

6.1 Section Background

The populated TVAC tables are the key pieces of analytical data for this study. However due to the fact that they take up 23 pages the author feels that they are better positioned in the Appendix of this dissertation (Appendix 3) for reasons of space and presentation and cross referenced when appropriate.

The author has aimed to define as many threats as possible within the limitations of time and knowledge. This is not an objective approach, however judgment has been utilised to determine the most common and the most severe forms of threat to the technologies being studied.

Ten threats, SCA-T1 to SCA-T10, have been defined for Contact Smart Cards and these have also been allocated to Contactless Smart Cards too as SCB-T1 to SCB-T10 respectively as they were deemed by the author as being equally applicable.

Four additional threats have been applied to Contactless Smart Cards as SCB-T11 to SCB-T14, giving Contactless Smart Cards a total of fourteen potential threats.

Eight threats have been defined for Wireless Sensor Network Nodes, defined as WSNN-T1 to WSNN-T8.

NB: On some occasions, results for the effectiveness of the countermeasure on mitigating the threat and also the applicability of the threat relative to the other technology were not clear cut. In this instance a 'Partial' or 'Partial to Total' rating was given.

The applicability of each one of these threats and its respective countermeasures from one of the technologies relative to the other has been assessed by the author and represented as results within a Comparative Threat Analysis Assessment Matrix. Next, we shall look at the results within this matrix and subsequently the rest of this section will be a discussion of the threats and countermeasures that do map from one technology to the other one. Due to time and space constraints the author

will not give any great detail to the threats that have no applicability from one technology to the other.

6.2 Comparative Threat Analysis Assessment Matrix

Matrix Key: -

1. SCA/B = Threat and/or Countermeasure is applicable to both Contact and Contactless cards and hence are referenced as so.

2. Contact Smart Card – has the prefix SCA and the threat reference to follow – e.g., SCA-T1

3. Contactless Smart Card – has the prefix SCB and the threat reference to follow – e.g., SCB-T1

4. WSN Node – has the prefix WSNN and the threat reference to follow – e.g., WSNN-T1

5. ✓(T) = Total Match; ✓(P) to (T) = Partial to Total Match; ✓(P) = Partial Match; ×(N) = No Match

Contact & Contactless Smart Card Threats

Smart Card Threat Ref:	Threat Applicable to WSN Nodes	Counter-measure Applicable to WSN Nodes
SCA/B-T1	✓(T)	✓(P) to (T)
SCA/B-T2	✓(T)	✓(P) to (T)
SCA/B-T3	✓(T)	✓(P) to (T)
SCA/B-T4	✓(T)	✓(P)
SCA/B-T5	✓(T)	✓(T)
SCA/B-T6	✓(T)	✓(P)
SCA/B-T7	✓(T)	✓(P) to (T)
SCA/B-T8	✓(T)	✓(P)
SCA/B-T9	✓(T)	✓(P) to (T)
SCA/B-T10	✓(P)	✓(P)
SCB-T11	✓(P)	✓(P)
SCB-T12	✓(P)	✓(P)
SCB-T13	✓(P)	✓(P)
SCB-T14	✓(P)	✓(P)

Threat Totals	**Countermeasure Totals**
✓(T) = 9	✓(T) = 1
✓(P) to (T) = 0	✓(P) to (T) = 5
✓(P) = 5	✓(P) = 8
×(N) = 0	×(N) = 0

WSN Node Threats

WSN Node Threat Ref:	Threat Applicable to Smart Cards (state whether contact or contactless)	Counter-measure Applicable to Smart Cards (state whether contact or contactless)
WSNN-T1	✓(P) SCB	✓(P) SCB
WSNN -T2	×(N)	×(N)
WSNN -T3	✓(P) SCA/B	✓(P) SCA/B
WSNN -T4	×(N)	×(N)
WSNN -T5	×(N)	×(N)
WSNN -T6	×(N)	×(N)
WSNN -T7	✓(P) SCA/B	✓(P) SCA/B
WSNN -T8	✓(T) SCA/B	✓(T) SCA/B

Threat Totals	**Countermeasure Totals**
✓(T) = 1	✓(T) = 1
✓(P) to (T) = 0	✓(P) to (T) = 0
✓(P) = 3	✓(P) = 3
×(N) = 4	×(N) = 4

Figure 12. Comparative Threat Analysis Assessment Matrix

In Figure 12 above, we can see on the left of the matrix that all of the fourteen catalogued smart card threats were deemed by the author to have an applicability to WSN nodes (nine totally applicable and the remaining five partially so).

Also, all of the fourteen possible countermeasures for these threats were also perceived to be applicable in some shape or form to mitigating the same threat within WSN Nodes (one totally, five partially to totally and eight partially).

In Figure 12 on the right of the matrix, we can see that only four of the eight threats on WSN Nodes were applicable to smart

cards (one totally and three partially). The remaining four threats were deemed not applicable.

Of the eight possible countermeasures, four were deemed applicable matching the threat applicability results (one totally and three partially) the remaining four being not applicable matching the threat values

The rest of this section will now cover the threats catalogued in the populated TVAC tables in Appendix 3. This will be a high level summary of the threat and countermeasure with an explanation as to why the threats and countermeasures are deemed as applicable to the other technology.

6.3 High Level Summary of Populated TVAC Tables in Appendix 3

Threats will be referred to by their Threat Unique ID: -

SCA/B-T1

Smart cards are susceptible to a threat of reverse engineering of the IC using specialist tools. Possible countermeasures include an active shield or mesh that once broken renders the IC unusable by initially destroying data held within the chip and secondly shutting down operations of the chip. The use of environmental sensors within the chip would have a similar affect as a countermeasure.

Most smart cards have these forms of tamper resistance included within their design and manufacture these days, but one thing the author found striking is that WSN nodes do not appear to have tamper resistant chips as it is perceived to be a cost overhead that may affect the purchase price.

Established and existing smart card chip tamper resistance techniques should be transferable to the world of WSN Nodes at only a marginal increase in the price of the item due to only subtle modifications being required and economies of scale should stabilise any price increases over time.

SCA/B-T2

Smart cards are susceptible to Microprobing. This attack and its countermeasure are closely related to SCA/B-T1above, and the explanation and rationale given above is also valid for this threat.

