WISTP ’07 – 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, Royal Holloway University of London
www.sensornets.co.uk k.eagles@sensornets.co.uk
{k.markantonakis, keith.mayes}@rhul.ac.uk

Presentation Structure

- Background to Research
- Objectives of Research
- Technology Definitions
- Security Analysis
- Results
- Conclusion
- Additional Information and Resources

Authors' Backgrounds

- Kevin Eagles:
  - UK MOD Civil Servant in Defence Equipment and Support (DE&S)
  - Security Assurance Manager for Defence Corporate Business Applications IPT
  - Directorate General Information Systems and Services (DGISS) - formerly Defence Communication Services Agency (DCSA)
- Dr. Konstantinos Markantonakis:
  - Smart Card Centre at Royal Holloway University of London
- Dr. Keith Mayes:
  - Director of the Smart Card Centre at Royal Holloway University of London

Background to Paper

- 2004 to 2006 - MSc Information Security at Royal Holloway
- MSc Project was: “A comparative analysis of common threats, vulnerabilities, attacks and countermeasures within smart card and wireless sensor network node technologies.”
- MSc Project is basis for the paper produced for WISTP07

Objectives of this Research

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

Technology Definitions

- Smart card
  - integrated circuit (crypto co-processor & tamper resistance a common feature)
  - packaged and embedded within a card carrier
  - not normally a networked device (Java Card 3.0 an exception)
  - normally receives power from a separate source (some exceptions)

  Contact and contactless Smart Cards and also RFID technologies under the unified banner of smart card technologies

- Wireless Sensor Network Node (Mote)
  - integrated circuit (basic micro-controller, no tamper resistance or crypto co-processor)
  - able to function as an element within a network, to send, receive or route
  - onboard battery but low power consumption
  - passing data onto other devices through wireless communications
  - collaborating to form a sensing network

  No focus on specific vendors or operating systems - broad view research

Background to Analysis #1

- Plenty of data on ‘known’ attacks and Security Mechanisms for Smart Cards
- Some data on ‘known’ and theoretical attacks on Motes
- Plenty of Risk Analysis methods around, not many Threat Analysis methods
- Definitions identity crisis – what is a threat?

Background to Analysis #2

- Chose four pillars for the Security Analysis and created own definitions, need to ‘harvest’ as much information as possible:
  - Threat: “an objective a foe might try to realise in order to misuse a target or asset”
  - Vulnerability: “a specific means by which a threat can be executed via an unmitigated attack path”
  - Attacker: “the entity that is exploiting a vulnerability to establish a threat”
  - Countermeasure: “a mitigation measure that prevents, detects or significantly reduces a misdeed associated with a specific threat or group of threats”

This led to the creation of the TVAC Table - four pillars became four blocks

Background to Analysis #3 - TVAC

Technology	Threat Unique ID	(1) THREAT BLOCK			(2) VULNERABILITY BLOCK		
		Target &/or Asset	Threat Class	Threat Summary	Vulnerability Summary	CRIPAL	STRIDE
		Physical – Chip & Logical - Operating System	Physical Static & Dynamic Logical Static & Dynamic Social	**Statement** : Protocol &/or functionality attack.Try to usurp onboard file system and/or execute rogue code - e.g., execute bogus application or bogus update code. **Entry Point**: Various **Impact**: M	**Statement** : Either by randomly trying spurious command sets or some of the attacks already mentioned, it might be possible to gain unauthorised access to the file system and/or run illegal code. **Probability**: L	C I P L	S T I E
Contact & Contactless Smart Card	SCA-T6 SCB-T6	(3) ATTACKER BLOCK			(4) COUNTERMEASURE BLOCK		
		Attacker Group	Attack Class	Countermeasure Summary Total/Partial/None)	Overhead of Countermeasure on Time, Performance & Cost		
		C I C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.	**Statement** : Memory Management & Firewall for access control to memory areas checking target addresses within limits. No code exec-ution in EEPROM or RAM. EEPROM has write/erase disallowed by setting page to prot-ected state, any bogus access attempt leaves content unaltered. Protection permanent once set, violations lead to prevention of execution and/or erasure of memory contents. Consider Global Platform with Card Manager, signed code, authentication/confirmation for updates. **Effectiveness**: Partial to Total	**Time**: Manufacture time goes up to incorporate these requirements. **Performance**: Possibly a tiny bit slower as these memory protection functions are executed and any signed code verified **Cost**: Cost of manufacture increases to cover this countermeasure		

