Improving Security of Autonomous UAVs Fleets by Using New Specific Embedded Secure Elements A Position Paper*

Raja Naeem Akram[1], Pierre-François Bonnefoi[2], Serge Chaumette[3]
Konstantinos Markantonakis[4] and Damien Sauveron[5]

***Abstract*— Unmanned Aerial Vehicles (UAVs) fleets are becoming more apparent in both military and civilian applications. However security of these systems still remains unsatisfactory if a strong adversary model is considered. The aim of this position paper is to draw requirements for this kind of adversaries and to propose theoretical solutions based on an embedded Secure Element (SE) that could help to accommodate these requirements.**

I. INTRODUCTION

Unmanned Aerial Vehicles (UAVs) are increasingly used in military and civilian applications. For instance, in the civilian applications they can be used for monitoring forest fires, searching missing people in avalanches, etc. However, most of UAVs being small and light they cannot be equipped with heavy equipments (e.g. heavy sensors or many sensors at the same time). Therefore UAVs often embed very few dedicated sensors and they have to collaborate together and fly in a swarm to provide all the features. Swarm formation helps simple UAVs to collectively form a complex multi-feature fleet; however, if there is no redundancy in the fleet it might become heavily dependent of each and every UAV of the fleet. In addition flying in swarm is helpful and efficient to cover a larger geographic area for the aforementioned applications. Such flights require a collaboration between UAVs which lead them to communicate in a way similar to Mobile Ad hoc Network (MANet) or Delay/Disruptive Tolerant Network (DTN) and as a result become exposed to the same security concerns.

In some contexts (like the civilian applications) security issues might not be of high significance or their exploitation might not have a high impact. However, in military applications it is crucial to address them. For instance UAVs need to securely store data like flight-plan for the mission, photos, coordinates of points of interest (enemies or allies) which are invaluable assets for an opponent. Similarly to avoid attacks at network level, routing (if applicable) must be secured. Nevertheless among all of the potential security problems, capture of UAV will be particularly discussed in this paper.

A. Contribution

In this paper, our main focus is on the enhancement of the security of UAVs fleets. The salient contributions of this paper are as follows:

1) discussion on the adversary model for UAVs fleets;
2) definition of a list of security requirements, which are derived from functional requirements and address the relevant adversary model;
3) proposals of candidate Secure Elements (SE) that can help a UAV to support the identified functional and security requirements;
4) comparison with existing works that proposed the deployment of "secure elements" on unmanned vehicles.

B. Structure of the Paper

Section II discusses the strong adversary model that we consider for UAV fleets. In section III, we list the requirements that a UAV equipped with a SE should satisfy to address the defined adversary model and we present a list of candidates for the SEs. Section IV compares our proposal with the related work. Then section V presents our future works for implementing our proposal along with our concluding remarks.

II. ADVERSARY MODEL

In this paper we consider a strong adversary model with a high attack potential. For instance the adversary has capabilities and knowledge to capture a UAV, to perform side-channel or fault injection or other physical, software or combined attacks in order to gain access to (or to modify for his profit) some secret data (e.g. cryptographic keys), software or hardware.

A. Capture of UAV by an Attacker

In this section we assume that the attacker can capture a UAV that is in functional state (i.e. there is no difference between the captured UAV and one in flight). It means that if there are self destruction mechanisms like the ones we

*This work is a position paper. Implementation of the proposed Secure Element for UAV fleet has not yet been done.

[1]R. N. Akram is with the Department of Computer Science, University of Waikato, Hamilton, New Zealand.
E-mail: rnakram@waikato.ac.nz

[2]P-F. Bonnefoi is with XLIM (UMR CNRS 7252 / Université de Limoges) Département Mathématiques Informatique, Limoges, France.
E-mail:pierre-francois.bonnefoi@unilim.fr

[3]S. Chaumette is with LaBRI, Bordeaux 1 University, Talence, France.
E-mail: serge.chaumette@labri.fr

[4]K. Markantonakis is with Information Security Group Smart Card Centre, Royal Holloway, University of London, Egham, United Kingdom.
E-mail: k.markantonakis@rhul.ac.uk

[5]D. Sauveron is with XLIM (UMR CNRS 7252 / Université de Limoges) Département Mathématiques Informatique, Limoges, France.
E-mail:damien.sauveron@unilim.fr

will mention in section IV the attacker is able to bypass or deactivate them. Even worst the attacker might perform attacks during the flight[1].

