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

Kevin Eagles, Konstantinos Markantonakis and Keith Mayes

Smart Card Centre
Information Security Group
Royal Holloway, University of London,
Egham, England TW20 0EX.
k.eagles@sensornets.co.uk
{k.eagles, k.markantonakis, keith.mayes}@rhul.ac.uk

Abstract. A threat analysis framework and methodology was developed by the authors to catalogue threats, vulnerabilities, attacks and countermeasures for smart cards (contact and contactless) and wireless sensor network node technologies. The goal of this research was to determine "Security Lessons" learned from the world of smart cards that may be applied to wireless sensor network nodes and vice versa.

Keywords: Sensor Networks, Security, Ubiquitous Networks, RFID, Smart Card Security, Security Models.

1 Introduction

Smart cards and wireless sensor network nodes (hereafter referred to as WSN nodes) are two functionally distinct technologies sharing similar design characteristics. Both have severe space and computational restrictions and require low levels of power to function.

Smart cards have evolved from being simple insecure data carriers, to quite sophisticated devices today (e.g., mobile cell phone SIM technology). There are many standards that govern the development and use of smart cards and many vendors in the market place.

Conversely, WSN nodes are a relatively new form of evolving technology and although products are widely available, there are only a few embryonic standards governing development and use [1].

With ever increasing miniaturisation and ubiquity of computing devices there may be overlapping areas within technologies such as smart cards and WSN nodes (and indeed PDAs, laptops and mobile cell phone technology too). The proposed framework and methodology for the systematic analysis of security issues within this paper may help to assess potential overlaps and/or convergences within technologies.

To enable this work, two high level objectives were established.

- 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.

The rest of this paper has the following structure: Section two outlines threat and attack models for smart cards. Section three outlines threat and attack models for WSN nodes. Section four discusses the framework and methodology established for the data capture phase of the study. Section 5 discusses the comparative threat analysis of the two technologies. Finally, section six provides conclusions and recommendations for further work.

2 Smart Card Threat and Attack Models

Historically, smart cards have endured many threats and attacks exposing vulnerabilities, however most of these threats now have effective countermeasures. Many smart cards have not been through a recognised security evaluation, however, it is important to note that some industries (e.g., banking/credit cards) have insisted that certain aspects of smart card technology are assessed through Common Criteria [2]. We believe that historically the drive to seek Common Criteria [2] evaluations has helped firm and mature security requirements and functionalities within many technologies.

2.1 Smart Card Definitions

A smart card consists of an integrated circuit with some form of tamper resistance, packaged and embedded within a card carrier. Overarching definitions of smart card technologies follow:

"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) [3]."

"The chip is embedded in a module which provides the capability for standardised connection to systems separate from the chip [3]."

The card carrier is usually made from plastic and typically conforms to ISO/IEC 7810:2003 [4] and ISO/IEC 7813:2006 [5].

Smart cards can be broken down into contact and contactless varieties.

Contact cards are typically in accordance with the standard ISO/IEC 7816 (parts 1-15) [6], which covers physical characteristics of the integrated circuit and also the electrical interface and connectivity for both power and data via a card reader.

Contactless cards can be broken down into two main areas, proximity cards and vicinity cards. Proximity cards are typically in accordance with ISO/IEC 14443-1:2000 (parts 1 to 4) [7]. Power and data are transferred via inductive coupling over a distance not exceeding 10cm. Vicinity cards are typically in accordance with ISO/IEC 15693 (parts 1 to 3) [8]. Power and data are transferred via inductive coupling over a distance not exceeding 1.2 metres.

Within this paper, the term smart card will be used to cover both contact and contactless smart cards (unless a distinction needs to be made).

2.2 Radio Frequency (RF) and Radio Frequency Identification (RFID) Definitions

Contactless smart cards utilise radio frequency fields for their communications and usually (although not always) as a source of power.

RFID devices are not restricted to card carriers and can be embedded into a range of objects, they are less sophisticated than contactless smart cards due to functional and cost requirements rather than technical limitations.

"RFID refers to procedures to automatically identify objects using radio waves [9]".