SCA/B-T3 and SCA/B-T4

Side Channel attacks like Simple Power Analysis, Differential Power Analysis or EM emanation analysis are novel ways to attack smart cards. WSN nodes may be susceptible to the same types of attack and as such would benefit form the techniques used within smart card chips today to combat these threats. Countermeasures such as randomness and scrambling should be easily retrofitted to WSN node chip specs

The same goes for Differential Fault Analysis which is SCA/B-T4. Existing smart card countermeasures could be transferable to WSN Node chip specs with some modifications.

SCA/B-T5

This threat seems to map directly onto WSNN-T8 and involves a Test Mode which smart card and WSN node chips seem to share [24]. It appears to be possible to attack the respective chips to unlock the Test Mode and as such get full logical control of the IC. Smart cards attempt to mitigate this threat by requesting authentication to the Test Mode function if an attacker has successfully managed to call up the Test Mode. Authentication failure leads to chip inoperability. As a matter of course this mitigation should be applied to WSN nodes.

SCA/B-T6

Modern smart cards are able to undertake a form of internal firewalling with memory management to prevent a protocol or functionality attack with the potential for rogue code to be executed. Upon researching this further it appears that WSN nodes do not have this type of protection. So, once again there should be the possibility of looking at the way smart cards mitigate this threat and adapt it for WSN nodes.

SCA/B-T7

Dr. Sergei Skorobogatov [22] has undertaken fascinating work in the field of Data Remanence. The countermeasures he proposes for the protection of smart cards from this type of threat should be applicable to WSN Nodes.

SCA/B-T8

This threat involves weaknesses in operating policies and adherence to policies. There is a need for clear operating policies such as CONOPS, CONUSE and CONEMP. Adherence to laws like the Data Protection Act 1998, RIPA 2000, and CMA 1990 are mandatory. Many publications mention the use of asymmetric keys within smart cards and WSN nodes and the potential for public key certificates; however these very same publications do not mention Certificate Policy or Key Management Policy which would underpin the use of keys or certificates. The threats and countermeasures are applicable to both technologies.

SCA/B-T9

WSN nodes do not appear to have crypto-coprocessors. Some smart cards do. This threat involves weakness in the randomness of random number generation. The capacity of WSN nodes is limited; however the addition of a crypto-coprocessor with protection for cryptographic services would make a WSN node much more robust.

SCA/B-T10

This relates to a Smart Card Management System and/or a Database Management System and how these are required for effective management of smart cards but also the fact that they need protecting from malicious attack, especially any form of reachback attack from a device like a smart card or WSN node back into an Enterprise network. The author has seen no mention of a WSN Node Management System – this in itself seems a vulnerability.

SCB-T11 and SCB-T12 (Contactless Smart Cards only)

These threats involve the interception of messages via RF communications and have partial applicability to WSN nodes due to the RF connection. However the countermeasures do not map across effectively to WSN nodes

SCB-T13

This threat and range of countermeasures refer to [23]. It is quite possible that a range of RFID exploits can be applied from smart cards to WSN nodes and proposed countermeasures may mitigate these threats.

SCB-T14

This involves the potential of a Denial of Service (DoS) attacks for contactless smart cards and the fact that there may be some applicability to WSN nodes.

WSNN-T1

This range of WSN node threats involves differing levels of DoS which may have a partial applicability to contactless smart cards (e.g., Jamming). The author also applies a new term to WSN nodes of Cessation of Service (CoS).
Because WSN nodes are battery powered, they are designed to exploit a sleep mode to conserve power. If the nodes are forced into continuous operations (transmit, receive, and standby use up significant amounts of energy for a WSN node) any continuous activity will use up pressure battery capacity. A sustained DoS attack may lead to a final CoS attack in that the node uses up all of its power and is no longer enable to function. Such an attack spread over a Wireless Sensor Network becomes a Distributed Cessation of Service (DCoS) attack.

WSNN-T2

This involves routing data between nodes and hence as such has no applicability to smart cards which are not networked devices.

WSNN-T3

The Sybil attack seems specific to WSN nodes, however the issue of spoofing, masquerading or exploiting multiple identities is something that can be shared to a partial degree between WSN nodes and smart cards. Sun's SSSL (Sizzle) mini web server [26] for WSN nodes may have some application with regard to smart cards as a way of enabling an efficient securing of communications.

WSNN-T4 through to WSNN-T6

This involves routing data between nodes and hence as such has no applicability to smart cards which are not networked devices.

WSNN-T7

This involves weaknesses in the underlying programming languages. nesC which is used to create Tiny OS a leading operating system for WSN nodes, is derived from C. The applicability to smart cards is minimal but may relate to the native functions that smart card manufacturers may utilise within their cards before more commercially widespread operating systems (Multos) or platforms (Java) are installed.

WSNN-T8

This threat and corresponding set of countermeasures maps directly onto SCA/B-T5

6.4 Section Summary

This section has assessed the vast amount of analytical information captured within the TVAC tables.

Most of the attacks catalogued involve high levels of expertise and access to specialist equipment; thus meaning that although many of these threats are very real and should be taken

seriously, they are not as widespread as threats to PCs are today.

The findings from this study imply that common threats on smart cards that are shared with WSN nodes are within the Integrated Circuit space; effective countermeasures to these threats that are currently applied to smart cards may be able to be possibly modified and adapted to become effective countermeasures for WSN nodes. A classic case in point being tamper resistance.

Common threats on WSN nodes that are shared with smart cards tend to be in the Radio Frequency space that relate to contactless smart cards, but they only share a slight relation. Indeed if we look at the technologies involved, one could perceive that between the worlds of contact smart cards and WSN nodes lies the bridge of contactless smart cards.

7. CONCLUSION AND RECOMMENDATIONS

7.1 Conclusion

It is important to note that this is a subjective study undertaken under the author's best judgment.

The author's knowledge and the amount of published material available is skewed more heavily toward smart cards rather than WSN nodes, primarily because more has been written and experienced with regard to smart cards compared to WSN nodes in today's world.

Taking these facts into account, the author still feels that the two Objectives that were stated at the start of this dissertation have been met fully by the research undertaken in this course of study.

The findings from this study imply that common threats on smart cards that are shared with WSN nodes are within the Integrated Circuit space; effective countermeasures to these threats that are currently applied to smart cards may be able to be possibly modified and adapted to become effective countermeasures for WSN nodes. A classic case in point being tamper resistance.