B. Attacks on a "Captured" UAV

Once a UAV is captured, the opponent can perform various well-known attacks studied and applied during past decades mainly in the world of smart cards. Even if a smart card (under its different form factors) is considered without any doubt, one of the most secure devices which runs successfully in the worst adversary conditions (where even its owner can be malicious), it has been and is still subject to very advanced attacks like:

- Side-channel attacks [14], [17], [32], [50], [53]. This kind of blackbox attacks consists in observing some information leakage from algorithms running on the target. From these leakages, different kinds of information can be retrieved (e.g. cryptographic keys [43], sequence of opcodes executed [62]). The nature of leakages can be time-based [42], the power consumption with several families of attacks (Simple Power Analysis [43], Differential Power Analysis [43], High-Order Differential Power Analysis [47], Corellation Power Analysis [23]), the electromagnetic radiations with the same declination of families of attacks (Simple Electromagnetic Analysis [35], [55], Differential Electromagnetic Analysis [5], [35], High-Order Differential Electromagnetic Analysis, Corellation Electromagnetic Analysis) or combination of different sources [6], [64]. There also exist some other powerful attacks using side-channels like Template-Attacks [24], [56].
- Fault injection attacks [15], [21], [36], [37], [44], [59]. This kind of attacks consists in perturbing, usually during a short time, the execution of a process for instance by using a laser or voltage glitches to reach a state the attacker can take advantage of. For instance, using fault injection at the right time on a RSA signature process, an attacker can recover very quickly the private key used [21] in exploiting the erroneous signatures delivered by the blackbox system signing the message. With Differential Fault Analysis, secret key cryptosystems like DES [20] or AES [34] are also vunerable.
- Physical attacks [44], [58]. This kind of attacks encompasses microprobing, circuitery modification with a Focused Ion Beam system or a laser cuter, etc.
- Software attacks. This kind of attacks is highly dependent on the possibility to load applications on the target. The loading can be or not protected by an authentication mechanism (but it can still be circumvented by another attack). However, if application loading is possible, it can be feasible to perform and sometime achieve some attacks from inside the target against other hosted applications or against the platform of the target [30], [49].
- Combined attacks [16], [63]. These attacks often combine fault injection during execution of a code loaded or already present in the target to alter the application execution in order to gain additional access priviledges.

These attacks are not only applicable to smart card but also to any processor [14], [17], [37], [53], [60] and thus to a UAV.

C. Attacks on a UAV in a Network

At the best of our knowledge, there is no paper specifically addressing attacks that a UAV can be subjected to through the network in a fleet or a swarm. We thus consider that the adversary can perform similar attacks to those existing in MANets, DTN and Wireless Sensors Networks. In particular, the attacker can perform the easiest attacks on a wireless link: a Denial-of-Service (DoS) [65]. This attack can be achieved:

- at the physical level by interfering on radio frequencies used by the UAVs (jamming attack);
- at the link level by exploiting the medium access control backoff and retransmission procedures (collision attacks);
- at the network level by using routing loop attacks [46];
- at the transport level using a flooding attack or a desynchronization attack [33].

If communications are not ciphered, the opponent can perform eavesdropping, packet injection or corruption and he can even attempt Man-in-the-Middle or relay attacks.

The attacker can also build a rogue UAV to attempt some attacks on routing protocols [22], [31], [40] like: blackhole attack, selective forwarding attack, sinkhole attack, rushing attack, sybil attack, wormhole attack, etc.

Some application specific attacks can also be performed but they are beyond the scope of this paper.

D. Rationale for the Adversary Model

In recent work, some academic researchers have done a Correlation Power Analysis [48] on Virtex-4 and Virtex-5 family, i.e. Xilinx FPGAs that are widely used in UAVs (including the Predator [66]). They shown that the encryption mechanism can be completely broken with moderate effort. Thus, a strong adversary model makes sense, especially in the context of military usage of UAVs fleets since the opponent can be a government-controlled organization capable of performing forensic analysis or attacks of the UAVs.

The reader should note that for all of the aforementioned attacks there are corresponding countermeasures which are well known to the industry and academia. The countermeasures that are implemented must not impact the real time capacities of the UAV, especially regarding its auto-pilot and its responsiveness to external, GPS and Inertial Measurement Unit (IMU) events. It is even more important because we are considering fleets of UAVs and not a single UAV.

III. REQUIREMENTS

This section describes the functional requirements that a UAV equiped with a SE should satisfy. Thereafter, based on the functional requirements and adversary model, we stipulate the security requirements.

[1]It is important to underline that the operating attacks mentioned in section II-B on a flying UAV (even if it should not be easy) are equivalent to have captured the UAV.

A. Functional Requirements

For a wide adoption, UAVs fleets should satisfy some functional requirements.

