AAU Ph.D. Degree

Updated PhD Study plan of research

Title :

Embedded Security for Internet of Things

PhD Candidate
Sachin Dilip Babar
(sdb@es.aau.dk)

Supervisor

Dr. Neeli Rashmi Prasad

(AAU, Denmark)

Co-Supervisor	**Co-Supervisor**
Prof. Ramjee Prasad	**Dr. Jaydip Sen**
(AAU, Denmark)	**(Tata Consultancy Services, India)**

AALBORG UNIVERSITET

Updated PhD Study Plan

Ph.D. Programme : Wireless Communications

Project title : Embedded Security for Internet of Things

Name of PhD student : Mr. Sachin Dilip Babar

Email Id : sdb@es.aau.dk

Education : Master of Computer Engineering

Institution : Pune Institute of Computer Technology, University of Pune, India

Supervisor : Neeli Rashmi Prasad

Co-supervisor :
1. Ramjee Prasad
2. Jaydip Sen (Tata Consultancy Services, Kolkata, India)

Department : Electronic Systems

Date of enrolment : 15 / 11 / 2009

Expected date of Completion : 14 / 11 / 2012

Signature

18 / 09 / 2011	Babar
Date	PhD student

Study plan approved

18 / 09 / 2011		Neeli Rashmi Prasad
Date	Supervisor	**(Has reviewed and approved by)**
		Børge Lindberg
Date	Head of Department	Printed name
		Gert Frølund Pedersen
Date	Head of Doctoral Programme	Printed name

Table of Contents

SECTION 1 : RESEARCH WORK SUMMARY / ABSTRACT

The Internet of Things(IoT) consist of billions of people, things and services having the potential to interact with each other and their environment. This highly interconnected global network structure presents new types of challenges from a security, trust and privacy perspective. Hence, Security for IoT will be a critical concern that must be addressed in order to enable several current and future applications. The resource constrained devices such as cell phones, PDAs, RFIDs, sensor nodes etc. are the part of IoT. The conventional security solutions become unfeasible under resource constraints in the devices. Many of these devices handle sensitive data (e.g., credit card information on a mobile phone/PDA) or perform critical functions (e.g., medical devices or automotive electronics), and the use of security protocols is imperative to maintain confidentiality, integrity and authentication of these applications. Design process for securing embedded devices is guided by factors like small form factor, good performance, low energy consumption and robustness to attacks. Nowadays Embedded security is growing as new dimension which designers should consider throughout the design process, along with other metrics such as cost, performance, and energy efficiency. Embedded security means integrating the security features right in to the hardware and software parts of the devices. The unusual design constraints placed on embedded devices require a novel, highly efficient, easy to deploy cryptography scheme that provides high levels of security while minimizing memory, execution speed requirements and power requirements. The complex security requirements of attack resistant systems in IoT bring in a paradigm shift for generic integration. Thus we hypothesize that Hybrid Security processing architecture will be best suited for the embedded devices for IoT which will give the best trade-off between efficiency and flexibility.

The main goal of the research topic is to design and implement embedded security framework and architecture for IoT.

To meet above challenges, the main research problem is divided into sub problems described in the following bullet points

- Embedded Secure Key Storage Platform with efficient memory management and protection units.
- To specify and design optimized Lightweight secure attack resistant techniques.
- Resistance against attacks and threats (Egs. Side-channel attacks, software attacks, etc)

SECTION 2: SCIENTIFIC CONTENTS OF RESEARCH

2.a Background

Embedded technologies are the fastest growing sectors in information technology today and they will increase their propagation in the future IoT. Embedded security being application dependent, the main technical challenge will be to maintain the necessary degree of security with available resource constraints. As embedded devices are integrated in personal and commercial infrastructures and they will be always connected to the internet, the security aspect becomes very important. Embedded security means incorporating security features into the device itself. [1-4]. Foundation for Embedded Security Architecture is based on three main components: Secure software Management, Secure hardware blocks and secure communications inside the processor. If any one of these elements is missing, platform security cannot be achieved.

1. Secure software management: Software security requirements must take into account things such as a secure kernel, secure booter / loader.

2. Required hardware blocks: Main hardware requirements are Secure Key Storage, Memory Management Units and Memory Protection Units (MMU/MPU), lightweight Cryptographic Functions.
3. Secure Communications inside the processor to establish a secure runtime environment.

As a summary, we conclude that embedded security will play a vital role at hardware level, Kernel level and operating system level. Figure 1 shows the structure of embedded security.

