wistp'07
Workshop in Information Security Theory and Practices Smart Cards, Mobile and Ubiquitous Computing Systems

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

www.sensornets.co.uk

Smart Card Centre
Royal Holloway

Royal Holloway
University of London

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.

RESEARCH AREA

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.

OUTCOME

This research proposes 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.

1. Project Outline

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.

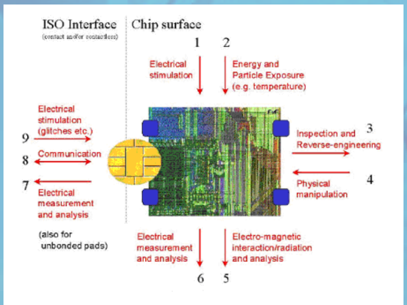
Smart cards have evolved from being simple insecure data carriers, to quite sophisticated devices today (e.g., mobile cell phone SIM technology). There are many standards that govern the development and use of smart cards and many vendors in the market place.

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.

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.

2. Smart Card Background

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. We believe that historically the drive to seek Common Criteria evaluations has helped firm and mature security requirements and functionalities within many technologies.

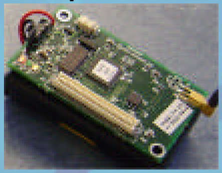

ISO Interface
(contact and/or contactless)
Chip surface
1
2
Electrical stimulation
Energy and Particle Exposure (e.g. temperature)
Electrical stimulation (glitches etc.)
9
Communication
8
7
Electrical measurement and analysis
(also for unbonded pads)
Inspection and Reverse-engineering
3
Physical manipulation
4
Electrical measurement and analysis
Electro-magnetic interaction/radiation and analysis
6
5

3. WSN Node Background

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

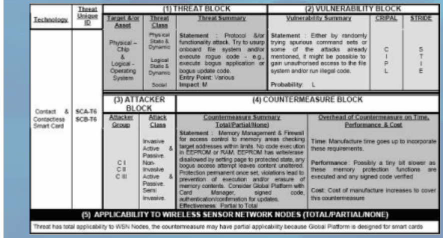
The term 'Mote' is often interchangeable with the notion of a sensor node or wireless network node. For this paper, a WSN node refers to a device consisting of an integrated circuit with a microprocessor and memory which is able to function as an element within a network, passing data onto other devices 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 [Tubaishat & Madria 2003]".



4. TVAC Table

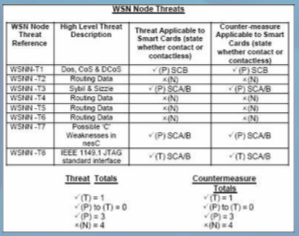
To capture and categorise data, we created a framework and methodology in the form of a Threat, Vulnerability, Attacker and Countermeasure (TVAC) table.



<table>
<tr><th rowspan="2">Technology</th><th rowspan="2">Threat Unique ID</th><th colspan="3">(1) THREAT BLOCK</th><th colspan="3">(2) VULNERABILITY BLOCK</th></tr>
<tr><th>Target &amp;/or Asset</th><th>Threat Class</th><th>Threat Summary</th><th>Vulnerability Summary</th><th>CRIPAL</th><th>STRIDE</th></tr>
<tr><td rowspan="4">Contact &amp; Contactless Smart Card</td><td rowspan="4">SCA-T6
SCB-T6</td><td>Physical – Chip &amp; Logical - Operating System</td><td>Physical Static &amp; Dynamic
Logical Static &amp; Dynamic
Social</td><td><b>Statement</b> : Protocol &amp;/or functionality attack. Try to usurp onboard file system and/or execute rogue code - e.g., execute bogus application or bogus update code.
<b>Entry Point</b>: Various
<b>Impact</b>: M</td><td><b>Statement</b> : 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</td><td>C
I
P
L</td><td>S
T
I
E</td></tr>
<tr><th colspan="2">(3) ATTACKER BLOCK</th><th colspan="4">(4) COUNTERMEASURE BLOCK</th></tr>
<tr><th>Attacker Group</th><th>Attack Class</th><th colspan="2">Countermeasure Summary Total/Partial(None)</th><th colspan="2">Overhead of Countermeasure on Time, Performance &amp; Cost</th></tr>
<tr><td>C I
C II
C III</td><td>Invasive Active &amp; Passive.
Non-Invasive Active &amp; Passive.
Semi Invasive.</td><td colspan="2"><b>Statement</b> : Memory Management &amp; 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.
<b>Effectiveness</b>: Partial to Total</td><td colspan="2"><b>Time</b>: Manufacture time goes up to incorporate these requirements.
<b>Performance</b> : Possibly a tiny bit slower as these memory protection functions are executed and any signed code verified
<b>Cost</b>: Cost of manufacture increases to cover this countermeasure</td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has total applicability to WSN Nodes, the countermeasure may have partial applicability because Global Platform is designed for smart cards</td></tr>
</table>

5. Comparative Assessments

These matrices record any commonality or 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).



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

6. Conclusion

This research proposes a novel framework and methodology for classifying and analysing threats that may have wider applicability (e.g., Java Card 3.0 & RFIDs).

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. High, Medium and Low assurance Tamper resistance features within smart cards should be considered for WSN nodes.

This paper has also defined two new definitions for attacks, 'Cessation of Service (CoS)' and/or a 'Distributed Cessation of Service (DCoS)'

Suggested further areas of research:

RF/Communications threats between WSN nodes and Mobile Cell Phones.

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 and Card Manager, Java Card Runtime Environment (JCRE) and smart card APIs to determine applicability to WSN nodes.

Alternative Authentication mechanisms for WSN nodes: (Attribute Certificates/Kerberos tickets). We are interested in investigating 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.