- (FR1) The fleet should be autonomous and should not rely on communication with its base/user to be more stealthy in the adversary conditions of the mission (e.g. intensive long RF communication with the base may be easier to locate than short range communication between UAVs).
- (FR2) The fleet should be easy and transparent to manage both in terms of functionality and security and management should be possible prior or during the fleet operations. For instance, at a scheduling step, the user just needs to define the mission she wishes the fleet to perform. Then, when rescheduling the mission is needed, (for instance if user wants to include new objectives like new measurements from embedded sensors), the update of the mission may be done during the refuelling in energy (e.g. in air from more powerful UAVs) or with new UAVs joining the current fleet to transmit the new mission. In addition, the user should not have to worry about the underlying security architecture for communication and management of the fleet.
- (FR3) The fleet should be reliable. It means that each UAV can have a dedicated mission but, if needed, for some reasons (e.g. failure, too low energy level to achieve the mission), it may decide to entrust its mission to another UAV according to the capabilities in term of equipments (e.g. sensors) and software stack of this UAV.
- (FR4) A UAVs fleet has to perform optimally in the adversely territories/environments. It thus must be able to analyze the situation and make decisions in real-time. Therefore, any hardware included in the system should not incur unnecessary performance penalties.

From these requirements, it means that the fleet should be self-organized and should be equipped with some sort of swarm intelligence.

B. Security Requirements

According to the adversary model defined in section II and from the functional requirements defined above, UAVs of the fleet should satisfy the following security requirements.

- (SR1) The UAV should be SE-driven to ensure security and privacy of its missions. In addition, the security architecture of the UAV system should not incur performance penalties. Therefore, any proposal for the UAV system should be robust and optimal in both security and performance — preserving a real-time processing environment with high level of assurance.
- (SR2) The whole UAV should be tamper resistant, or at least a part of it (the SE).
- (SR3) The UAV should provide assurance in implemented security mechanisms to its user. For instance it, or more precisely its SE, has to be subjected to a security evaluation and certification to prove that it can resist an attacker compliant with the strong adversary model defined above. The certification can be Common Criteria evaluation [2] with a minimum in the Evaluation Assurance Level of EAL4+, where '+' means 'augmented' with security assurance requirement component AVA_VAN5 (i.e. the highest assurance component of the vulnerabilities analysis family of the vulnerability assessment class).
- (SR4) The UAV at a very basic level should provide a secure unique ID on which the whole fleet can rely for its management and networking operations.
- (SR5) The UAV should provide secure key management and crytographic features to protect communication integrity and confidentiality among the members of the fleet.
- (SR6) UAV should provide a secure storage for data collected (e.g. measurements, photos) and/or those used for the purpose of the mission (e.g. flight-plan for the mission, coordinates of points of interest).
- (SR7) The UAV should provide a secure multi application platform. This requirement is justified since in the context of SE-driven UAV there will be installation of new applications (for new purposes according to FR2) or transfer of applications between UAVs (when an entrustment of a mission from a deficient UAV to another one occurs according to FR3). Update of already embedded applications containing flaws with new versions covering the threats can even occur. This SR facilitates a scalable and flexible design, where new sensors can be added to individual UAVs depending upon the mission and the associated sensor management application can then be loaded onto the SE. Note that installation or update can occur for instance during air refuelling.

An additional functional requirement may be optionally added if the context of SE-driven UAV is accepted: (FR5) the SE may have its own communication capabilities to communicate with other SEs which can form an overlay network (for specific control operations) parallel to the one that already exists between UAVs (i.e. the SE can communicate with its own RF communication module operating with a dedicated part of the RF spectrum).

These requirements define a secure Machine to Machine (M2M) platform over a fleet of UAVs.

C. Candidate Secure Elements

In this section, we present several candidates for the SE. As none of them is satisfying all of the requirements defined above, we are defining our SE, that we will develop in our future activities.

1) Wireless Sensor Node: A Wireless Sensor Node (WSN) has communicating capabilities that would satisfy FR5. However as it has been shown in [31], in its current "form" a WSN cannot be the SE because in case of capture it fails to satisfy SR2 to SR7 and thus SR1. However it should be noted that some work is in progress to design, evaluate and certified WSN in very specific contexts [18], [19] or to add to it a Trusted Platform Module (that is a candidate for being a SE discussed below) to enhance its own security [39].