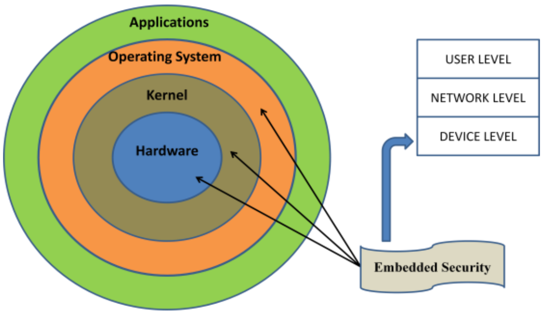

Figure 1: Structure of Embedded Security

Major building blocks for embedded security are listed below:

- **Cryptographic Algorithms :** These are basically the essential building block of a robust security solution. The unusual design constraints placed on embedded devices forces to take a new look at security with highly efficient, easy to deploy lightweight cryptography scheme that provides high levels of security while minimizing memory, execution speed requirements and power requirements. ECC is an essential methodology for meeting these requirements of embedded designs and that is the reason why it is essential for embedded security.
- **Secure Storage :** Cryptographic algorithms require keys as their basis for operation. Secure Storage essentially deals with protecting access to keys and other pieces of data. Secure Storage also needs to be persistent, such that items are not lost during power cycles.
- **Secure Boot :** The purpose of Secure Boot is to bring the system to a known and trusted state. The Secure Boot routine is a ROM-based routine, so that an attacker cannot intercept the procedure. Additional features are required in order to provide a complete Secure Boot solution. These include the ability for software update at any point in time i.e A Software Version Revocation mechanism for system advancement to a new version of the software image with prevention of roll-back to an older version is a must.
- **Secure Execution Environment (SEE) :** The building blocks of an SEE are : a secure processor (either a dedicated processor or one capable of supporting a secure mode) which is hardware compartmentalized from the non-secure mode, Secure code and Data memory (most likely dedicated on-chip RAMs) and a Secure kernel for providing the interface between hardware and software.

2.b Motivation

For framing the Embedded Security framework as shown in figure 2 for IoT following facts are fundamentals [4,5]:

1) Security is about policy, procedure, and implementation apart from encryption.
2) Security should be considered at every phase of the development cycle, from requirements to design to testing, and even support.

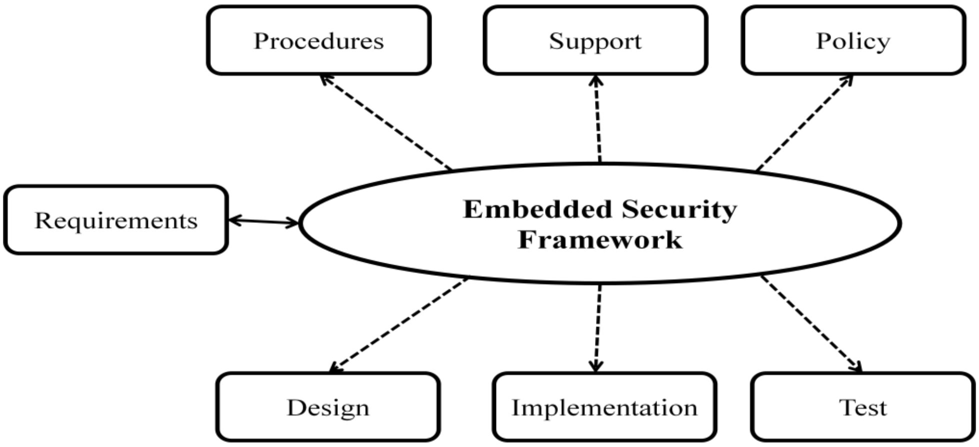

Figure 2: Embedded Security Framework

The basic idea for framing the embedded security architecture for IoT is to utilize security mechanisms and protocols effectively and to start off with a design that takes security into consideration from the start of requirements gathering to maintenance as seen in Figure 3 following the software development life cycle.