Common threats on WSN nodes that are shared with smart cards tend to be in the Radio Frequency space that relate to contactless smart cards, but they only share a slight relation. Indeed if we look at the technologies involved, one could perceive that between the worlds of contact smart cards and WSN nodes lies the bridge of contactless smart cards.

Smart cards have learned valuable lessons from the world of Hardware Security Modules, with respect to tamper resistance and secure creation and storage of cryptographic keys. Security modifications have been successfully adapted to the miniaturised world of smart cards and could further be passed onto WSN nodes if required.

Not all WSN nodes are going to need tamper resistance, the same way that not all smart cards require all of the robust security measures available to them. What seems unusual however is that no tamper resistance seems available within commercially available WSN nodes. Security has been a

business enabler for smart cards, increasing their appeal and due to the benefits of economies of scale prices have been dropping whilst volume has increased – a virtuous circle. The same benefits could be derived for WSN node production.

The capacity of WSN nodes is very limited so they cannot carry much in the way of functions. This was and to some degree still is similar to smart cards; however smart cards have matured and continue to mature into more multi-functional, multi-purpose and multi-application devices. What has helped this maturing process is standardisation and vendor neutrality and schemes like Common Criteria.

The production of Protection Profiles to which microcontrollers and Operating Systems can adhere to and the potential to achieve a formal evaluation of products under the internationally recognised scheme of Common Criteria has helped mature the development of smart cards, in much of the same way that it helped the development of HSMs before too. The same route of evaluation may help speed up the maturity of WSN nodes

Most attacks on smart cards and WSN nodes still require high levels of expertise and access to specialist equipment, which makes them unlikely to move into the realm of the 'script-kiddie' for some time yet.

It is quite possible that technologies like smart cards, embedded systems and WSN nodes may converge in the future to provide a framework or glue to facilitate Ubiquitous Computing utilising wireless communications.

7.2 Recommendations

vi. The author feels that there might be similarities to explore with threats and countermeasures within the functioning of Mobile Cell Phone compared against WSN nodes. Also, could SIMs be used within some WSN nodes out of interest too?

vii. An assessment of the applicability of Global Platform and its Card Manager, Java Card Runtime Environment (JCRE) and various existing smart card APIs compared to WSN nodes may prove of interest.

viii. There might also be scope to explore network mapping tools such as those used in the TCP/IP world like Eracent Network Probe (ENP), to see if they can be adapted to work in the WSN node world to produce a similar mapping capability for Wireless Sensor Networks. The same can be said of things like SNMP, and there may also be some overlap with projects like AVISPA.

ix. The exploration of Attribute Certificates [27] and/or Kerberos tickets for Authentication requirements that may be applied to both smart cards and WSN nodes may produce some interesting areas of study.

x. The author would be interested to develop an authentication and routing protocol which he has labelled KAFKA (Know Allies & Family, Know Adversaries) to suit the adaptive nature of Wireless Sensor Networks.

BIBLIOGRAPHY

References

[1] F. Stajano, *Security for Ubiquitous Computing* John Wiley and Sons Ltd, 2002, pp267

[2] Common Criteria for Information Technology Security Evaluation. Smart Card Security User Group Smart Card Protection Profile Version 3.0 9 September 2001

[3] German Federal Office for Information Security (BSI). 'Security Aspects and Prospective Applications of RFID Systems' 2004

[4] "Secure routing in wireless sensor networks: attacks and countermeasures" by Chris Karlof and David Wagner, University of California, Berkeley, Elsevier Article 2003

[5] Enisa Quarterly No. 4, “Security in Wireless Sensor Networks: Status, Problems, Current Technologies and Trends”. Sead Muftic, Chih-Chun Chang Mar 2006 page 5-6

[6] Seth Hollar MS Thesis on Cotsdust, 1996. http://www-bsac.eecs.berkeley.edu/archive/users/hollar-seth/publications/cotsdust.pdf

[7] “Spec takes the next step toward the vision of true smart dust” 2003. http://www.jlhlabs.com/jhill_cs/spec/index.htm

[8] World’s Fastest Computers. http://www.top500.org/.

[9] Bell's Law of Computer Classes. http://en.wikipedia.org/wiki/Bell's_Law_of_Computer_Classes

[10] Eurosmart: Smartcard IC Platform Protection Profile Version 1.0 July 2001.

[11] IEEE 1451 FAMILY OF SMART TRANSDUCER INTERFACE STANDARDS http://grouper.ieee.org/groups/1451/0/body%20frame_files/Family-of-1451_handout.htm

[12] IEEE 802.15 WPAN™ Task Group 4 (TG4)
http://www.ieee802.org/15/pub/TG4.html

[13] ZigBee Alliance Home page
http://www.zigbee.org/en/index.asp

[14] M. Tubaishat, S. Madria. "*Sensor Networks : An Overview*", IEEE Potentials, 22 (2003), 20--23.

[15] "Yang Yu, Bhaskar Krishnamachari, and Viktor K. Prasanna, "Issues in Designing Middleware for Wireless Sensor Networks," IEEE Network Magazine, January 2004.

[16] "Maté: A Tiny Virtual Machine for Sensor Networks." *Proceedings of the 10th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS X).* 2002

[17] "Wireless sensors from UC Berkeley and Intel researchers help conservation biologists monitor elusive seabird in Maine" 05 August 2002
http://www.berkeley.edu/news/media/releases/2002/08/05_snsor.html

[18] 'Security of The Internet Presentation' at Chatham House, London - New Security Issues Programme, 4th May 2005 by David Aucsmith Microsoft Corporation.