2) Trusted Platform Module: A Trusted Platform Module (TPM) is an interesting candidate since it can partially satisfy SR2 to SR6. TPM may fail to satisfy SR3 for which the device has to provide an assurance of its own security. Indeed there is no compulsory requirement that a TPM has to be subjected to security evaluation and certification. Since in the traditional deployments, TPMs are going through the security evaluation, they are intrinsically considered to be trusted and secure. Therefore, they are used to provide a trusted measurement of the individual applications and Operating System (OS). However, a TPM itself cannot verify whether an application or the OS is secure or not. This decision has to be taken by the user based on the (trusted) integrity measurement provided by the TPM. Similarly, the TPM partially satisfies the SR6 as it does have small (secure) storage but mostly for cryptographic material. The TPM storage can potentially be increased or data can be stored in encrypted form outside the TPM where the encryption key remains securely stored. However, the later scheme will only incur additional computational requirements, thus adding performance penalties. However it cannot execute code, thus it fails to satisfy SR1, and SR7. As the UAVs fleet, once in a mission, should not be constantly required to provide state attestations by the base station or peer UAVs because it will incur unnecessary performance penalty violating both FR1 and FR4. Including a TPM will only be useful if the UAVs fleet is grounded, or in instances where the base station requires to verify the state of the system before the mission starts. In addition, since a TPM does not have standalone decision capabilities it would fail to satisfy FR3 and FR5.

3) Smart Card: Smart cards are designed with a strong adversary model in mind which assumes that they are in the possession of a potentially malicious user. Under such an adversarial model, the smart cards are required to provide a secure and trusted execution environment. Therefore, the smart card platform has a matured architecture that can adequately support the functional and security requirements given in the previous sections. As a result, smart cards intrinsically support SR2 to SR6.

To comprehensively support SR7, the ownerhip model for the deployment of smart card based SE in UAV should support User Centric Smart Card Ownership Model (UCOM) [8] which provides a dynamic, scalable and flexible architecture for multi-application platforms. In addition, the UCOM proposal of Trusted Execution and Environment Manager (TEM) [13] has the potential to provide a strong trusted device and (application) execution architecture. Furthermore, UCOM based smart cards also support remote attestation and validation mechanims [7], [11], [12] along with a secure architecture for application migration [10] between different smart cards.

For a collaborative and dynamic capability to reassign resources to accomplish a mission (FR3), the UCOM based smart card architecture provides a solid foundation as per the proposal for a secure and trusted application sharing mechanism between two or more smart cards [9]. Thus the UCOM smart card with TEM has all qualities to withstand SR1. Although, it can be argued that smart cards do not possess the RF communication capabilities, such a functionality can be built around it as a standalone module.

4) Active RFID: Active RFID are difficult to categorize because a mobile phone could be considered as a long range RFID with additional functionalities (by the way it can also be considered as a big WSN). In our vision, we are more considering as Active RFID devices like the OpenBeacon Tag [1] but with a secure chip.

However, even if there exist some active RFIDs (e.g. remote control keys for cars), initial experiments seem to show they are vulnerable to several attacks [41], [52]. However, it must take into account the active RFIDs studied are necessarily vulnerable because they are not designed to withstand a high potential attack.

At best, current Active RFIDs are only supporting SR4, SR5 and FR5.

5) Our proposal: Our proposal of SE consists in bringing together the best of active RFID, WSN and smart card in what can be called an Active Radio Frequency Smart Secure Device (ARFSSD) to address the only features that the smart card fails to satisfy: the optional FR5. Then ARFSSD would then satisfy all the above requirements.

As illustrated in figure 1 our first prototype will be based on an ARM-based platform as the ubiquitous Raspberry Pi embedding Linux and the PC/SC middleware to support a smart card reader. These components will only serve to interface between the UCOM smart card and the RF communication module that we will use. The dotted line represents communication level between the smart card and the RF communication module whereas the plain arrows represent the real communications between the different subsystems of the prototype. We have not yet decided which

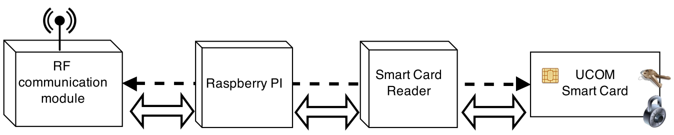

Fig. 1. An overview of the future prototype of our Active Radio Frequency Smart Secure Device

RF communication module we will use since making a final decision requires to run some experimentations. However we have in mind, the NRF24L01 from Nordic Semicondutor, the Xbee module (a ZigbBee implementation) from Digi International or the Wifly module (a Wi-Fi implementation) from Roving Networks.

6) Summary: As shown in table I, smart card is actually the most serious candidate. However, ARFSSD should fullfil the only missing smart card functional requirement to be the ultimate solution.