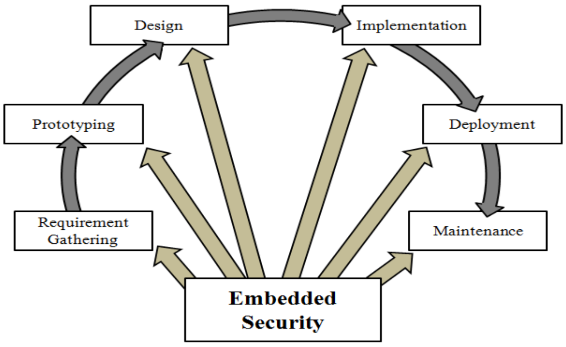

Figure 3. Embedded Security Design Steps

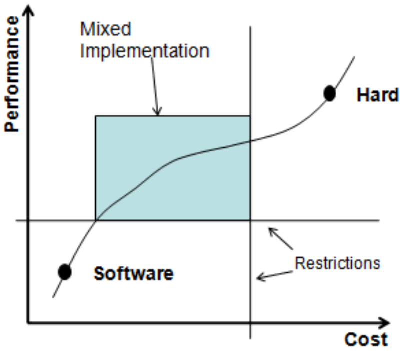

Figure 4. Hardware Software Security implementation performance

For building the embedded security Framework, we need to look at all of the tradeoffs between performance, cost, and security. Unfortunately, these three concepts are almost always directly at odds with one another. More performance means the cost goes up, lowering the cost means lowering security and performance, and implementing higher security means performance(time & space efficiency) will decrease.

A hardware software based security processing architecture for IoT is required which should give the best trade off cost/efficiency or security/performance as shown in figure 4.

A cost effective designs use a mixture of hardware and software to accomplish overall Security goals. This provides sufficient motivation for attempting a synthesis-oriented approach to achieve Security system implementations having both hardware and software components. Such an approach would benefit from a systematic analysis of design trade-offs that is common in synthesis while also creating cost effective systems. So the main goal of the research topic is to design and implement an optimized embedded security framework and architecture for IoT.

2.c State-of-Art

Following table 1 summarizes some publications with respect to countermeasures for attacks and optimization parameters.

Ref.	Name of publication	Counter measures against security attack			Optimisation Parameters			
		Side-channel countermeasure	HW-attack countermeasures	SW-attack Countermeasure	Energy Efficiency	Flexibility efficiency	Computational time	cost efficient
[6]	Implementing Embedded Security on Dual-Virtual-CPU System			√	√			√
[7]	A security approach for off-chip memory in embedded microprocessor systems			√				√
[8]	A compiler-hardware approach to software protection for embedded systems		√	√		√		
[9]	An FPGA implementation of a flexible secure elliptic curve cryptography processor			√		√	√	
[10]	Hardware - Software Implementation of Public-Key Cryptography for Wireless Sensor Networks			√		√		√
[11]	Embedded Security: New Trends in Personal Recognition Systems		√	√				√
[12]	A Data-Driven Approach for Embedded Security			√				
[13]	Secure Embedded Processing through Hardware-assisted Run-time Monitoring			√	√		√	
[14]	Mobile Device Security Using Transient Authentication		√	√		√		√
[15]	SPA resistant Elliptic Curve Cryptosystem using Addition Chains	√		√			√	

Table 1: Summary of State of Art

We conclude from the state of art that Side channel attacks and software attacks will be the crucial concerns for IoT and needs to be addressed accordingly with inbuilt security mechanisms.

The existing systems have following drawbacks:

- Inadequate to handle complex security requirement.
- Deficient in handling generic attacks
- No lightweight generalized solutions for resource constraint devices.
- No generic solutions for all types of things
- Not suitable for heterogeneous networks.
- Lagging in Performance Metrics

Comparison of Lightweight Cryptographic Algorithms

Following table 2 summarizes the comparison of lightweight cryptographic algorithms.[16-19]

Sr. No.	Algorithm	Key Bits	Block Bits	Cycles per Block	Technology / Logic Process (µm)	Area (GEs)	Throughput at 100 KHz (Kbps)
1	AES	128	128	1032	0.35	3400	12.40
2	HIGHT	128	64	34	0.25	3048	188.20
3	Present	80	64	32	0.18	1570	200.00
4	Clefia	128	128	36	0.09	4993	355.56
5	mCrypton	96	64	13	0.13	2681	492.30
6	DESL	64	64	144	0.18	1848	44.40
7	DESXL	184	64	144	0.18	2168	44.40
8	Camellia	128	128	20	0.35	11350	640
9	TEA	128	64	-	-	2100	-
10	SEA	96	96	-	0.13	449	-
11	KTANTAN	80	64	-	0.13	688	25.1
12	Trivium	80	1	1	0.13	2599	100.00
13	Grain	80	1	1	0.13	1294	100.00

Table 2: Comparison of Lightweight Cryptographic Algorithms

The unusual design constraints for IoT requires a lightweight secure scheme that that provides high levels of security while minimizing memory, execution speed and power requirements. AES is suitable for IoT environment with reduced number of rounds during key generation process and maintaining the same level of security. Existing research have claimed that ECC will also be an essential methodology for meeting the requirements of embedded designs and it will play a crucial role in enhancing embedded security.

