Populated TVAC Tables

<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 &/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 & Contactless Smart Card</td><td rowspan="4">SCA-T1
SCB-T1</td><td>Physical - Chip</td><td>Physical Static & Dynamic

Logical Static & Dynamic</td><td>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</td><td>Statement : Use of etching, microscope, photography and image processing and microprobes to study the build and workings of the IC.

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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Invasive Active Passive.
Non-Invasive Active & Passive.
Semi Inv</td><td colspan="2">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</td><td colspan="2">Time: Manufacture time goes up to incorporate these requirements.

Performance : Nil

Cost: Cost of design & 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 and the countermeasure may have partial to total applicability</td></tr>
</table>

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

<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 &/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="5">Contact & Contactless Smart Card</td><td rowspan="5">SCA-T4
SCB-T4</td><td>Physical - Chip</td><td>Physical Static & Dynamic

Logical Static & Dynamic</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><td colspan="6"></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 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.</td></tr>
</table>

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
Contact & Contactless Smart Card	SCA-T6 SCB-T6

(1) THREAT BLOCK

Target &/or Asset	Threat Class	Threat Summary
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

(2) VULNERABILITY BLOCK

Vulnerability Summary	CRIPAL	STRIDE
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

Attacker Group	Attack Class
C I C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.

(4) COUNTERMEASURE BLOCK

Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost
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

<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 &/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="5">Contact & Contactless Smart Card</td><td rowspan="5">SCA-T7
SCB-T7</td><td>Physical - Chip</td><td>Physical Static & Dynamic

Logical Static & Dynamic</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Invasive Active & Passive.
Non-Invasive Active & Passive.
Semi Invasive.</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><td colspan="6"></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 and the countermeasure may have partial to total applicability [22]</td></tr>
</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 &/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="5">Contact & Contactless Smart Card</td><td rowspan="5">SCA-T8
SCB-T8</td><td>Other: Integrity of Organisation</td><td>Social
Policy</td><td>Statement : Possible that underpinning smart card policy weak and exposes the company to malicious use

Entry Point: Organisation’s IT System

Impact: M</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C I
C II
C III</td><td>Non-Invasive
Passive</td><td colspan="2">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</td><td colspan="2">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.</td></tr>
</table>

(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

Technology	Threat Unique ID	(3) ATTACKER BLOCK		(4) COUNTERMEASURE BLOCK	
		Attacker Group	**Attack Class**	**Countermeasure Summary Total/Partial/None)**	**Overhead of Countermeasure on Time, Performance & Cost**
Contact & Contactless Smart Card	**SCA-T9 SCB-T9**	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.

<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 &/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="5">Contact & Contactless Smart Card</td><td rowspan="5">SCA-T10
SCB-T10</td><td>Other:
Smart Card Management System

and/or Enterprise Database Management System (DBMS)</td><td>Logical Static & Dynamic

Social

Policy</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.
.</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO WIRELESS SENSOR NETWORK NODES (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">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.</td></tr>
</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 &/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">Contactless Smart Card</td><td rowspan="4">SCB-T11</td><td>Commun-ication Bearer: (between contactless card and reader device)</td><td>Physical Dynamic and Logical Dynamic</td><td>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</td><td>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</td><td>C
I
P
L</td><td>S
T
I
E</td></tr>
<tr><th colspan="2">(3) ATTACKER</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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">Time: Manufacture time goes up to incorporate these requirements.

Performance : Nil

Cost: Cost of design & 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 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.</td></tr>
</table>

Technology	Threat Unique ID	(1) THREAT BLOCK: Target &/or Asset	(1) THREAT BLOCK: Threat Class	(1) THREAT BLOCK: Threat Summary	(2) VULNERABILITY BLOCK: 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: Attacker Group	(3) ATTACKER BLOCK: Attack Class	(4) COUNTERMEASURE BLOCK: 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.

<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 &/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">Contactless Smart Card</td><td rowspan="4">SCB-T13</td><td>Other: (Threat to backend middleware systems supporting RFID Devices)</td><td>Physical Dynamic and Logical Dynamic</td><td>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</td><td>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</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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">Time: Manufacture time goes up to incorporate these requirements.