IV. RELATED WORK

There is very little work in publicly available literature related to the security of identity in fleets of UAVs. This

TABLE I

REQUIREMENTS FULLFILLED BY THE CANDIDATE SE

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	FR5
WSN								x
TPM		x	x	x	x	x		
Smart Card	x	x	x	x	x	x	x	
Active RFID				x	x			x
Our proposal	x	x	x	x	x	x	x	x

must be explored further because it is on the security of data involved in the authentication mechanisms that the trust for future transactions between UAVs (data exchange, routing in the cases where it is used, etc.) relies. In security architectures for fleets of UAVs supporting group communications (e.g. [54]) or collaborative work (e.g. [57]), the possibility of an attacker with high attack potential (i.e. for instance being able to physically access a UAV after its capture) is almost never considered. In the few studies considering this kind of attacker model, the physical security of the elements used to support identification, i.e. the heart of security, is relegated to the assumptions on the equipment used or additional countermeasures such as self-destruction of the UAV [45], [67]. However attacks can occur during flights which can defeat the physical protection. The only papers that actually consider to protect the identifiers are those initiated by Chaumette et al. through the use of Java Card [25], [26]. Some other papers [27], [38] are considering a secure token (i.e. a smart card) in swarms of UAVs but without giving details except it is used to securely store some data and perform some ciphering operations.

Since our proposal of ARFSSD can be seen as an extension of these works through the use of active RFIDs, it is interesting to survey the use of RFIDs in nearby contexts. In the area of fleets of robots, passive RFIDs are used to make a sort of communication between robots for the allocation of tasks [61] or for synchronization [68]. However, in no case these papers address any security concerns. Other papers related to the use of RFIDs for UAVs include an inventory of goods with a UAV carrying a RFID reader in a warehouse [4] or an hypothetical future RFID injection under the skin of people with cyber insects [3] which is far from our concerns.

V. FUTURE WORKS AND CONCLUSIONS

From the requirements listed in section III, we will develop a first prototype of ARFSSD as a Secure Element for UAVs fleets. It is worth noting how such UAVs fleets equipped with our SE raise problems close to those we are addressing in other contexts (e.g. Multilevel Mobile Java Card Grid [28], [29] and multilevel, secure (smart card), communication based services on a fleet of mobile phones [51]). We thus believe that our work will impact not only the domain of fleets of UAVs but more generally the domain of mobile communicating objects, i.e. the Internet of Things.

REFERENCES

[1] OpenBeacon Tag. http://www.openbeacon.org/OpenBeacon_Tag. [Online; accessed 3-May-2014].

[2] Common Criteria for Information Technology Security Evaluation, Std. Version 3.1, Rev. 3, July 2009.

[3] The Future of Drone Surveillance: Swarms of Cyborg Insect Drones. http://www.networkworld.com/community/blog/future-drone-surveillance-swarms-cyborg-insect-drones, August 2012. [Online; accessed 3-May-2014].

[4] MAV RFID Swarm: Fast and Low Cost RFID Inventory System. http://marblar.com/idea/kWpA7, October 2013. [Online; accessed 3-May-2014].

[5] D. Agrawal, B. Archambeault, J. Rao, and P. Rohatgi. The EM SideChannel(s). In B. S. Kaliski, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 29–45. Springer Berlin Heidelberg, August 2003.

[6] D. Agrawal, J. R. Rao, and P. Rohatgi. Multi-channel Attacks. In C. D. Walter, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2003*, volume 2779 of *Lecture Notes in Computer Science*, pages 2–16. Springer Berlin Heidelberg, September 2003.

[7] R. N. Akram, K. Markantonakis, and K. Mayes. A Dynamic and Ubiquitous Smart Card Security Assurance and Validation Mechanism. In Kai Rannenberg and V. Varadharajan, editors, *25th IFIP International Information Security Conference (SEC 2010)*, IFIP AICT Series, pages 161–171, Brisbane, Australia, September 2010. Springer.

[8] R. N. Akram, K. Markantonakis, and K. Mayes. A Paradigm Shift in Smart Card Ownership Model. In Bernady O. Apduhan, Osvaldo Gervasi, Andres Iglesias, D. Taniar, and M. Gavrilova, editors, *Proceedings of the 2010 International Conference on Computational Science and Its Applications (ICCSA 2010)*, pages 191–200, Fukuoka, Japan, March 2010. IEEE Computer Society.

[9] R. N. Akram, K. Markantonakis, and K. Mayes. Cross-Platform Application Sharing Mechanism. In H. Wang, S. R. Tate, and Y. Xiang, editors, *10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-11)*, Changsha, China, November 2011. IEEE Computer Society.