Following table 3 shows the comparative chart for security evaluation for the broad key management schemes[20-21].

Table 3 : Security Evaluation of Key Management Schemes

Sr. No	Key management Scheme	Evaluation Parameters				
		Resilience against node capture	Resistance against node replication	Scalability with dynamic support	Revocation of compromised node	Efficient Resource consumption
1	Single network wide key	N	N	Y	N	Y
2	Trusted Base Station	Y	Y	N	Y	N
3	Hybrid Cryptography	Y	Y	Y	N	N
4	Probabilistic Key Pre-distribution	P – Y *	Y	Y	P	P – Y
5	Deterministic Key Pre-distribution	Y	P	P	P	Y
6	ID based one way hash function	P	P	P	P	Y
7	Key infection Schemes	Y	Y	N	Y	Y
8	Pairwise key establishment	Y	N	N	Y	P

Y : Good Support P : Partial Support N : No Support

* Resiliency increases if more keys are put into key ring
Based on the comparative chart it is concluded that there is a need for dynamic key generation process for embedded devices which will satisfy the security requirements of future Internet.

2.d Statement of the Research Objective

The research Objectives are:

- To specify and design optimized lightweight secure techniques with hardware software co-design approach.
- To develop a Trusted Platform module that will taken into account the vulnerabilities of the hardware device at physical level.
- To develop a robust and attack resistant system against side channel attacks, software attacks, etc.
- To develop standardized security protocols which are both lightweight with respect to communication and cryptographic computations.
- Find a balance between cost and performance for embedded security.
- To design and implement embedded security framework and architecture for IoT.

2.e Key Methods

There are a number of key properties of IoT that create several issues for security and raises additional requirements for security:

1. Embedded Use: Major IoT devices have a single use (e.g., blood pressure or heart monitors and household appliances). As a result, the detection of communication patterns unique to a specialized device allows users to be profiled.
2. Diversity: These devices span a range of computational abilities from full-fledged PCs to low-end RFID tags. Privacy designs must accommodate even the simplest of devices.
3. Scale: These devices are convenient, growing in number daily, and increasingly embed network connectivity into everyday settings. This makes it difficult for users to monitor privacy concerns.
4. Scarcity of resources: The computation power available in IoT is limited and may be insufficient for the processing of security algorithms. The battery capacity is also limited and their life duration is strongly connected to the quantity of computation executed in the embedded processor. Storage limitations also are hurdles for embedding security features.

Side channel attacks and Software attacks are the major attacks that need to be tackled for framing a secure architecture.

Side Channel attacks: These are based on “side channel Information” that can be retrieved from the encryption device that is neither the plaintext to be encrypted nor the ciphertext resulting from the encryption process. Encryption devices produce timing information that is easily measurable, radiation of various sorts, power consumption statistics, and more. Side channel attacks makes use of some or all of this information to recover the key the device is using. It is based on the fact that logic operations have physical characteristics that depend on the input data[22].

The main side channel attacks are :

1. Timing Attacks : These attacks are based on measuring the time it takes for a unit to perform operations. By carefully measuring the amount of time required to perform private key operations, an attacker might find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems.

2. Power Analysis Attacks: These attacks are based on analyzing the power consumption of the unit while it performs the encryption process i.e. the operating current drawn by a hardware device is correlated to computations it is performing.
    - Simple Power Analysis: This type of attack is generally based on looking at the visual representation of the power consumption of a unit while an encryption operation is being performed.
    - Differential Power Analysis: It is based on visual and statistical analysis and error-correction statistical methods to obtain information about the keys.
3. Fault Analysis Attacks: Fault analysis relates to the ability to investigate ciphers and extract keys by generating faults in a system that is in the possession of the attacker, or by natural faults that occur. Faults are most often caused by changing the voltage, tampering with the clock, or by applying radiation of various types.
4. Electromagnetic Attacks: These types of attacks attempt to measure the electromagnetic radiation emitted by a device to reveal sensitive information. Like power analysis attacks, two classes of EMA attacks, namely, simple EMA (SEMA) and differential EMA (DEMA) attacks have been proposed.