2.3 Smart Card Threats

We have derived Threat/Attack groups from the following research [10, 11]. These groups map effectively to popular generic attacker groupings

- Class I (Clever outsiders): Smart but lack sufficient knowledge of the system having access to only moderately sophisticated equipment. They exploit existing weaknesses rather than creating any. "Opportunist Attacker" (Hobbyist/Vandal/Minor Criminal possibly using widely available tools);
- Class II (Knowledgeable insiders): Substantial and specialised technical education and experience, understanding parts of the system and potential access to most of it. They have sophisticated tools and instruments for analysis. "Expert/Professional Attacker/Major Criminal" (Personal gain generally financially motivated, using tools adapted specifically for the purpose);
- Class III (Funded organisations): Specialist teams with related and complementary skills backed up with significant resources. Capable of in-depth analysis of the system, designing sophisticated attacks, and have the most advanced analysis tools available. They may use Class II adversaries as part of the attack team. "Sophisticated Attacker" (Intelligence Services, highly resourced Research Labs or very highly skilled Organised Crime).

2.4 Smart Card Attacks

This subsection will outline well known and established attacks on smart cards. Often an attacker is aiming to 'Reverse Engineer' the technology to establish how it works [10, 12]. The main objective is to identify the structure of the chip as well as detailed information on its internal operations.

Invasive Attacks 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. This is done by physical probing and/or physical modification of the chip.

Semi-Invasive Attacks Skorobogatov [12] describes semi-invasive attacks involving some depackaging to reach the chip's surface, however it is not necessary to break through the passivation layer to access the chip's interior (e.g., the use of light to induce a processing fault).

Non-Invasive Attacks This type of attack is aimed at retrieving sensitive data (e.g., keys) while observing a smart card 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.

Observation Attacks: Information Leakage and/or Cryptanalysis Kocher [13] described an attack on the RSA algorithm by conducting timing attacks on a CPU to count and log cycles between known events (e.g., measure the decryption times for several known cipher-texts) in order to obtain decryption keys.

Simple Power Analysis (SPA) is an analysis of power consumption to determine which set of CPU instructions are being processed and under which parameters. Differential Power Analysis (DPA) is similar to SPA but differs due to the measurement of power when known data is processed by the card and results are statistically analysed to look for patterns. Differential Electro-Magnetic (Radiation) Analysis (DEMA) looks at the electromagnetic emanation from the smart card to attempt to retrieve sensitive data. Differential Fault Analysis (DFA) aims to retrieve secret information from the card by inducing an error whilst a cryptographic calculation is being performed by the card. With the exception of DFA, these attacks are sometimes known as Side Channel attacks.

Protocol and/or Functionality attacks This type of attack looks for flaws in the protocol implementation. Techniques can be replay-attacks or interrupting the smart card while it is executing a command.

Software Attacks This type of attack is looking into software malfunctions of the smart card (e.g., software loading and badly formatted commands aiming to circumvent security mechanisms on the card).

Deficiency of Random Numbers An attacker may predict or obtain information about random numbers generated by the microcontroller because of poor quality entropy and/or seeding of the random numbers created.

Perturbation, Malfunction, State, Environmental Stress This involves operating the smart card outside of its normal operating conditions (e.g., increasing or decreasing operational temperatures) to attempt to deactivate security features or disclose information.

3 WSN Node Threat and Attack Models

Although there is research on Java Card 3.0 [14] and TCP/IP and there has been research with secure distributed computing on a Java Card grid [15], the typical usage of smart cards today is not as networked devices; conversely a WSN node is a networked device.

3.1 Wireless Sensor Network Nodes Definitions

The term 'Mote' (originally labelled COTS Dust [16]) is often interchangeable with the notion of a sensor node or wireless network node. For this paper, a WSN node refers to a device consisting of an integrated circuit with a microprocessor and memory which is able to function as an element within a network, passing data onto other devices through wireless communications.

"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 [17]".

3.2 WSN Node Threats

Initially, many WSN routing protocols were vulnerable to targeted attacks, to some degree this is still the case. Although there are many 'open' routing protocols today, some implementations use proprietary routing protocols and algorithms.

Many papers categorise threats as being network Outsiders or Insiders [18, 19, 20]; further, attackers are categorised as Mote-class attackers or laptop-class attackers [18, 19]. Mote-class attackers are perceived to have access to only a few WSN nodes to exploit and derive weaknesses; they also have an attack surface affecting only 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).