[10] R. N. Akram, K. Markantonakis, and K. Mayes. Recovering from Lost Digital Wallet. In F. G. M. Y. Xiang and S. Ruj, editors, *The 4th IEEE International Symposium on Trust, Security, and Privacy for Emerging Applications (TSP-13)*, Zhangjiajie, China, November 2013. IEEE CS.

[11] R. N. Akram, K. Markantonakis, and K. Mayes. Remote Attestation Mechanism based on Physical Unclonable Functions. In C. M. J. Zhou and J. Weng, editors, *The 2013 Workshop on RFID and IoT Security (RFIDsec'13 Asia)*, Guangzhou, China, November 2013. IOS Press.

[12] R. N. Akram, K. Markantonakis, and K. Mayes. Remote Attestation Mechanism for User Centric Smart Cards using Pseudorandom Number Generators. In S. Qing and J. Zhou, editors, *5th International Conference on Information and Communications Security (ICICS 2013)*, Beijing, China, November 2013. Springer.

[13] R. N. Akram, K. Markantonakis, and K. Mayes. Trusted Platform Module for Smart Cards. In O. Alfandi, editor, *6th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Dubai, UAE, March 2014. IEEE CS.

[14] H. Aly and M. ElGayyar. Attacking AES Using Bernsteins Attack on Modern Processors. In A. Youssef, A. Nitaj, and A. Hassanien, editors, *Progress in Cryptology AFRICACRYPT 2013*, volume 7918 of *Lecture Notes in Computer Science*, pages 127–139. Springer Berlin Heidelberg, June 2013.

[15] H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan. The Sorcerer's Apprentice Guide to Fault Attacks. *Proceedings of the IEEE*, 94(2):370–382, February 2006.

[16] G. Barbu and C. Giraud. New Countermeasures against Fault & Software Type Confusion Attacks on Java Cards. In D. Naccache and D. Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things*, volume 8501 of *Lecture Notes in Computer Science*, pages 57–75, July 2014.

[17] D. J. Bernstein. Cache-timing attacks on AES. Technical report, 2005.

[18] A. Bialas. Common Criteria Related Security Design PatternsValidation on the Intelligent Sensor Example Designed for Mine Environment. *Sensors*, 10(5):4456–4496, 2010.

[19] A. Bialas. Intelligent Sensors Security. *Sensors*, 10(1):822–859, 2010.

[20] E. Biham and A. Shamir. Differential fault analysis of secret key cryptosystems. In B. S. Kaliski, editor, *Advances in Cryptology CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 513–525. Springer Berlin Heidelberg, August 1997.

[21] D. Boneh, R. A. DeMillo, and R. Lipton. On the Importance of Checking Cryptographic Protocols for Faults. In W. Fumy, editor, *Advances in Cryptology EUROCRYPT 97*, volume 1233 of *Lecture Notes in Computer Science*, pages 37–51. Springer Berlin Heidelberg, May 1997.

[22] P. F. Bonnefoi, D. Sauveron, and J. H. Park. MANETS: an exclusive choice between use and security? *Computing and Informatics. Special Issue on Interactive Multimedia & Intelligent Services in Mobile and Ubiquitous Computing (MUC)*, 27(5):799–821, 2008.

[23] E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In M. Joye and J.-J. Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer Berlin Heidelberg, August 2004.

[24] S. Chari, J. R. Rao, and P. Rohatgi. Template Attacks. In B. S. Kaliski, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 13–28. Springer Berlin Heidelberg, August 2003.

[25] S. Chaumette and R. Laplace. Embedding Java Cards to secure communications and manage identities in a UAVnet (network of drones). In *Proceedings of e-Smart'11*, September 2011.

[26] S. Chaumette, R. Laplace, C. Mazel, and A. Godin. Secure cooperative ad hoc applications within UAV fleets – Position paper –. In *Military Communications Conference, 2009. MILCOM 2009. IEEE*, pages 1–7, October 2009.

[27] S. Chaumette, R. Laplace, C. Mazel, and R. Mirault. SCUAL, swarm of communicating UAVs at LaBRI: An open UAVNet testbed. In *Proceedings of International Workshop on Opportunistic and Delay/disruption-Tolerant Networking in conjunction with the 14th International Symposium on Wireless Personal Multimedia Communications (WODTN 2011 (WPMC 2011 Workshop)*, pages 1–5, Oct 2011.

[28] S. Chaumette, K. Markantonakis, K. Mayes, and D. Sauveron. The Mobile Java Card Grid Project. In *Proceedings of e-Smart'06*, September 2016.

[29] S. Chaumette and J. Ouoba. Roadmap to a Multilevel Java Card Grid, May 2007. Poster - WISTP 2007, May 8-11 Heraklion Greece.