[19] F. Swiderski and W. Snyder, *Threat Modeling*, Microsoft Press 2004 pp259

[20] "Low Cost Attacks on Tamper Resistant Devices", Ross Anderson, Markus Kuhn 1997

[21] "DG Abraham, GM Dolan, GP Double, JV Stevens, "Transaction Security System", in IBM Systems Journal v 30 no 2 (1991) pp 206-229: -

[22] "Semi-invasive attacks - A new approach to hardware security analysis." Sergei P. Skorobogatov April 2005 UCAM-CL-TR-630 ISSN 1476-2986

[23] ‘Is your cat infected with a computer virus’ Melanie R. Rieback, Bruno Crispo, Andrew S. Tanenbaum, Vrije Universiteit Amsterdam. 2006

[24] Tampering with Motes: Real World Physical Attacks on Wireless Sensor Networks. Alexander Becher, Zinaida Benenson, Maximillian Dornseif, October 2005

[25] T. FINKE and H. KELTER, Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO14443 - Systems. BSI, 2004
http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf

[26] SUN's Sizzle (SSSL) Webserver for small devices
http://research.sun.com/spotlight/2004-12-20_vgupta.html

[27] TICKET BASED IDENTITY SYSTEM FOR DRM, Alapan Arnab and Andrew Hutchison, South Africa, 2006

Additional Sources

W. Rankl and W.Effing, *Smart Card Handbook*, John Wiley and Sons Ltd, 2003 pp.1120

R. Pastor-Satorras and A. Vespignani, *Evolution and Structure of the Internet – A Statistical Physics Approach*, Cambridge University Press, 2004

M. Ilyas (Ed.), *The Handbook of Ad Hoc Wireless Networks*, CRC Press 2003

APPENDICES

1. Primary Correspondence with Subject Matter Experts

From: **Philip Levis** [pal@cs.stanford.edu]
Sent: 07 December 2005 16:38
To: Kevin Eagles
Subject: Re: Masters Project Idea

DoS in wireless networks is trivial: just get a powerful transmitter.

Generally, the interesting twist you see in sensor network security is that nodes can be physically compromised. If you don't consider that a valid attack (e.g., there's someone watching the network), then you can get pretty good security by just installing every node with a shared private key and use AES at the data link level, etc.

If you do consider physical compromise a valid attack, then it starts to get trickier. This path starts to go towards using consensus-based protocols. That is, if an adversary compromises one node the rest of the nodes don't agree with it and so ignore it. Of course, if the adversary compromises a large fraction of the nodes this will no longer work, but, well, the adversary has already compromised a large fraction of the nodes and owns them. :)

Chris Karlof has an interesting paper on the kinds of attacks that sensornet protocols can be easily vulnerable to with regards to consensus, etc.

Phil

On Dec 7, 2005, at 12:42 AM, Kevin Eagles wrote:

> Dear Phillip
>
> Please excuse the email out of the blue, I appreciate that you are an
> intensely busy person.
>
> However, I am deeply fascinated by Sensor Networks (Smart Dust), Tiny
> OS and Mate.
>
> My name is Kevin Eagles and I am a part-time student on an Masters
> course in Information Security: -

> http://www.isg.rhul.ac.uk/msc/

[...]

From: **Chris Karlof** [ckarlof@cs.berkeley.edu]
Sent: 09 March 2006 19:14
To: Kevin Eagles
Subject: Re: Sensornets Project

Hi Kevin,

As I mentioned, I'm not involved in sensor networks much at all right now, so I don't know the answers to many of your questions, nor do I know what a good direction to work in is. TinySec is for the obsolete
Mica2 platform and is not supported on "Zigbee compliant" plaforms. We have some undergrads working on getting the hardware security mechanisms on the Telos motes made by Moteiv, but that's it. Moteiv is composed of former Berkeley students and are good guys. Any release of TinyOS will be pretty good. You should probably use the latest version. Regarding routing, most motes don't use internet protocols. I don't know what TinyOS does for routing now, but I'm sure it's somewhere in the docs.
David and Naveen are probably too busy and they are no longer working in sensor networks either.

-chris

[...]

From: **dka@inf.ed.ac.uk**
Sent: 22 March 2006 09:24
To: Kevin Eagles
Subject: Re: Sensornets Project #3

Speak to you at 10am.
A.

Quoting Kevin Eagles <K.Eagles@rhul.ac.uk>:

> Hi Arvind
>
> Many thanks for your email.
>
> No worries, I appreciated that something must have come up. Hope that
> the stress levels have dropped back today.
>
> So, I'll call you tomorrow. Is 10.00hrs ok?

>
> Regards,
>
> Kevin
>
> dka@inf.ed.ac.uk wrote:
>
>> Hi Kevin,
>>   My apologies for my absence from the office today - I
>> arrived from Washington last night and had to attend to a family
>> emergency today and am just catching with my email. What times are
>> you available on Wednesday? It will be best if I were to call you.
>> Yes, I am very keen to discuss security-related issues re:specknets.
>> Best regards,
>> Arvind

[...]

From: Sterley, Candice [Candice.Sterley@uk.bp.com]
Sent: 24 January 2006 09:42
To: Kevin Eagles
Subject: RE: RE: MSc RHUL Project - Sensornets and Pervasive Computing

Attachments: Sunbury travel one pager.doc

Kevin

I have confirmed Monday, 6th Feb, 15:30 at our BP offices in Sunbury for you with Harry.

Our address is:
BP International Ltd
Chertsey Road
Sunbury
Middlesex
TW16 7LN

I have attached some travel information for you, i.e. if you are coming by train, please make your way to Feltham Station and we have a free BP Shuttle bus that runs from the station to site and returns every 15 min.

On arrival on site, please make your way to Building 200, or ask at any Buildings reception for 200 and they will direct you. At reception ask for myself or Harry and we will come down and collect you.

If you need any further information or I can help in anyway, please do not hesitate to contact me.

Kind Regards
Candice

Candice Sterley
DCT Chief Technology Office
E mail: Candice.Sterley@uk.bp.com
Address: BP International Ltd, Chertsey Road, Sunbury-upon-Thames, Middlesex, TW16 7LN

-----Original Message-----
From: Kevin Eagles [mailto:K.Eagles@rhul.ac.uk]
Sent: 23 January 2006 23:18
To: Sterley, Candice
Subject: Re: RE: MSc RHUL Project - Sensornets and Pervasive Computing

Hi Candice

My name is Kevin Eagles, and further to Mr. Paul Dorey's email below, I understand Mr. Harry Cassar has agreed to speak with me on the topic at reference.

[...]

From: Phil Buonadonna [pbuonadonna@archedrock.com]
Sent: 09 March 2006 22:26
To: 'Kevin Eagles'
Subject: RE: RE: Sensornet Project

Kevin,

I think the best way to address things is via a phone call. I"m out of town at the moment.

Would you be available to talk next week?