3.3 WSN Node Attacks

WSN nodes have limited storage, processing and bandwidth capability and power (battery) management is essential [17].

C. Karlof and D. Wagner 2003 [18] 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."

Attacks tend to focus on the nature of WSN nodes and known vulnerabilities:

- Denial of Service attacks on the device by running down the power source (battery) through continuous operation;
- Denial of Service through Radio Frequency jamming so data can not be transmitted or received;
- Most (if not all) devices do not seem to have a crypto-coprocessor, thus any encryption creates a processing overhead for already constrained capabilities;
- WSN node Integrated Circuits are not tamper resistant, any secret information on the chip may be susceptible to standard smart card attacks.

We were not able to find any references for WSN node Common Criteria [2] evaluated products or Protection Profiles to enable evaluations. However, NIST are involved with the US Department of Homeland Security in the development of advanced CBRNE - (chemical, biological, radiological, nuclear, and explosive) detection sensors that could provide the underpinnings for a national sensor network [21, 22].

4 Threat, Vulnerability, Attacker and Countermeasure Table

To capture and categorise data, we created a framework and methodology in the form of a TVAC Table(Fig. 1).

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 State & Dynamic Logical State & 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 execution in EEPROM or RAM. EEPROM has write/erase disallowed by setting page to protected 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							

Fig. 1. A Sample Threat, Vulnerability, Attack and Countermeasure (TVAC) Table

The TVAC table has five main blocks with subsections. It has two initial columns categorising the technology and its unique identifier (TUID). A contact smart card is prefixed SCA, a contactless smart card prefixed SCB and a WSN node prefixed WSNN.

4.1 Threat Block

In the context of this project, we have defined a threat as being, "an objective a foe might try to realise in order to misuse a target or asset."

Target and/or Asset: The following categories are used to categorise the threat type:

- Physical - Chip; Physical - Other;
- Logical - Operating System; Logical - Platform;
- Logical - Application; Logical - Other;
- Communications Bearer (e.g., Physical Card Reader, RF or RFID);
- Other.

Threat Class: The classification of the threat type as follows:

- Physical Static (e.g., No Power to Hardware);
- Physical Dynamic (e.g., Power to Hardware);
- Logical Static (e.g., No Power source active, but using glitches, light, temperature variances to affect software before power activated);
- Logical Dynamic (e.g., Power to Software);
- Social (e.g., Social Engineering);
- Policy (e.g., Weakness in Governing Policies);
- Other.

Threat Summary: This includes a 'Statement' of the Threat indicating 'Entry Point' and rating the 'Impact' of the Threat from High, Moderate or Low.

4.2 Vulnerability Block

In the context of this project, we have defined a vulnerability as being, "a specific means by which a threat can be executed via an unmitigated attack path."

Vulnerability Summary: A 'Statement' of the Vulnerability, with a 'Probability' rating from High, Moderate or Low.

CRIPAL: is an acronym and methodology we have established to cover high level 'primary' security goals. The acronym stands for: (C)onfidentiality; (R)eliability; (I)ntegrity; (P)rivacy; (A)vailability; (L)egitimate Use.

STRIDE: a method used by Microsoft [23] to categorise threats during software development. This adds low level granularity to 'CRIPAL' area. It stands for: (S)poofing, (T)ampering, (R)epudiation, (I)nformation disclosure, (D)enial of Service, (E)levation of Privilege

4.3 Attacker Block

In the context of this project, we have defined an attacker as being, "the entity that is exploiting a vulnerability to establish a threat."

Attacker Group: As stated earlier they consist of:

- Class I (clever outsiders) - "Opportunist Attacker";
- Class II (knowledgeable insiders) - "Expert/Professional Attacker";
- Class III (funded organisations) - "Sophisticated Attacker".

Attack Class: This consists of:

- Invasive Active (e.g., Cutting new tracks);
- Invasive Passive (e.g., Microprobing to observe not to modify);
- 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).

4.4 Countermeasure Block

In the context of this project, we have 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."

Countermeasure Summary: A 'Statement' of the Countermeasure, indicating its 'Effectiveness' represented by the following options: Total (Complete Effectiveness); Partial (Some Effectiveness); None

Overhead of Countermeasure on Time, Performance & Cost: This looks at what impact the countermeasure may bring if implemented.

