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

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

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

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

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

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

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

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

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

The blocks are as follows: -

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

A walkthrough description of the TVAC Table now follows.

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

5.2.1 Technology Column

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

- Contact Smart Card
- Contactless Smart Card
- WSN Node

5.2.2 Threat Unique Identifier (TUID) Column

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

TUID referencing is as follows: -

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

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

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

A breakdown of each block now follows: -

5.2.3 THREAT BLOCK

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

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

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

5.2.3.1 Target and/or Asset

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

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

5.2.3.2 Threat Class

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

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

5.2.3.3 Threat Summary

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

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

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

5.2.4 VULNERABILITY BLOCK

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

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

5.2.4.1 Vulnerability Summary

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

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

5.2.4.2 CRIPAL

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

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

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

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

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

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

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

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

5.2.4.3 STRIDE

STRIDE is a method used by Microsoft [19] to help categorise threats during software development. In the context of this project, STRIDE helps to add a low level granularity to the previous 'CRIPAL' column. Similarly to CRIPAL

above, any of the letters that make up the STRIDE acronym can be used as an entry within the TVAC table.

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

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

Table 2. STRIDE Table.

5.2.5 ATTACKER BLOCK

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

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

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

5.2.5.1 Attacker Group

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

"Class I (= clever outsiders): They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately

sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.

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

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

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

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

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

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

5.2.5.2 Attack Class

These are tied to Threat section: -

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

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

Attacks can be either passive or active:-

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

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

Semi-invasive attacks [22] involve some depackaging to reach the chip's surface, however it is not necessary to break through the passivation layer to gain physical access to the chip's interior.
Many attacks can be blended, i.e. which means that there is a potential for mixed threats which are potentially more effective – especially if it is a form of avalanche attack.

5.2.6 COUNTERMEASURE BLOCK

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

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

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

5.2.6.1 Countermeasure Summary

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

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

5.2.6.2 Overhead of Countermeasure on Time, Performance & Cost

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

5.2.7 APPLICABILITY to WSN NODES/SMARTCARDS

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

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

- Total – Complete Applicability

- Partial – Some Applicability
- None – No Applicability

5.3 Section Summary

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

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