If a phone call is not possible, I can draft up a reply.

pb

Phil Buonadonna
Arched Rock Corp.
657 Mission St. Ste 600
San Francisco, CA 94105-4120

> -----Original Message-----
> From: Kevin Eagles [mailto:K.Eagles@rhul.ac.uk]
> Sent: Thursday, March 09, 2006 11:03 PM

> To: Phil Buonadonna
> Cc: 'Roland Acra'; 'Wei Hong'
> Subject: Re: RE: Sensornet Project
>
> Hi Phil
>
> I am new to the field of Sensornets, Motes and Tiny
OS.
>
> Just to recap, my project is as follows: -
>
> "Security Analysis of Sensor Networks" - encompassing:
-
>
> (i) "Sensor Networks Attacks (Exploits and
Vulnerabilities)"
> (ii) "Secure Routing in Sensor Networks"
>
> I appreciate that you are very busy, but I have a few
queries below: -
>

[...]

2. Blank TVAC Table

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
				**Statement** : **Entry Point**: **Impact**:	**Statement** : **Probability**:		
Contact Smart Card Contactless Smart Card WSN Node	**SCA-T1** **SCB-T1** **WSNN-T1**						
							

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
		Statement : **Effectiveness**:	**Time**: **Performance** : **Cost**:

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Is the Threat applicable to WSN Nodes and can the same countermeasure be applied

TVAC TABLE – (Threat, Vulnerability, Attacker and Countermeasure Table)

3. Populated TVAC Tables

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	**SCA-T1 SCB-T1**	Physical - Chip	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Reverse Engineering - identify the structure of the chip as well as detailed information on the internal operation of the chip's building blocks and interconnections **Entry Point**: Various **Impact**: H	**Statement** : Use of etching, microscope, photography and image processing and microprobes to study the build and workings of the IC. **Probability**: L	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Invasive Active Passive. Non-Invasive Active & Passive. Semi Inv	**Statement** : Tamper resistant topological design measures. Chip surface protected by an active shield/sensor mesh or security fuse. Attack detected when shield lines cut or contacted. An interruption or short circuit in shield/mesh triggers a countermeasure, such as the erasure of the chip's memory & an end to all functions – card death. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Nil **Cost**: Cost of design & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Threat has total applicability to WSN Nodes and the countermeasure may have partial to total applicability

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	SCA-T2 SCB-T2	Physical – Chip & Logical Other: (Data Flow & potential Data Extraction)	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Microprobe memory buses on the microcontroller by making an electrical contact to record the stored data as it is accessed. **Entry Point**: Passivation layer **Impact**: H	**Statement** : Using several probes to observe various subsets of the data and address bus lines while the processor runs a program, it's possible to record the data accessed by the program. Time consuming, but without adequate outer protection, attack is possible given access to equipment. **Probability**: L	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Invasive Passive	**Statement** : Tamper resistant topological design measures. Chip surface protected by an active shield/sensor mesh or security fuse. Attack detected when shield lines cut or contacted. An interruption or short circuit in shield/mesh triggers a countermeasure, such as the erasure of the chip's memory and an end to any functions – basically card death. **Effectiveness**: Partial to Total	**Time**: Manufacturing Process takes longer **Performance**: Nil **Cost**: Cost of design and manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Threat has total applicability to WSN Nodes and the countermeasure may have partial to total applicability

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contact & Contactless Smart Card	SCA-T3 SCB-T3	Physical - Chip	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Side Channel attack - observing behaviour of signals within card (e.g. SPA, DPA, DEMA). Retrieve sensitive information e.g. Keys. **Entry Point**: Various **Impact**: H	**Statement** : Information Leakage: Processors react differently when undertaking different operations. Encrypt and Decrypt times are different. Also, all electronic devices give off Electro-magnetic emanations **Probability**: M	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Passive	**Statement** : All data must be encrypted & also disguised to protect against data analysis of stored & internally transmitted data. Randomness of behaviour prevents interpretation of leaked info. Memory layout scrambling, memory address bus encryption, noise generation, traffic adding/padding, time disturbance and algorithmic process masking. Use EM shielding along TEMPEST lines to curtail emanations. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate countermeasure of EM shield **Performance**: Possibility of minor delays due to time or power randomisation **Cost**: Cost of redesign & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Threat has total applicability to WSN Nodes and the countermeasure may have partial to total applicability

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	**SCA-T4 SCB-T4**	Physical - Chip	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Environmental State Attack – brute force and glitch attacks to interfere with the signals that occur within IC e.g. Differential Fault Analysis (DFA) **Entry Point**: Various **Impact**: M	**Statement** : Attempts to create faults in the IC due to irregular operating conditions – e.g. Differential Fault Analysis with power and/or temperature changes. **Probability**: M	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active	**Statement** : Monitor state with sensors acting as an IDS to ensure proper operating parameters are not left. Sensors can detect operating voltage (high & Low), clock signal & frequency, temperature, detection of illegal access and instruction. Use a regular self-test to detect any modification of these onboard sensor devices. If breech occurs memory erases and chip becomes inoperable **Effectiveness:** Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Possibility of False Positives with the heat and power sensors **Cost**: Cost of redesign & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has total applicability to WSN Nodes but the countermeasure may have partial applicability because WSN Nodes operate in potentially hostile conditions so there may be a higher tendency for greater false positives when compared to smart cards.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contact & Contactless Smart Card	SCA-T5 SCB-T5	Physical – Chip and Logical Other: (Test Function Exploit)	Physical Static & Dynamic Logical Static & Dynamic Social	**Statement** : Exploit 'Test Mode' within the IC to reach 'Live Mode' of and extract sensitive data. This can utilise any of the Threats already highlighted including possible social engineering on how Test Mode is accessed. **Entry Point**: Various **Impact**: H	**Statement** : Some microcontrollers have a manufacturer's test interface to access memory for testing of device. It may be possible to exploit this interface to extract sensitive information stored within the chip. Such test circuitry is usually destroyed after use, but an adversary may try to create a track to re-enable a test circuit. **Probability**: L	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.	**Statement** : Test Mode should be physically disabled. As a failsafe, the chip will check during start-up whether it is going into user mode or test mode, depending on several phase identifiers. If test mode is the active phase, a trusted path authentication request will occur before any further action. Authentication failure will lead to test mode lock-out and/or card disablement. **Effectiveness**: Total	**Time**:Manufacture time goes up to incorporate these requirements. **Performance**: Nil **Cost**: Cost of manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Threat has total applicability to WSN Nodes and the countermeasure may have total applicability – See WSNN-T8 Threat on JTAG interface.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	SCA-T6 SCB-T6	Physical – Chip & Logical - Operating System	Physical Static & Dynamic Logical Static & Dynamic Social	**Statement** : Protocol &/or functionality attack.Try to usurp onboard file system and/or execute rogue code - e.g., execute bogus application or bogus update code. **Entry Point**: Various **Impact**: M	**Statement** : Either by randomly trying spurious command sets or some of the attacks already mentioned, it might be possible to gain unauthorised access to the file system and/or run illegal code. **Probability**: L	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C I C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.	**Statement** : Memory Management & Firewall for access control to memory areas checking target addresses within limits. No code exec-ution in EEPROM or RAM. EEPROM has write/erase disallowed by setting page to prot-ected state, any bogus access attempt leaves content unaltered. Protection permanent once set, violations lead to prevention of execution and/or erasure of memory contents. Consider Global Platform with Card Manager, signed code, authentication/confirmation for updates. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Possibly a tiny bit slower as these memory protection functions are executed and any signed code verified **Cost**: Cost of manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has total applicability to WSN Nodes, the countermeasure may have partial applicability because Global Platform is designed for smart cards