Software Attacks: Software Attacks are the major source of security vulnerabilities in any system. These problems are due to three main parameters i.e. Complexity, Extensibility & Connectivity. Software attacks exploit implementation vulnerabilities in the system through its own communication interface. This kind of attack includes exploiting buffer overflows and using Trojan horse programs, worms or viruses to deliberately inject malicious code into the system [22]. Once the malwares get into the system, they can corrupt code and data of programs in the system. These malwares also have the ability to leak critical information out of the system. Most of these malwares try to take advantage of some shortcomings that exist in softwares. Buffer overflow attacks and format string attacks are examples of this. Vulnerable programs can also put operating system kernel at risk. The operating system has full access of the system and can communicate with any part of the address space. As such, malware can attack the kernel and jeopardize any parts of the memory including BIOS memory. A malware can even get written into the motherboard memory or device peripherals memory and go totally unnoticed. Attackers can use viruses, worms and Trojan horses that target these software shortcomings to gain unauthorized access to systems. Wireless Physical layer security approaches[23] can be adapted for protection against software attacks.

2.f Potential Significance and Applications

The expected output of the research is analyze the security requirements for IoT like Tamper resistance, Secure authentication, Secure storage, Key management, Inter-operatability and mapping the requirements to existing solutions and listing the requirements which will create major difference in IoT environment. The limited resources available in IoT environment raises serious barrier to implementing adequate security to our application. So to overcome these barriers we have to find a balance between security, cost and performance with proper hardware software partitioning of security features. Security has to be taken care at all levels right from manufacturing the device to deployment phases. There is a need for optimized lightweight solutions suitable for IoT environment with strong resistance against side channel and software attacks. Embedded security is application dependent. Applications areas will cover all sectors including Retail, Logistics, Pharmaceutical, Food, Health, Intelligent Home, Transportation, Military, Online shopping, etc.

2.g Time Schedule

TIME SCHEDULE FOR PhD RESEARCH WORK (3 years Plan)

Sr. No	Topics	Year 1				Year 2				Year 3			
1	Literature Survey and Background Study	■	■										
2	Concept Development		■										
3	Problem Formulation		■	■									
4	Security analysis, Evaluation and Verification			■	■								
5	Security requirements & Threat model for IoT				■	■	■						
6	System Modeling and Architecture Development						■	■	■				
7	Study of lightweight Techniques/ Protocols						■	■					
8	Design of Hardware Software Architecture								■	■			
9	Implementation and Validation									■	■		
10	Optimization and Refinement										■	■	
11	Write of the Thesis										■	■	■
12	Attending PhD Courses **	■			■	■			■	■			
13	Paper writing (Journal and conferences)		■	■	■	■	■	■	■	■	■	■	■
14	Stay abroad*		■	■	■	■		■	■	■	■	■	

* **3 months** at AAU & **9 months** at INDIA (GISFI, Lonavala) every year (Will be working with AAU supervisors & GISFI Indian co-supervisor)

** Courses organized by AAU through video conferencing related to research topic.

MILESTONES:

These are the milestones planning to achieve as part of my PhD with tentative months.

- **Milestone 1 (M3):** Completed the literature survey of Security for Embedded Systems and software & hardware based security processing architectures for embedded devices.
- **Milestone 2 (M3):** Determined motivations, questions and research challenges and problem specifications.
- **Milestone 3(M6):** Defined the functional requirements which included detailed attacks, vulnerabilities and threat analysis and the necessary extensions and novel developments. A Conference paper titled “Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)" was published.
- **Milestone 4(M12):** Worked on software & hardware based security processing architecture for resource constrained devices and adapting them to IoT without compromising their robustness. A Conference paper titled “Proposed Embedded Security Framework for Internet of Things (IoT)” was published.
- **Milestone 5 (M15):** Design of optimized Cryptographic algorithms and their efficient implementation in hardware and software for resource constrained devices. A conference paper titled “Proposed on Device Capability based Authentication using AES-GCM for Internet of Things(IoT)” was published.
- **Milestone 6 (M18):** Design of embedded secure storage platform with efficient memory management and memory protection unit. A survey paper titled “Key Management schemes for Wireless Sensor Networks : A Survey” submitted for review.
- **Milestone 7 (M20):** Enhancing Physical layer security techniques for embedded security and to prepare a mathematical security model. Plan to submit a Journal paper.

- **Milestone 8(M24):** To work on hardware architecture and design of a hardware software embedded Security processing architecture and framework.
- **Milestone 9 (M24):** To finish the courses and complete 30 ECTS and submission of conferences / Journal Paper.
- **Milestone 10 (M30):** To validate methods using system level simulation and test bed developments, and try to combine all the previous work.
- **Milestone 11 (M32):** Submission of Journal Papers.
- **Milestone 12 (M34):** To start writing thesis and simultaneously do refinements towards finishing PhD, by the end of M34.
- **Milestone 13 (M36):** Wind up the PhD work, and publish the all the work done.