4.5 Applicability to WSN Nodes/Smart Cards

This is an assessment of whether any security issues and mitigation can be applied from one technology type to the other represented by the following options: Total (Complete Effectiveness); Partial (Some Effectiveness); or None

5 Comparative Threat Analysis Assessment Matrices

Fig. 2 and Fig. 3 below illustrate Comparative Threat Analysis Assessment Matrices designed by the authors, which use data from populated TVAC tables.

These matrices record any commonality/applicability from one technology to the other. Ten threats, SCA-T1 to SCA-T10, have been explored for contact smart cards and these have also been applicable to contactless smart cards too as SCB-T1 to SCB-T10 respectively. Four additional threats have been applied to contactless smart cards as SCB-T11 to SCB-T14, giving contactless smart cards a count of fourteen. Eight threats were listed for WSN nodes (WSNN-T1 to WSNN-T8).

Key to Matrices:

- SCA/B: Threat and/or Countermeasure is applicable to both Contact and Contactless cards and hence are referenced as so;
- Contact Smart Card: has SCA prefix with threat reference following - e.g., SCA-T1;
- Contactless Smart Card: has SCB prefix with threat reference following - e.g., SCB-T1;
- WSN Node: has WSNN prefix with threat reference following - e.g., WSNN-T1;
- $\surd(T) = TotalMatch; \surd(P)to(T) = PartialtoTotalMatch;$ $\surd(P) = PartialMatch; \times(N) = NoMatch.$

Contact & Contactless Smart Card Threats

Smart Card Threat Reference	High Level Threat Description	Threat Applicable to WSN Nodes	Counter-measure Applicable to WSN Nodes
SCA/B-T1	IC Reverse Engineering	✓(T)	✓(P) to (T)
SCA/B-T2	Microprobing	✓(T)	✓(P) to (T)
SCA/B-T3	Side Channel Attacks: SPA, DPA, EM	✓(T)	✓(P) to (T)
SCA/B-T4	DFA	✓(T)	✓(P)
SCA/B-T5	Test Mode Function	✓(T)	✓(T)
SCA/B-T6	Memory Mgt & Firewalling	✓(T)	✓(P)
SCA/B-T7	Data Remanence	✓(T)	✓(P) to (T)
SCA/B-T8	Governing Policies and Acts	✓(T)	✓(P)
SCA/B-T9	Random No. Generation	✓(T)	✓(P) to (T)
SCA/B-T10	Smart Card Mgt &/or Database Mgt System	✓(P)	✓(P)
SCB-T11	Interception of RF Comms	✓(P)	✓(P)
SCB-T12	Malicious Masquerading Reader	✓(P)	✓(P)
SCB-T13	Reach-back to Attack Enterprise Network	✓(P)	✓(P)
SCB-T14	Jamming RF Comms	✓(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

Fig. 2. Smart Cards Compared to WSN Nodes Matrix

The following is a summarised breakdown of our findings:

SCA/B-T1: Smart cards are susceptible to reverse engineering of the Integrated Circuit (IC). Possible countermeasures include an active shield, mesh or

sensor that once affected renders the IC unusable, destroying data on the chip and then shutting down operations. The use of environmental sensors within the chip would have a similar affect. Most smart cards have tamper resistance, most if not all WSN nodes do not. Although some WSN nodes are ruggedised for use in harsh environments, this offers no protection from known threats. Smart card tamper resistance techniques should be transferable to WSN nodes.

SCA/B-T2: Smart cards are susceptible to Microprobing. This attack and its countermeasure are closely related to SCA/B-T1 above.

SCA/B-T3 and SCA/B-T4: Side Channel attacks like SPA, DPA or EM analysis may apply to WSN nodes. Randomness and scrambling countermeasures used within smart cards maybe transferable to WSN nodes. The same stands for DFA which is SCA/B-T4.

SCA/B-T5: This maps to WSNN-T8 and involves a Test Mode which smart card and WSN node chips have [24]. It is possible to unlock the Test Mode function and as such get full logical control of the IC. Smart cards mitigate this by requesting authentication to the Test Mode function with a failure leading to chip inoperability.

SCA/B-T6: Some smart cards undertake a form of internal firewalling with memory management to prevent a protocol or functionality attack. WSN nodes do not have this protection, but could learn from smart card countermeasures.