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contact & Contactless Smart Card	SCA-T7 SCB-T7	Physical - Chip	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Data remanence issues with volatile and non-volatile memory, whereby memory retains information for some time after power down [22] **Entry Point**: Via memory bus to memory cells **Impact**: M	**Statement** : Security processors hold secret information (e.g. keys) in SRAM. If tampering occurs, power removed & SRAM erased. SRAM contents below -20°C can be frozen. Skorobogatov [22] has proved info can be extracted from erased memory before it reaches -20°C. Potential remanence issue. **Probability**: L	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.	**Statement** : Do not store sensitive information for long periods in SRAM & move sensitive information to new areas periodically and zeroise the original storage area. Use temperature detection circuits in addition to the tamper detection. Use encryption if possible to make data recovery from erased memory more difficult. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Possibly a tiny bit slower as these memory protection functions are executed. **Cost**: Cost of manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)
Threat has total applicability to WSN Nodes and the countermeasure may have partial to total applicability [22]

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	**SCA-T8** **SCB-T8**	Other: Integrity of Organisation	Social Policy	**Statement** : Possible that underpinning smart card policy weak and exposes the company to malicious use **Entry Point**: Organisation's IT System **Impact**: M	**Statement** : Carelessly drafted or inadequate policy on using smart cards within an organisation coupled with poor implementation may lead to unnecessary vulnerability exposure to that organisation, due to incorrect Access Control or robust smart card enrolment procedures **Probability**: M	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C I C II C III	Non-Invasive Passive	**Statement**: Have a Concept of Use CONUSE document - describes how equipment is used in a range of operations. Users sign & adhere to Acceptable Use Policy or Subscriber Agreement. Adherence with Data Protection Act 1998, RIPA 2000, Computer Misuse Act 1990 & Human Rights Act principle on Privacy. Implementation of a Smart Card Management System should help with enrolment issues and smart card management. **Effectiveness**: Partial to Total	**Time**: If documents aren't written they will have to be written and this will take time **Performance** : Nil **Cost**: External Assistance in the form of consultants may be required to produce relevant documentation and implement a Smart Card Management System.

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has total applicability to WSN Nodes and the countermeasure may have partial applicability (NB: Certificate Policy, Key Mgt Policy)

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contact & Contactless Smart Card	SCA-T9 SCB-T9	Physical – Chip: (Crypto-graphic Operations)	Physical Static & Dynamic Logical Static & Dynamic	**Statement** : Deficiency of Random Numbers - An attacker may predict or obtain information about random numbers generated by the IC. **Entry Point**: Various **Impact**: M	**Statement** : Due to a lack of entropy for the generation of random nos, an adversary may gather info about the produced random numbers. This may prove an issue because these random nos may be used in the creation of cryptographic keys. It might be possible to take advantage of the statistical properties of these random numbers.. **Probability**: L	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Invasive Passive. Non-Invasive Active & Passive. Semi Invasive.	**Statement** : Cryptographic Support using hardware accelerators through crypto co-processors supporting all crypto operations, including a robust Random or Pseudo-Random Number Generator. Mask the value and location of random numbers once they are generated and when finished delete them. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Possibly a tiny bit slower as these protection functions add process overheads when executed. **Cost**: Cost of design and manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has total applicability to WSN Nodes and the countermeasure may have partial to total applicability.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contact & Contactless Smart Card	**SCA-T10 SCB-T10**	Other: Smart Card Management System and/or Enterprise Database Management System (DBMS)	Logical Static & Dynamic Social Policy	**Statement** :Threat to management of smart cards as an asset, exposure of ownership details. Also information on the card has to be tracked. **Entry Point**: Via malicious code on card or malicious user access to a Mgmt System **Impact**: M	**Statement** : It might be possible to attack the back-end systems that support the tracking and use of smart cards. An attack on these systems could have reach-back to an enterprise network with wide ranging consequences. **Probability**: L	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active & Passive. .	**Statement** : Two-Person rule required to enrol someone for a smart card, and have stronger vetting for these operators. Use code signing to restrict bogus code and with regard to an Enterprise DBMS, have a scaled down DBMS (with hash codes) stored and regularly updated (synchronised) on card **Effectiveness**: Partial to Total	**Time**: Design and implementation time goes up to incorporate these requirements. **Performance**: Possibly a tiny bit slower as these protection functions add process overheads when executed. **Cost**: Cost of design and implementation increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat may have partial applicability to WSN Nodes and the countermeasure may have partial applicability.The author has not found any infor-mation stating a WSN Node equivalent to a Smart Card Management System. However, there are snippets of research on DBMS for smart cards & WSN Nodes that may reside on these devices to manage the vast respective information that now exists on these respective devices.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contactless Smart Card	SCB-T11	Commun-ication Bearer: (between contactless card and reader device)	Physical Dynamic and Logical Dynamic	**Statement** : Eavesdropping threat between reader & transponder is viewed as a specific threat to RFID systems which Finke and Kelter have investigated [25]. **Entry Point**: Comms Channel **Impact**: H	**Statement** : Due to the nature of broadcast and receive within RFID devices, access to and/or data on an RFID device could be intercepted and eavesdropped by unintended (malicious) parties. This leads to issues of Confidentiality, Privacy and Spoofing and possible replay and injection attacks. **Probability**: M	C I P L	S T I E