2.h Outline of the content of the Thesis

Below is the brief outline of the thesis.

Chapter 1 : Introduction

- Background
- Security Requirements for IoT
- Need for Embedded Security
- Previous work
- Problem specification and definition

Chapter 2 : Security Analysis, Evaluation and Verifications

- Security requirement
- Analysis and verification
- Evaluation and verification of the security Interfaces
- Security Mechanisms and protocols for Resource constrained devices

Chapter 3: System Model

- Design of Crypto Algorithms / Protocols
- Design of Software and Hardware Architecture

Chapter 4: Implementation

- Heterogeneous HW/SW development Platform
- Design Methodology
- Refinement and Optimization

Chapter 5: Simulation methods

Chapter 6: Conclusions and future work

Appendix (Reference)

2.i Publication Plan

The Plan is to publish two Journal papers during the course of Phd work, in high quality security related journals as given below.

Journal

- Sachin Babar, Neeli Prasad, Jaydip Sen and Ramjee Prasad , “Enhancing Physical layer security for Internet of Things (IoT)”, ACM Transactions on Information and System Security. (**Working Title**)
- Sachin Babar, Neeli Prasad, Jaydip Sen and Ramjee Prasad , “Embedded Security framework and architecture for Internet of Things (IoT)”, Springer Wireless Personal Communication Journal. (**Working Title**)

Conferences

- Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT)" , The

Third International Conference on Network Security and Applications (CNSA 2010), Recent Trends in Network Security and Applications, Communications in Computer and Information Science, 2010, Volume 89, Part 2, 420-429. **(Accepted & Published)**

- Parikshit Mahalle, Sachin Babar, Neeli R. Prasad and Ramjee Prasad, "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges" , The Third International Conference on Network Security and Applications (CNSA 2010), Recent Trends in Network Security and Applications, Communications in Computer and Information Science, 2010, Volume 89, Part 2, 430-439. **(Accepted & Published)**
- Sachin Babar, Antonietta Stango, Neeli Prasad, Jaydip Sen and Ramjee Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)" , 2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, Wireless VITAE 2011, vol., no., pp.1-5, Feb. 28 2011 - March 3 2011. **(Accepted & Published)**
- Sachin Babar, Parikshit Mahalle, Neeli Prasad and Ramjee Prasad, " Proposed on Device Capability based Authentication using AES-GCM for Internet of Things(IoT)" , 3rd International ICST Conference on Security and Privacy in Mobile Information and Communication Systems, May 17-19, 2011 - Aalborg, Denmark.
  (Accepted & Published)
- Sachin Babar, Neeli Prasad, Jaydip Sen and Ramjee Prasad, Conference paper “Key Management schemes for Wireless Sensor Networks : A Survey”, **(Submitted for Review).**
- Sachin Babar, Neeli Prasad, Jaydip Sen and Ramjee Prasad, Conference paper “A Novel lightweight secure solution for resource constrained devices”, **(Working Title).**

Conference papers will be published as well along the three years of the PhD.

SECTION 3: AGREEMENT ON THE RELATIONSHIP BETWEEN SUPERVISOR AND STUDENT

1. **Roles:** The student and the supervisors are together responsible for time management in the project. Time plan for the Ph.D. study will be reviewed by supervisors every six months.
2. **Type of collaboration:** Research Report prepared by PhD student is reviewed by Supervisors through formal meetings and discussions. Feedback regarding the progress and quality of work will be given during the meetings, conferences and workshops. Common documents will be distributed and maintained via e-mail and/or AFS servers at AAU.
3. **Supervision meetings:** Telephone / Skype meetings every second week between the student and the AAU and Indian supervisors. Telephone conferences every two months for all PhD students, supervisors and manager. Meetings twice a month between the student and the Indian supervisors.
4. **Workplace participation:** The student will be able to get access to lab equipment and technical assistance from both AAU and India. In cases when advanced equipments are required, the student will make a request at least one month in advance and the supervisors should help the student as much as they can. The student will get involved in research groups at AAU and TCS labs, Kolkata India.

5. **Writing papers:** Paper writing is on the basis of collaboration between the student and the supervisors. In most of cases, the student prepares the first draft and the supervisors give feedback and comments timely.
6. **Developing the cooperation and updating the agreement:** At Regular intervals PhD students and supervisors can discuss the potential needs for updating the agreement and for any modifications will consult with the department or the Research school. This agreement will be evaluated every six months.