*SCA/B-T7:*Skorobogatov has undertaken research in the field of Data Remanence. The countermeasures he proposes [12] for the protection of smart cards should be applicable to WSN nodes.

SCA/B-T8: Policies. There is a need for clear operating policies such as CONOPS, CONUSE and CONEMP, and adherence to 'laws of the land' (e.g., UK Data Protection Act 1998). Many publications also mention asymmetric keys within smart cards and WSN nodes and public key certificates; however these publications do not mention a Certificate Policy or Key Management Policy which would underpin the use of keys or certificates.

SCA/B-T9: This threat involves weakness in random number generation and many smart cards mitigate this through crypto-coprocessors. WSN nodes do not appear to have crypto-coprocessors and their addition may help with processing capability.

SCA/B-T10: This relates to a Smart Card Management System and/or a Database Management System. These are required for effective management of smart cards but also provide a path for a reach-back attack from a device like a smart card into an Enterprise network. This may apply to WSN nodes, but we have seen no mention of a WSN Node Management System -which in itself seems vulnerability.

SCB-T11 and SCB-T12: These threats involve the interception of messages via RF communications and have partial applicability to WSN nodes. SCB-T11 is an eavesdropping threat between reader & transponder [25]. SCB-T12 is similar but involves a malicious masquerading reader. The countermeasures in both cases are not totally effectively for WSN nodes.

SCB-T13: Potential RFID attacks with SQL, buffer overrun and threat of reach-back to Enterprise networks [26]. A range of RF/RFID exploits may be applied from smart cards/RFIDs to WSN nodes and proposed countermeasures [26] may mitigate these threats.

SCB-T14: Denial of Service (DoS) attacks on contactless smart cards by jamming communications signals. There may be significant similarities and applicability to WSN nodes and their communications.

WSN Node Threats

WSN Node Threat Reference	High Level Threat Description	Threat Applicable to Smart Cards (state whether contact or contactless)	Counter-measure Applicable to Smart Cards (state whether contact or contactless)
WSNN-T1	Dos, CoS & DCoS	✓(P) SCB	✓(P) SCB
WSNN -T2	Routing Data	×(N)	×(N)
WSNN -T3	Sybil & Sizzle	✓(P) SCA/B	✓(P) SCA/B
WSNN -T4	Routing Data	×(N)	×(N)
WSNN -T5	Routing Data	×(N)	×(N)
WSNN -T6	Routing Data	×(N)	×(N)
WSNN -T7	Possible 'C' Weaknesses in nesC	✓(P) SCA/B	✓(P) SCA/B
WSNN -T8	IEEE 1149.1 JTAG standard interface	✓(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

Fig. 3. WSN Nodes Compared to Smart Cards Matrix

WSNN-T1: DoS which may have a partial applicability to contactless smart cards (e.g., Jamming). We also apply a new term 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 undergo continuous operations they will drain the battery. 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. An attack spread over a Wireless Sensor Network is a Distributed Cessation of Service (DCoS) attack.

WSNN-T2: This involves routing data between nodes and hence as such has no current applicability to the typical use of smart cards today, this may change in the near future with Java Card 3.0 and grid computing concepts for smart cards [14, 15].

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 [27] for WSN nodes may secure communications enabling confidentiality and if used with TLS meet integrity requirements too.

WSNN-T4 through to WSNN-T6: This involves routing data between nodes and hence as such has no applicability to smart cards. See WSNN-T2 above.

WSNN-T7: This involves weaknesses in the underlying programming languages. nesC [28] which is a C derivative used to create Tiny OS (a leading operating system for WSN nodes). The applicability to smart cards is minimal but may relate to native functions that smart card manufacturers utilise within their cards before installation of widespread operating systems or platforms.

WSNN-T8: This threat and countermeasure maps directly onto SCA/B-T5. Many nodes examined by Becher, Benenson and Dornseif had a JTAG connector on the node board easily accessible [24]. Attackers with appropriate kit may take control of the WSN Node.

6 Conclusion

This paper proposed a framework and methodology for classifying and analysing threats against smart cards and WSN nodes. Indications are that many attacks against smart card integrated circuits apply to WSN nodes and some WSN node RF/Communications attacks may apply to contactless smart cards and RFIDs.