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : If the card is placed in a sleeve lined with metal, it will not function, and RFID cards could be secured in such wallets when not in use. A PIN or some secondary factor in addition to the possession of the care must be required to authorise access. Also commun-ication and data transmission between a card and reader should be encrypted. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance** : Nil **Cost**: Cost of design & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has partial applicability to WSN Nodes due to the nature of comms between WSN Nodes. Some aspects of the countermeasure may have partial applicability, especially device enabling sentient authorisation via a trusted path and also use of encrypted comms channels.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contactless Smart Card	SCB-T12	Commun-ication Bearer: (between contactless card and reader device)	Physical Dynamic and Logical Dynamic	**Statement** : Similar to threat SCB-T11 but involves a malicious masquerading reader either impersonating a valid reader or snooping and working independently to but at the same time as a genuine reader. **Entry Point**: Comms Channel **Impact**: H	**Statement:** In some cases, if two or more terminals were close together, not only did both terminals read the card, but the read range of each terminal increased to as much as 9 metres **Probability**: M	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : Same as for SCB-T11 but in addition any contactless card should undergo mutual authentication with strong authentication challenge-response principles with a reader to ensure validity of reader and prevent potential replay attacks. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance** : Nil **Cost**: Cost of design & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has partial applicability to WSN Nodes due to the nature of comms between WSN Nodes. Some aspects of the countermeasure may have partial applicability, especially notion of strong authentication using a challenge-response approach.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Contactless Smart Card	SCB-T13	Other: (Threat to backend middleware systems supporting RFID Devices)	Physical Dynamic and Logical Dynamic	**Statement** : Similar to threat SCA/SCB-T10.Various potential RFID attacks mentioned in [23] that define threats with SQL, Buffer Overuns and the threat of reachback to Enterprise networks. **Entry Point**: Various **Impact**: M to H	**Statement:** SQL Injection Attack to a backend 'middleware' system that uses SQL. Buffer overflow attacks to middleware and potential virus or worm attack. Main concern is the reach back to the RFID middleware or enterprise data base. **Probability**: M	C I P L	S T I E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : Disable multiple SQL statements in a single query and make database tables read only. Undertake thorough and 'open' code reviews to weed out bugs in the RFID device code that could be exploited. Request authentication to shut down a database server to prevent the trigger of a DOS. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Nil **Cost**: Cost of design & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has partial applicability to WSN Nodes due to the fact that WSN Nodes do have their data collated within a central repository. Some aspects of the countermeasure may have partial applicability.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Contactless Smart Card	SCB-T14	Commun-ication Bearer: (between contactless card and reader device)	Physical Dynamic and Logical Dynamic	**Statement** : Abuse of comms channel to create a DOS attack **Entry Point**: Comms Channel **Impact**: M to H	**Statement:** Jamming the comms signals could disrupt data exchange as the air interface is not very robust, even simple passive measures can prove an effective attack. Possibility of high-energy burst of RF to damage chips too perhaps **Probability**: M	R A L	T D

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active & Passive.	**Statement** : Try and use source tracking via triangulation or power meters to track jamming source. Also, ensure card is temporarily housed or stored in sleeve lined with metal when not in use to prevent any harm from an RF high energy surge. **Effectiveness**: Partial	**Time**: Implementation time goes up to incorporate the tracking requirements and manufacture of metal shielded card sleeves **Performance** : Nil **Cost**: Cost of design, manufacture & implementation increases to cover this countermeasure

(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)

Threat has partial applicability to WSN Nodes due to the fact that WSN Nodes can suffer DOS or DDOS via jamming techniques. Some aspects of the countermeasure may have partial applicability.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Wireless Sensor Network Node	WSNN-T1	Commun-ications Bearer: (Radio Frequency)	Physical Dynamic & Logical Dynamic	**Statement** : Jamming, Flooding & collisions cause disruption & an eventual denial of service (DOS). Excessive & unplanned use of WSN Nodes use up valuable battery life & hence can be deemed a Cessation of Service (COS) attack. **Entry Point**: Comms Channel **Impact**: H	**Statement** :RF is an open medium & susceptible to jamming: noise or interference on the same channels that are delivering the wireless service, or a direct malicious attack. Flooding is when there is a continuous viral like promulgation of a message to many if not all nodes. Transmit, Receive and Standby Modes use the most power. Byzantine General's Problem **Probability**: M	R A L	D

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C I C II C III	Non-Invasive Active & Passive.	**Statement** : Adapt existing real-time RF management & wireless prevention/detection. Blacklist rogue nodes. Automatically reconfigure transmit channel. Possibly use Frequency-hopping spread spectrum (FHSS) to switch/change many channels by pseudorandom sequence known to both transmitter and receiver. IBM has a security solution Wireless Intrusion Detection Extensions (WIDE) that might be adaptable too. **Effectiveness**: Partial to Total	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: My improve as it might be possible to remove the noise from comms **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has partial applicability to Contactless Smart Cards, only in the sense that this type of smart card is susceptible to jamming and collision attacks but only on a per card basis and not on a network basis, also adaptation of countermeasures may have partial applicability.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Wireless Sensor Network Node	**WSNN-T2**	Communications bearer: (Routing Protocol) & Logical Other: (data within node)	Physical Dynamic & Logical Dynamic	**Statement** : Spoof, Alter, or Replay WSN Routing Information. **Entry Point**: Comms Channel **Impact**: H	**Statement** : Targeted attack on the routing information exchanged between nodes which can attract or repel network traffic, create wasteful routing loops, false error message generation, increase end-to-end latency **Probability**: M	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active & Passive.	**Statement** : The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key. Could use Public Key Elliptic Curve Cryptography (ECC) with a small footprint as key distribution for a globally shared symmetric key or use ECC Dig Sigs. Sun has Sizzle (SSSL) a form of SSL that uses ECC **Effectiveness**: Partial to Total	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: Encryption may produce a slight overhead in performance. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Wireless Sensor Network Node	WSNN-T3	Commun-ications bearer: (Routing Protocol) & Logical Other: (data flow)	Physical Dynamic & Logical Dynamic	**Statement** : The Sybil attack has a solo node presenting itself to the WSN with multiple different identities **Entry Point**: Comms Channel **Impact**: M	**Statement** : This causes a raft of security issues and can lead to many different attacks being attributed to different sources which are in fact all emanating by the disguised 'sybil' node. **Probability**: M	C R I P L	S T R I