SECTION 4 : PHD COURSES PLAN

Plan for PhD Courses adding up to 30 ECTS Points *

Name of the Course	Place/ Organizer (AAU)	Research related / General course	Status	ECTS
Introduction, What is IoT ? IoT application, Synergistic Technologies.	Neeli Prasad , Albena Mihovska , Zheng Tan, Ole Madsen ,Jens Erik Pederson	Research	Completed	1
Intellectual Property Rights	Lisbeth Tved Linde	General	Completed	2
Vehicle Communication	Tatiana Kozlova	Research	Completed	3
Air Interface Design for Future Wireless Systems – Towards Real 4G and Cognitive Radio	Ramjee Prasad, Frederikson, Suvra Das, Nicola Marchetti	Research	Completed	4
Sensors and RFID Networks	Neeli Rashmi Prasad	Research	Completed	3
Distributed source coding and Multiple descriptions	Jan Østergaard	Research	Completed	3
Seminar for scientists-patenting and commercialization	Nicolla Marchetti	Project	Completed	1
Analysis and design of high performance future internet infrastructure	Jens Myrup Pedersen, M. Tahir Riaz, Anna Tzanakaki	Research	Completed	2,0
Bayesian statistics, simulation and software -With a view to application examples	Kasper K. Berthelsen, Søren L. Buhl	General	Completed	3,0
Physical-layer security, From markov renewal models to mean field limits. (Organized at IISc, Bangalore)	Matthieu Bloch (Georgia Tech- Lorraine) Anurag kumar (IISc, Bangalore)	Research	Completed	-
Subtotal (Completed)				**22**
Writing and reviewing scientific papers	Jakob Stoustrup ,Jan Dimon Bendtsen	General	Registered	3,75
Special Courses for GISFI PhD Students / Conference / Tutorials*	I4CT, India	Research	Planned*	5
Subtotal (Planned)				**8,75**
Total (completed and planned)				**30,75**

* Will be decided in consultation with Supervisor.

**Above list is Based on the 2011 PhD Courses Catalogue. This list may change according to the courses available in India and Denmark.

SECTION 5: PLAN FOR DISSEMINATION OF KNOWLEDGE

- Most of the findings from the research work are going to be published in official conferences and included in the IEEE database according to the standard proceedings.
- Furthermore, depending on the quality of the future results, other ways of dissemination - as newspaper articles, seminars, etc. will be considered.
- Depending on the solution and the application, some findings can be published as patents.

SECTION 6: AGREEMENTS ON IMMATERIAL RIGHTS TO PATENTS

All the rights about patents obtained during the PhD course will be shared between the university and the PhD student, following the standard procedures in AAU.

SECTION 7: PLAN FOR EXTERNAL COLLABORATION

It is planned to work along with research groups of Tata Consultancy Services, Kolkata, India.

SECTION 8: FINANCING BUDGET FOR THE PHD

CTiF, Aalborg University will provide the research facility.

Expenses for tuition fee, lodging, boarding and travelling will be borne by STES, Pune (India)

SECTION 9 : LIST OF REFERENCES

[1]. Paul Kocher, Ruby Lee, Gary McGraw, Anand Raghunathan / Srivaths Ravi, "Security as a new dimension in embedded system design", June 2004, DAC '04: Proceedings of the 41st annual Design Automation Conference , Publisher: ACM

[2]. Christof Paar, André Weimerskirch, “Embedded security in a pervasive world” , Information **Security** Technical Report, 2007 – Elsevier , Volume 12, Issue 3, 2007, Pages 155-161.

[3]. Matthew Eby, Jan Werner, Gabor Karsai, Akos Ledeczi, "Embedded systems security co-design" , April 2007, SIGBED Review , Volume 4 Issue 2 ,Publisher: ACM

[4]. Ukil, A.; Sen, J.; Koilakonda, S.; , "Embedded security for Internet of Things," Emerging Trends and Applications in Computer Science (NCETACS), 2011 2nd National Conference on , vol., no., pp.1-6, 4-5 March 2011

[5]. Eric Uner, “A Framework for Considering Security in Embedded Systems”, Embedded.com, Sept. 2005.