Tamper resistance features within smart cards should be considered for WSN nodes. We suggest the need to establish High, Medium and Low assurance benchmarks for WSN nodes offering differing levels of security relative to use. Many technologies have matured through schemes like Common Criteria [2]and the production of Protection Profiles may help focus the development of security within WSN nodes.

Threats within WSN nodes shared with smart cards (specifically contactless smart cards) lie within the Radio Frequency space. However, communication and routing attacks are more effective against WSN nodes compared to smart cards due to the 'networked' nature of these attacks.

This paper has also defined two new definitions for attacks, 'Cessation of Service (CoS)' and/or a 'Distributed Cessation of Service (DCoS)' which may have wider applicability than just WSN nodes.

Overall, we feel that this 'path-finder' research has established the need for thorough scientific testing to prove or disprove the assertions made in this paper.

Other research areas that may closely tie into this research are suggested below:

Investigate RF/Communications threats between WSN nodes and Mobile Cell Phones for similarities (e.g., Bluetooth [29], IEEE 802.15.4 [1] and also ZigBee [30]).

A study of WSN nodes and sensor technologies in airports to assist baggage and passenger screening.

An assessment of smart card services/functionalities such as Global Platform [31] and Card Manager [32], Java Card Runtime Environment (JCRE) [33] and smart card APIs to determine applicability to WSN nodes.

The proposed framework and methodology in this paper may help to assess any shared security issues between Java Card 3.0 [13], secure distributed

computing on a Java Card grid [14] and also the use of Active-RFID [34] and Passive-RFID [35] (which have an onboard power supply) and WSN nodes.

Authentication of WSN nodes is an often quoted security challenge [36, 37, 38]. The exploration of Attribute Certificates [39] and/or Kerberos tickets may enable novel secure authentication methods.

We are interested in investigating the potential for a secure authentication and routing protocol similar to IPSEC which we have provided a working label of KAFKA (Know Allies & Family, Know Adversaries) to suit the adaptive nature of Wireless Sensor Networks.

7 References

1. Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4 (Second Edition),
http://shop.ieee.org/ieeestore/Product.aspx?product_no=SP1150
2. Common Criteria website: http://www.commoncriteriaportal.org
3. Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP) Version 3.0 9 (September 2001)
4. JTC 1/SC 17: ISO/IEC 7810:2003 Identification cards - Physical characteristics (December 2005)
http://http://www.iso.org/iso/en/prods-services/ISOstore/store.html
5. JTC 1/SC 17: ISO/IEC 7813:2006 Information technology -Identification cards – Financial transaction cards (June 2006)
{http://http://www.iso.org/iso/en/prods-services/ISOstore/store.html
6. JTC 1/SC 17: ISO/IEC 7816-1 to 15 Identification cards – Integrated circuit(s) cards with contacts (Parts 1 to 15)
http://http://www.iso.org/iso/en/prods-services/ISOstore/store.html
7. JTC 1/SC 17: ISO/IEC 14443-1 to 4 Identification cards – Contactless integrated circuit(s) cards – Proximity cards (Parts 1 to 4)
http://http://www.iso.org/iso/en/prods-services/ISOstore/store.html
8. JTC 1/SC 17: ISO/IEC 15693-1to 3 Identification cards – Contactless integrated circuit(s) cards – Vicinity cards (Parts 1 to 3)
http://http://www.iso.org/iso/en/prods-services/ISOstore/store.html
9. German Federal Office for Information Security (BSI): Security Aspects and Prospective Applications of RFID Systems (2004)
10. Anderson, R., Kuhn, M.: Low Cost Attacks on Tamper Resistant Devices (1997)
11. Abraham, D.G., Dolan, G.M., Double, G.P., Stevens, J.V.: Transaction Security System. IBM Systems Journal v 30 no 2 (1991) 206-229
12. Skorobogatov, S.P.: Semi-invasive attacks - A new approach to hardware security analysis. PhD Thesis UCAM-CL-TR-630 ISSN 1476-2986 (April 2005)
13. Kocher, P. C.: Timing attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other systems. Crytpography Research Inc. CRYPTO (1996)
14. Java Card Forum: Working status & Deliverables Presentation (2005)
http://www.javacardforum.org/03_documents/00_documents/marketingpre