[30] S. Chaumette and D. Sauveron. Some Security Problems Raised by Open Multiapplication Smart Cards. In *Proceedings of the 10th Nordic Workshop on Secure IT-systems (NordSec 2005)*, pages 1–12, Tartu, Estonia, October 2005.

[31] S. Chaumette and D. Sauveron. Wireless Sensor Nodes. In K. Markantonakis and K. Mayes, editors, *Secure Smart Embedded Devices, Platforms and Applications*, pages 335–350. Springer New York, 2014.

[32] J.-S. Coron, P. Kocher, and D. Naccache. Statistics and Secret Leakage. In Y. Frankel, editor, *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 157–173. Springer Berlin Heidelberg, February 2001.

[33] W. Dargie and C. Poellabauer. *Fundamentals of Wireless Sensor Networks: Theory and Practice*. Wireless Communications and Mobile Computing. Wiley, 2010.

[34] P. Dusart, G. Letourneux, and O. Vivolo. Differential Fault Analysis on A.E.S. In J. Zhou, M. Yung, and Y. Han, editors, *Applied Cryptography and Network Security*, volume 2846 of *Lecture Notes in Computer Science*, pages 293–306. Springer Berlin Heidelberg, October 2003.

[35] K. Gandolfi, C. Mourtel, and F. Olivier. Electromagnetic analysis: Concrete results. In Ç. K. Koç, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 251–261. Springer Berlin Heidelberg, May 2001.

[36] C. Giraud and H. Thiebeauld. A Survey on Fault Attacks. In J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. Kalam, editors, *Smart Card Research and Advanced Applications VI*, volume 153 of *IFIP International Federation for Information Processing*, pages 159–176. Springer US, 2004.

[37] S. Govindavajhala and A. W. Appel. Using Memory Errors to Attack a Virtual Machine. In *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, SP '03, pages 154–165, Washington, DC, USA, May 2003. IEEE Computer Society.

[38] V. Guyot, A. Gademer, L. Avanthey, L. Beaudoin, and R. Erra. Swarm UAV attack: how to protect sensitive data? In *Proceedings of European Conference on Information Warfare and Security ECIW 2012*, 2012.

[39] W. Hu, H. Tan, P. Corke, W. C. Shih, and S. Jha. Toward trusted wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 7:5:1–5:25, August 2010.

[40] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Sensor Network Protocols and Applications, 2003. Proceedings of the First IEEE. 2003 IEEE International Workshop on*, pages 113–127, 2003.

[41] T. Kasper, D. Oswald, and C. Paar. Wireless security threats: Eavesdropping and detecting of active RFIDs and remote controls in the wild. In *Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on*, pages 1–6, Sept 2011.

[42] P. C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In N. Koblitz, editor, *Advances in Cryptology CRYPTO 96*, volume 1109 of *Lecture Notes in Computer Science*, pages 104–113. Springer Berlin Heidelberg, August 1996.

[43] P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 388–397, London, UK, UK, 1999. Springer-Verlag.

[44] O. Kömmerling and M. G. Kuhn. Design Principles for Tamper-resistant Smartcard Processors. In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, WOST'99, pages 9–20, Berkeley, CA, USA, 1999. USENIX Association.

[45] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu. Adaptive Security for Multi-layer Ad-hoc Networks. In *Special Issue of Wireless Communications and Mobile Computing*, pages 533–547. Wiley Interscience Press, 2002.

[46] A. Larsson. Report on the State of the Art of Security in Sensor Networks, 2011.

[47] T. Messerges. Using Second-Order Power Analysis to Attack DPA Resistant Software. In Ç. K. Koç and C. Paar, editors, *Cryptographic Hardware and Embedded Systems CHES 2000*, volume 1965 of *Lecture Notes in Computer Science*, pages 238–251. Springer Berlin Heidelberg, August 2000.

[48] A. Moradi, M. Kasper, and C. Paar. Black-Box Side-Channel Attacks Highlight the Importance of Countermeasures. In O. Dunkelman, editor, *Topics in Cryptology CT-RSA 2012*, volume 7178 of *Lecture Notes in Computer Science*, pages 1–18. Springer Berlin Heidelberg, February 2012.

[49] W. Mostowski and E. Poll. Malicious Code on Java Card Smartcards: Attacks and Countermeasures. In G. Grimaud and F.-X. Standaert, editors, *Smart Card Research and Advanced Applications*, volume 5189 of *Lecture Notes in Computer Science*, pages 1–16. Springer Berlin Heidelberg, September 2008.

[50] J. A. Muir. Techniques of Side Channel Cryptanalysis. 2001. Master's thesis, Master of Mathematics in Combinatorics and Optimization, University of Waterloo, Ontario, Canada.