[6]. Wilson P, Frey A, Mihm T, Kershaw D, Alves T., "Implementing Embedded Security on Dual-Virtual-CPU Systems" , Design & Test of Computers, IEEE Volume 24, Issue 6, Nov.-Dec. 2007

[7]. Romain Vaslin, Guy Gogniat, Jean-Philippe Diguet, Eduardo Wanderley, Russell Tessier, Wayne Burleson, "A security approach for off-chip memory in embedded microprocessor systems", Microprocessors and Microsystems, Volume 33, Issue 1, February 2009, Pages 37-45

[8]. Olga Gelbart, Eugen Leontie, Bhagirath Narahari, Rahul Simha, “A compiler-hardware approach to software protection for embedded systems”, Computers and Electrical Engineering 35 (2009) 315–328, 2008 Elsevier Ltd.

[9]. T. Kerins, W.P. Marnane E.M. Popovici: An FPGA Implementation of a Flexible Secure Elliptic Curve Cryptography Processor. Distinguished Paper. International Workshop on Applied

Reconfigurable Computing ARC 2005, Proceedings, pp.22-30, IADIS press.

[10]. Murphy, Gerard; Keeshan, Aidan; Agarwal, Rachit; Popovici, Emanuel,"Hardware - Software Implementation of Public-Key Cryptography for Wireless Sensor Networks ", Irish Signals and Systems Conference, 2006. IET , 28-30 June 2006 Page(s):463 – 468.

[11]. Fons, M.; Fons, F.; Canto, E.;"Embedded security: New trends in personal recognition systems"; Microelectronics and Electronics Conference, 2007. RME. Ph.D. Research in 2-5 July 2007.

[12]. Saputra, H.; Ozturk, O.; Vijaykrishnan, N.; Kandemir, M.; Brooks, R.;"A data-driven approach for embedded security" ; VLSI, 2005. Proceedings. IEEE Computer Society Annual Symposium on 11-12 May 2005 Page(s):104 - 109.

[13]. Arora, D., Ravi, S., Raghunathan, A., and Jha, N. K. 2005.Secure Embedded Processing through Hardware-Assisted Run-Time Monitoring. In *Proceedings of the Conference on Design, Automation and Test in Europe - Volume 1* (March 07 - 11, 2005). Design, Automation, and Test in Europe. IEEE Computer Society, Washington, DC, 178-183.

[14]. Anthony J. Nicholson, Mark D. Corner, Brian D. Noble, "Mobile Device Security Using Transient Authentication," IEEE Transactions on Mobile Computing, pp. 1489-1502, November, 2006

[15]. Andrew Byrne, Francis Crowe , William Peter Marnane , Nicolas Meloni , Arnaud Tisserand , Emanuel Popovici , "SPA resistant elliptic curve cryptosystem using addition chains", International Journal of High Performance Systems Architecture [1751-6528] yr:2007 vol:1 iss:2

[16]. Panasayya Yalla, Jens-Peter Kaps, "Lightweight Cryptography for FPGAs," Reconfigurable Computing and FPGAs, International Conference on, pp. 225-230, 2009 International Conference on Reconfigurable Computing and FPGAs, 2009

[17]. Thomas Eisenbarth, Sandeep Kumar, Christof Paar, Axel Poschmann, Leif Uhsadel, "A Survey of Lightweight-Cryptography Implementations," IEEE Design and Test of Computers, pp. 522-533, November-December, 2007

[18]. S. Kumar, "Elliptic Curve Cryptography for Constrained Devices," doctoral dissertation, Electrical Engineering and Information Sciences, Ruhr University Bochum, Germany, 2006.

[19]. Özen, O., Varıcı, K., Tezcan, C., and Kocair, Ç. 2009. Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT. In Proceedings of the 14th Australasian Conference on information Security and Privacy (Brisbane, Australia, July 01 - 03, 2009). C. Boyd and J. González Nieto, Eds. Lecture Notes In Computer Science, vol. 5594. Springer-Verlag, Berlin, Heidelberg, 90-107.

[20] Xiangqian Chen; Makki, K.; Kang Yen; Pissinou, N.; , "Sensor network security: a survey," Communications Surveys & Tutorials, IEEE , vol.11, no.2, pp.52-73, Second Quarter 2009.

[21] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: A survey," Computer Science Department at RPI Tech, Rep. TR-05-07, 2005.

[22]. Srivaths Ravi, Anand Raghunathan, Paul Kocher, Sunil Hattangady , "Security in embedded systems: Design challenges " ,August 2004 , Transactions on Embedded Computing Systems (TECS) , Volume 3 Issue 3 , ACM

[23]. Lun Dong; Zhu Han; Petropulu, A.P.; Poor, H.V.; , "Improving Wireless Physical Layer Security via Cooperating Relays," Signal Processing, IEEE Transactions on , vol.58, no.3, pp.1875-1888, March 2010