sentationgeneral.pdf
15. Chaumette, S., Grange, P., Karray, A., Sauveron, D.: Secure distributed computing on a Java Card Grid - 19th IEEE International Parallel and Distributed Processing Symposium (IPDPS'05), 7th International Workshop on Java for Parallel and Distributed Computing (2005)
16. Hollar, S.: Cots Dust Masters Degree Thesis (1996)
http://www-bsac.eecs.berkeley.edu/archive/users/hollar-seth/publications/cotsdust.pdf
17. Tubaishat, M., Madria, S.: Sensor Networks: An Overview. IEEE Potentials, 22 (2003), 20–23.
18. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier Article (2003)
19. Shi, E., Perrig, A.: Designing Secure Sensor Networks. IEEE Publication (2001). http://www.cs.ucsb.edu/~suri/Spr05/generalB.pdf
20. Benenson, Z., Freiling, F. C.: On the Feasibility and Meaning of Security in Sensor Networks. 4th GI/ITG KuVS Fachgesprch "Drahtlose Sensornetze", (2005)
http://user.it.uu.se/~zina/publications/security-taxonomy.pdf
21. Healy, W.: Standards and Test Methods for Sensor Networks and Alert Systems (2007)
http://www2.bfrl.nist.gov/projects/projcontain.asp?cc=8634508431
22. Official Website of the US Govt. Sensornet Project
http://www.sensornet.gov/
23. Swiderski, F., and Snyder, W.: Threat Modelling, Microsoft Press (2004) 259
24. Becher, A., Benenson, Z., Dornseif, M.: Tampering with Motes: Real World Physical Attacks on Wireless (2005)
25. Finke, T., Kelter,H.: Abhrmglichkeiten der Kommunikation zwischen Lesegert und Transponder am Beispiel eines ISO14443 - Systems. BSI, (2004)
http://www.bsi.de/fachthem/rfid/Abh_RFID.pdf
26. Rieback, M. R., Crispo, B., Tanenbaum, A. S.: Is your cat infected with a computer virus. Vrije Universiteit Amsterdam. (2006)
27. SUN's Sizzle (SSSL) Webserver for small devices
http://research.sun.com/spotlight/2004-12-20_vgupta.html
28. Brewer, E., Culler, D., Gay, D., Levis, P., von Behren, R., Welsh, M.: nesC: A Programming Language for Deeply Networked Systems - (2004)
http://nescc.sourceforge.net/
29. Official Website for the Bluetooth Short Range Wireless Connectivity Standardb http://www.bluetooth.com/bluetooth/
30. ZigBee Alliance Official Website. http://www.zigbee.org/en/index.asp
31. Global Platform Official Website. http://www.globalplatform.org/
32. Bernabeu, G.: GlobalPlatform Mobey Forum 2005 Presentation: Page 15 Card Manager Responsibilities (2005)
http://www.globalplatform.org/uploads/Mobey%20Forum_Oct2005.pdf
33. Java Card Technology Datasheet (incl. JCRE)

http://java.sun.com/products/javacard/datasheet.html
34. DoD Radio Frequency Identification Update: Enterprise Data Collection Across the Supply Chain (June 14, 2006).
http://www.dla.mil/j-6/AIT/Files/Conferences/AirForce_Supply_Chain_AIT_Forum/2006_06_13/Day2/Smith%20-%20OSD%20RFID.pdf
35. United States Department of Defense Suppliers' Passive RFID Information Guide ver.8.0 (2005)
http://www.acq.osd.mil/log/rfid/DoD_Suppliers'_Passive_RFID_Information_Guide_v8.0.pdf
36. Shaikh, R. A., Lee, S., Song, Y. J., Zhung, Y.: Securing Distributed Wireless Sensor Networks: Issues and Guidelines (2006) 226-231
37. Chan, H., Perrig, A.: Security and Privacy in Sensor Networks. IEEE Publication Computer, vol. 36, no. 10, (2003) 103-105
38. Muftic, S., Chang, C.: Security in Wireless Sensor Networks: Status, Problems, Current Technologies and Trends. Enisa Quarterly No. 4 (2006) 5-6
39. Arnab, A., Hutchison, A.: Ticket Based Identity System for DRM (2006)