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : Outsider attack prevented by link layer encryption & authentication using a globally shared key. Could use Public Key Elliptic Curve Cryptography (ECC) with a small footprint as key distribution for a globally shared symmetric key or use ECC Dig Sigs. Sun has Sizzle (SSSL) [26] a form of SSL that uses ECC. To prevent 'Insider' attack, entities may be verified using public key cryptography - verification key pair to enable digital signing. **Effectiveness**: Partial to Total	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: Encryption may produce a slight overhead in performance. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)

Threat has partial applicability to Smart Cards in that a smart card could theoretically be attacked in such a way that the card ends up carrying many identities or could have a new identity added – however, due to robust tamper resistance of modern smart cards this type of attack is unlikely to be commonplace. Countermeasure may have partial applicability [26]

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Wireless Sensor Network Node	WSNN-T4	Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)	Physical Dynamic & Logical Dynamic	**Statement** : HelloFlood attack: Many protocols expect broadcast of 'HELLO' packets to neighbours. Nodes receiving these packets think they are in acceptable radio range of transmitting node. However a laptop class attacker & powerful transmitter could convince nodes that the malicious (laptop-class) node was a neighbour. **Entry Point**: Comms Channel **Impact**: M	**Statement** : This attack causes a large number of nodes to try to use a routing path via the bogus malicious (laptop-class) node.It could be considered a uni-directional broadcast wormhole attack. This attack uses a single hop broadcast to reach many receiving nodes and is not a flooding attack in the true sense. **Probability**: M	C R I P A L	S T I D

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : Verify the bidirectionality of a link before taking acting on a message received over that link. This is less effective when an attacker has a highly sensitive receiver as well as a powerful transmitter as they can create a wormhole to every node within range of their transmitter/receiver. Since the links between these nodes & the attacker are bidirectional, the above approach is unlikely to be able to locally detect or prevent a HELLO flood. **Effectiveness**: None to Partial	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance** : Nil. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Wireless Sensor Network Node	**WSNN-T5**	Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)	Physical Dynamic & Logical Dynamic	**Statement** : Wormholes. Messages tunnelled from part of the network & replayed in a different part. Involves at least two different malicious nodes working together to deceive their distance to the rest of the network by passing packets via out-of-bound channel used only by the attackers **Entry Point**: Comms Channel **Impact**: H	**Statement** : An attacker located near a base station can utterly disrupt routing by convincing nodes that might be multiple hops from a base station that they are in only a few hops away via the wormhole. This creates a form of sinkhole & all traffic in the area will be drawn through the node if alternative routes do not appear as good. **Probability**: M	C R I P A L	S T R I D

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active & Passive.	**Statement** : Wormhole attacks may be used in tandem with selective forwarding or eavesdropping and detection is potentially difficult when used in conjunction with the Sybil attack – mitigation of these attacks will lessen the impact. Geographic and clustering protocols related to routing within WSNs may protect Wormhole attack specifically. The wormhole attack is still widely viewed as a challenge to that lacks adequate mitigation. **Effectiveness**: None to Partial	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: If encryption used it may produce a slight overhead in performance. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	**Threat Class**	**Threat Summary**	**Vulnerability Summary**	**CRIPAL**	**STRIDE**
Wireless Sensor Network Node	**WSNN-T6**	Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)	Physical Dynamic & Logical Dynamic	**Statement** : Sinkhole attacks:- Goal is to attract as much traffic as possible from a particular area via a compromised node, creating 'sinkhole' with the malicious node at the centre. **Entry Point**: Comms Channel **Impact**: M	**Statement** : This attack has it's grounding in making a compromised node look appealing to neighbouring nodes with respect to appearing to be a conduit to a promising routing path. **Probability**: M	C R I P A L	S T R I D

(3) ATTACKER		(4) COUNTERMEASURE BLOCK	
Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
C II C III	Non-Invasive Active & Passive.	**Statement** : Outsider attack prevented by link layer encryption & authentication using a globally shared key. Could use Public Key Elliptic Curve Cryptography (ECC) with a small footprint as key distribution for a globally shared symmetric key or use ECC Dig Sigs. Sun has Sizzle (SSSL) a form of SSL that uses ECC. To prevent 'Insider' attack, entities may be verified using public key cryptography - verification key pair to enable digital signing. **Effectiveness**: Partial to Total	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: If encryption used it may produce a slight overhead in performance. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Wireless Sensor Network Node	WSNN-T7	Logical OS: (TinyOS) & Logical Other (NesC a C derived language used to make TinyOS)	Logical Dynamic	**Statement** : TinyOS nesC Stack overflow: execution stack raids memory used for other purpose. Common source of crashes in embedded systems with little RAM & often lack an MMU. Not easy to diagnose - worst-case stack size encountered rarely (e.g. several interrupts signalled same time). **Entry Point**: Code Level **Impact**: M	**Statement** : If an attacker can change memory locations he can cause IC to execute code of his choosing. Stack overflow changes the return address on the stack. C and C++ programs are vulnerable to this attack. **Probability**: L	R A	D

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C II C III	Non-Invasive Active & Passive.	**Statement** : Undertake a peer code review. Also, check code parameters. If an overflow occurs because a large array is used in a function consider reducing the size of array so that the function can be executed. **Effectiveness**: Partial	**Time**: Test and implementation time goes up to incorporate these requirements. **Performance**: Nil. **Cost**: Cost of design & implementation increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat may have partial applicability to smart cards and the countermeasure may also have partial applicability.

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
Wireless Sensor Network Node	WSNN-T8	Physical Chip & Logical Other (JTAG Connector)	Logical Static & Dynamic	**Statement** : IEEE 1149.1 JTAG standard designed to assist testing. It can be used to read and write arbitrary code. **Entry Point**: JTAG Interface **Impact**: H	**Statement** : Many nodes examined by Becher, Benenson and Dornseif 2005 [24] had a JTAG connector on the node board easily accessible. Attackers with appropriate kit can take control of the WSN Node. **Probability**: H	C R I P A L	S T R I D E

(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
C I C II C III	Non-Invasive Active & Passive.	**Statement** : This attack is very similar to SCA/SCB-T5 for smart cards. Consider implementing the countermeasures highlighted in the table for the SCA/SCB-T5 threat. **Effectiveness**: Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Nil. **Cost**: Cost of design & manufacture increases to cover this countermeasure

(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)
Threat has total applicability to smart cards and the countermeasures are similar – See SCA/SCB-T5 on Test Mode Threat