[51] J. Ouoba. *Étude, conception et validation d'une architecture multi-niveaux mobile à base de terminaux communicants, sécurisés par cartes à puce*. PhD thesis, LaBRI - University Bordeaux 1, 2013.

[52] J. Park, H. Lee, and M. Ahn. Side-Channel Attacks against ARIA on Active RFID Device. In *Convergence Information Technology, 2007. International Conference on*, pages 2163–2168, Nov 2007.

[53] C. Percival. Cache missing for fun and profit. In *Proceedings of BSDCan 2005*, 2005.

[54] A. N. Phillips. *A Secure Group Communication Architecture for a Swarm of Autonomous Unmanned Aerial Vehicles*. Air Force Institute of Technology., 2008.

[55] J.-J. Quisquater and D. Samyde. ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards. In I. Attali and T. Jensen, editors, *Smart Card Programming and Security*, volume 2140 of *Lecture Notes in Computer Science*, pages 200–210. Springer Berlin Heidelberg, September 2001.

[56] C. Rechberger and E. Oswald. Practical Template Attacks. In C. Lim and M. Yung, editors, *Information Security Applications*, volume 3325 of *Lecture Notes in Computer Science*, pages 440–456. Springer Berlin Heidelberg, August 2004.

[57] M. Sbeiti, A. Wolff, and C. Wietfeld. PASER: Position Aware Secure and Efficient Route Discovery Protocol for Wireless Mesh Networks. In *SECURWARE 2011, The Fifth International Conference on Emerging Security Information, Systems and Technologies*, pages 63–70, August 2011.

[58] S. Skorobogatov. Tamper resistance and hardware security. `http://`

www.cl.cam.ac.uk/~sps32/PartII_030214.pdf, February 2014. [Online; accessed 3-May-2014].

[59] S. Skorobogatov and R. Anderson. Optical Fault Induction Attacks. In B. S. Kaliski, Ç. K. Koç, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems - CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 2–12. Springer Berlin Heidelberg, 2003.

[60] R. Spreitzer and B. Gérard. Towards More Practical Time-Driven Cache Attacks. In D. Naccache and D. Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things*, volume 8501 of *Lecture Notes in Computer Science*, pages 24–39, July 2014.

[61] T. Tammet, J. Vain, A. Puusepp, E. Reilent, and A. Kuusik. RFID-based Communications for a Self-Organising Robot Swarm. In S. A. Brueckner, P. Robertson, and U. Bellur, editors, *Self-Adaptive and Self-Organizing Systems, 2008. SASO '08. Second IEEE International Conference on*, pages 45–54, October 2008.

[62] D. Vermoen, M. Witteman, and G. N. Gaydadjiev. Reverse Engineering Java Card Applets Using Power Analysis. In D. Sauveron, K. Markantonakis, A. Bilas, and J.-J. Quisquater, editors, *Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems*, volume 4462 of *Lecture Notes in Computer Science*, pages 138–149. Springer Berlin Heidelberg, May 2007.

[63] É. Vétillard and A. Ferrari. Combined Attacks and Countermeasures. In *Smart Card Research and Advanced Application*, volume 6035 of *Lecture Notes in Computer Science*, pages 133–147. Springer Berlin Heidelberg, April 2010.

[64] C. Walter and S. Thompson. Distinguishing Exponent Digits by Observing Modular Subtractions. In D. Naccache, editor, *Topics in Cryptology CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 192–207. Springer Berlin Heidelberg, April 2001.

[65] A. D. Wood and J. A. Stankovic. Denial of Service in Sensor Networks. *Computer*, 35:54–62, October 2002.

[66] J. A. Xilinx. Case study: Secure FPGA technology enables UAV communications and control. http://mil-embedded.com/articles/case-enables-uav-communications-control/, April 2011. [Online; accessed 3-May-2014].

[67] A. Yavuz, F. Alagoz, and E. Anarim. HIMUTSIS: Hierarchical Multi-tier Adaptive Ad-Hoc Network Security Protocol Based on Signcryption Type Key Exchange Schemes. In A. Levi, E. Sava, H. Yenign, S. Balcsoy, and Y. Saygn, editors, *Computer and Information Sciences ISCIS 2006*, volume 4263 of *Lecture Notes in Computer Science*, pages 434–444. Springer Berlin Heidelberg, 2006.

[68] G. Zecca, P. Couderc, M. Banâtre, and R. Beraldi. A swarm of robots using RFID tags for synchronization and cooperation. *International Journal of Intelligent Computing and Cybernetics*, 2(4):846–849, 2009.