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

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

Background to Analysis #4 - TVAC

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

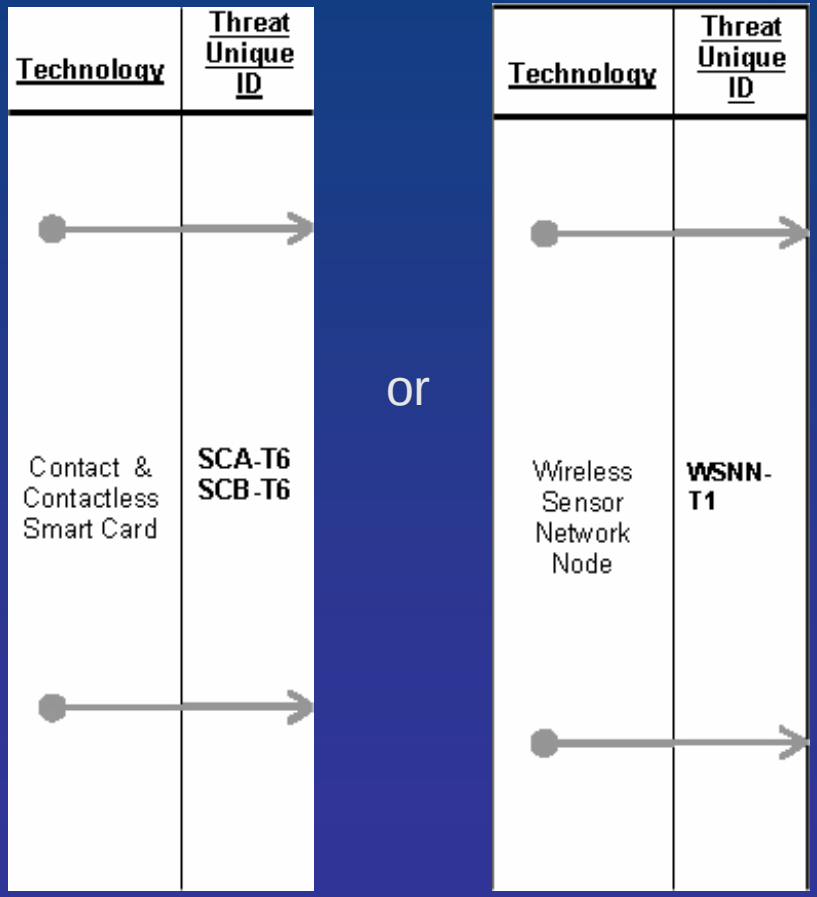
(2) VULNERABILITY BLOCK		
Vulnerability Summary	**CRIPAL**	**STRIDE**
Statement : Either by randomly trying spurious command sets or some of the attacks already mentioned, it might be possible to gain unauthorised access to the file system and/or run illegal code. **Probability**: L	C I P L	S T I E

(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

Background to Analysis #5 - TVAC



or

The two initial left hand columns categorise the technology type and the threat unique identifier (TUID).

- contact smart card is prefixed SCA
- contactless smart card prefixed SCB
- Wireless Sensor Network Node prefixed WSNN

Background to Analysis #6– TVAC

8 Categories of Threat 'type', indicating what the target or asset is:

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

(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

Threat Summary:

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

7 Threat Classifications:

- 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 e.g., temp)
- Logical Dynamic (e.g., Power to Software);
- Social (e.g., Social Engineering);
- Policy (e.g., Weakness in Governing Policies);
- Other.

Background to Analysis #7 - TVAC

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

(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

S = Spoofing
T = Tampering
R = Repudiation
I = Information disclosure
D = Denial of Service
E = Elevation of Privilege

Microsoft method to categorise threats during software development. Added granularity to 'CRIPAL'

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 (DPA '98, CMA '90).

Background to Analysis #8 - TVAC

(3) ATTACKER BLOCK	
Attacker Group	**Attack Class**
C I C II C III	Invasive Active & Passive. Non-Invasive Active & Passive. Semi Invasive.

5 Attack Classes:

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).

3 Attacker Groups:

- Class I (clever outsiders) - “Opportunist Attacker”
- Class II (knowledgeable insiders) - “Expert/Professional Attacker
- Class III (funded organisations) - “Sophisticated Attacker”

Background to Analysis #9 - TVAC

Countermeasure Summary:

A 'Statement' of the Countermeasure, indicating its 'Effectiveness' represented by the following options:

- Total (Complete Effectiveness)
- Partial (Some Effectiveness)
- None

(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

Overhead of Countermeasure on Time, Performance & Cost:

This looks at any impacts the countermeasure may bring if implemented.

Background to Analysis #10 - TVAC

Short Assessment: “Can the threat and the mitigation to one technology be applied to the other technology”:

- Total
- Partial
- None

(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

Results – 22 TVAC Tables

- 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)
- The Comparative Threat Analysis Assessment Matrices (CTAAMs) record any commonality/applicability from one technology to the other

Smart Card Technologies Analysis Assessment

Comparative Threat Analysis Assessment Matrix:

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

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

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

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

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

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

WSN Nodes Analysis Assessment

Comparative Threat Analysis Assessment Matrix:

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

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

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

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

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

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

Conclusion

- Novel framework and methodology, for:
  - classifying threats
  - analysing threats
  - assessing threats
- The TVAC Table and the CTAAMs, may have wider applicability to other technologies (e.g., Java Card 3.0 & RFIDs)
- Many attacks against smart card integrated circuits apply to WSN nodes
- 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 (crypto co-processors too).
  - Many technologies have matured through schemes like Common Criteria and the production of Protection Profiles may help focus the development of security within WSN nodes
- Two new definitions for attacks:
  - Cessation of Service (CoS)
  - Distributed Cessation of Service (DCoS)
- 'Path-finder' research has established the need for thorough scientific testing to prove or disprove assertions

Further Areas of Research?

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 (similar work in US Dept. Homeland Security)
- 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: (e.g., Attribute Certificates/Kerberos tickets)
- We are interested in investigating an OS/platform independent secure authentication and routing protocol similar to IPSEC, which has a working label of KAFKA (Know Allies & Family, Know Adversaries) to suit the adaptive nature of Wireless Sensor Networks. Also, Sun's SSSL 'sizzle' could lead to work with TLS for secure authentication, confidentiality and Integrity.

More Info & Additional Items

- More information and additional resources (e.g., populated TVAC Tables and CTAAMs) are available at:

  www.sensornets.co.uk

- Thank you & QUESTIONS?