Performance : Nil

Cost: Cost of design & 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 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.</td></tr>
</table>

Technology	Threat Unique ID	(1) THREAT BLOCK: Target &/or Asset	(1) THREAT BLOCK: Threat Class	(1) THREAT BLOCK: Threat Summary	(2) VULNERABILITY BLOCK: Vulnerability Summary	(2) VULNERABILITY BLOCK: CRIPAL	(2) VULNERABILITY BLOCK: 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: Attacker Group	(3) ATTACKER BLOCK: Attack Class	(4) COUNTERMEASURE BLOCK: Countermeasure Summary Total/Partial/None)	(4) COUNTERMEASURE BLOCK: 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.

<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 &/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="5">Wireless Sensor Network Node</td><td rowspan="5">WSNN-T2</td><td>Commun-ications bearer: (Routing Protocol) & Logical Other: (data within node)</td><td>Physical Dynamic & Logical Dynamic</td><td>Statement : Spoof, Alter, or Replay WSN Routing Information.

Entry Point: Comms Channel

Impact: H</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information</td></tr>
</table>

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]

<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 &/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="5">Wireless Sensor Network Node</td><td rowspan="5">WSNN-T4</td><td>Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)</td><td>Physical Dynamic & Logical Dynamic</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
I
D</td></tr>
<tr><th colspan="2">(3) ATTACKER</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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">Time: Test and implementation time goes up to incorporate these requirements.

Performance : Nil.

Cost: Cost of design & implementation increases to cover this countermeasure</td></tr>
<tr><th colspan="6">(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information</td></tr>
</table>

<table>
<tr><th rowspan="2"><u>Technology</u></th><th rowspan="2"><u>Threat Unique ID</u></th><th colspan="3">(1) THREAT BLOCK</th><th colspan="3">(2) VULNERABILITY BLOCK</th></tr>
<tr><th><u>Target &/or Asset</u></th><th><u>Threat Class</u></th><th><u>Threat Summary</u></th><th><u>Vulnerability Summary</u></th><th><u>CRIPAL</u></th><th><u>STRIDE</u></th></tr>
<tr><td rowspan="5">Wireless Sensor Network Node</td><td rowspan="5">WSNN-T5</td><td>Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)</td><td>Physical Dynamic & Logical Dynamic</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D</td></tr>
<tr><th colspan="2">(3) ATTACKER</th><th colspan="4">(4) COUNTERMEASURE BLOCK</th></tr>
<tr><th><u>Attacker Group</u></th><th><u>Attack Class</u></th><th colspan="2"><u>Countermeasure Summary Total/Partial/None)</u></th><th colspan="2"><u>Overhead of Countermeasure on Time, Performance & Cost</u></th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information</td></tr>
</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 &/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">Wireless Sensor Network Node</td><td rowspan="4">WSNN-T6</td><td>Commun-ications bearer: (Routing Protocol) & Logical Other: (Attempt to attack data flow)</td><td>Physical Dynamic & Logical Dynamic</td><td>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</td><td>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</td><td>C R I P A L</td><td>S T R I D</td></tr>
<tr><th colspan="2">(3) ATTACKER</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 & Cost</th></tr>
<tr><td>C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">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</td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has no applicability to smart cards because smart cards are not a networked device and hence do not route information</td></tr>
</table>

		(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
Technology	**Threat Unique ID**	**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.

<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 &/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="5">Wireless Sensor Network Node</td><td rowspan="5">WSNN-T8</td><td>Physical Chip & Logical Other (JTAG Connector)</td><td>Logical Static & Dynamic</td><td>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</td><td>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</td><td>C
R
I
P
A
L</td><td>S
T
R
I
D
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 & Cost</th></tr>
<tr><td>C I
C II
C III</td><td>Non-Invasive Active & Passive.</td><td colspan="2">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</td><td colspan="2">Time: Manufacture time goes up to incorporate these requirements.

Performance : Nil.

Cost: Cost of design & manufacture increases to cover this countermeasure</td></tr>
<tr><td colspan="6"></td></tr>
<tr><th colspan="8">(5) APPLICABILITY TO SMART CARDS (TOTAL/PARTIAL/NONE)</th></tr>
<tr><td colspan="8">Threat has total applicability to smart cards and the countermeasures are similar – See SCA/SCB-T5 on Test Mode Threat</td></tr>
</table>