COST Action IC1403: CRYPTACUS

CRYPTAnalysis of Ubiquitous Computing Systems

Improve the security and privacy of ubiquitous computing systems, from theory to practice.

Dec. 2014-2018

MC Chair: Gildas Avoine, INSA Rennes, France

MC Vice-Chair: Julio Hernandez-Castro, Univ. of Kent, UK

Grant Holder Manager: Isabelle Mesguen, INSA Rennes, France

COST Science Officer: Luule Mizera

COST Administrative Officer: Leo Guilfoyle

cost
EUROPEAN COOPERATION
IN SCIENCE AND TECHNOLOGY

Adoption of the Agenda

- Agenda
- Welcome
- Minutes
- Update from Chair
- Update from GH
- Update from COST
- Gender Balance
- MoU Objectives
- Scientific Planning
- Promotion
- AoB
- Next Meeting
- Decisions
- Closing

Agenda was sent with the official invitation.

1. Welcome to participants and adoption of agenda
2. Approval of minutes and decisions since last meeting
3. Update from the Action Chair
4. Update from the Grant Holder
5. Update from the COST Association
6. Promotion of gender balance and of Early Career Investigators (ECI)
7. Follow-up of MoU objectives
8. Scientific planning
9. Promotion of the Action
10. AoB
11. Location and date of next meeting
12. Summary of MC decisions
13. Closing

Welcome to Participants

- New MC Members (since last meeting)
  - New country : Montenegro.
  - Milena DJUKANOVIC, Montenegro
  - Marios Omar CHOUDARY, Roumania
- Number of represented countries in the Action: 30
- Number of represented countries in the meeting ?
  - Quorum to vote if greater than or equal to 20
- Signature of the attendance list (to be reimbursed)

COST Actions

- COST aim: develop scientific networks
- Budget can only fund networking activities
- COST Actions: 4 years (Dec. 2018)
- Budget negotiated every year
- Working groups, short-term scientific missions (visit a lab during a few weeks or months), organization of a conference or training school
- COST does not fund: attendance to a conference, financial support for a conference.

Organization

- Agenda
- Welcome
- Minutes
- Update from Chair
- Update from GH
- Update from COST
- Gender Balance
- MoU Objectives
- Scientific Planning
- Promotion
- AoB
- Next Meeting
- Decisions
- Closing

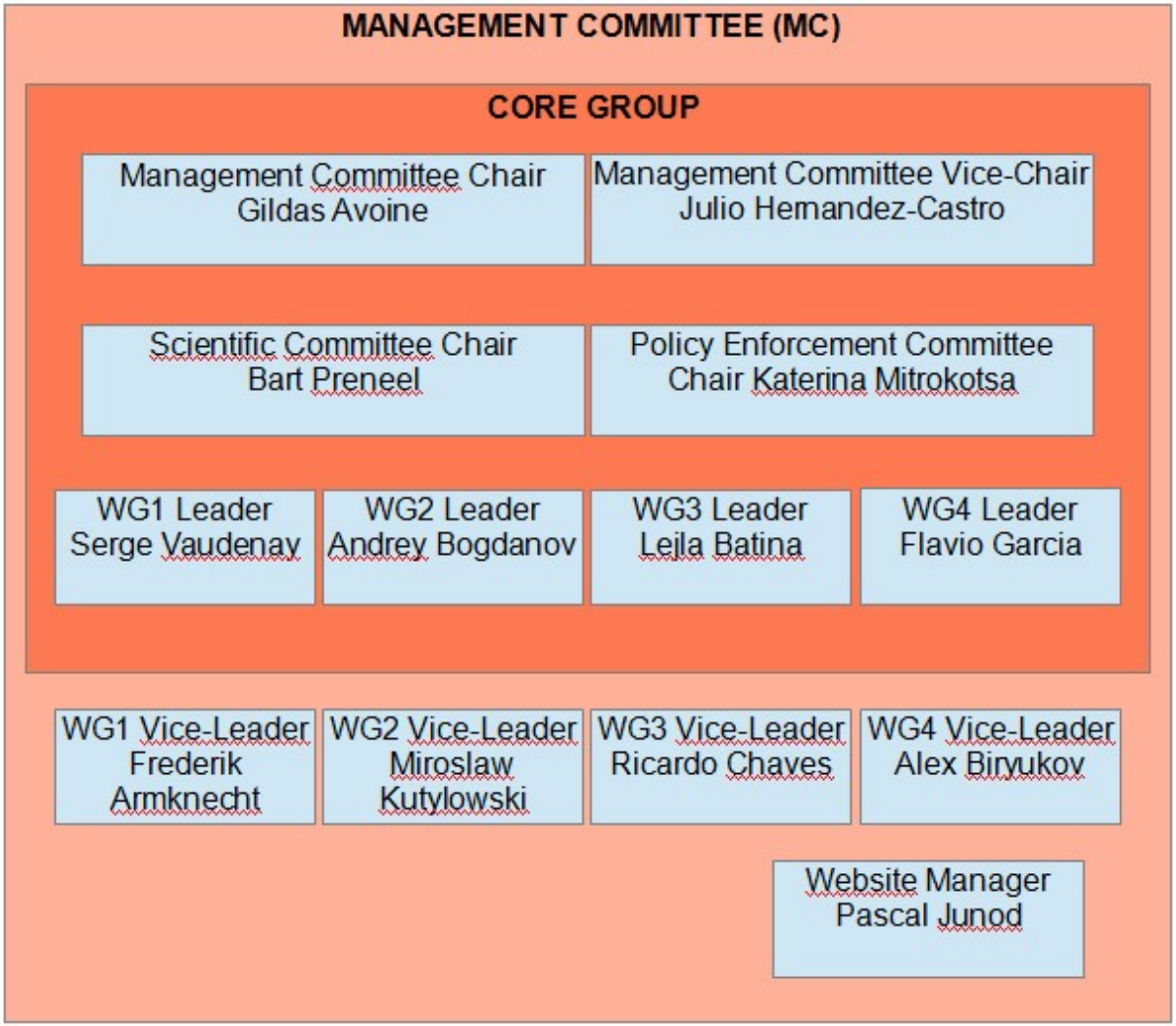
Year1				Year2				Year3				Year4			
01-03	04-06	07-09	10-12	13-15	16-18	19-21	22-24	25-27	28-30	31-33	34-36	37-39	40-42	43-45	46-48
					WS	TS			WS	TS			WS		CNF
			WG1		WG1		WG1		WG1		WG1		WG1		
			WG2		WG2		WG2		WG2		WG2		WG2		
			WG3		WG3		WG3		WG3		WG3		WG3		
			WG4		WG4		WG4		WG4		WG4		WG4		
KO			MC		MC		MC		MC		MC		MC		MC

Documents and Tools

- Memorandum of Understanding (**MoU**).
- COST **Vademecum**.
- **E-COST** online application.
- Cryptacus **website** (www.cryptacus.eu).
- **Work and Budget Plan** of considered Grant Period

Organigram

- Agenda
- Welcome
- Minutes
- Update from Chair
- Update from GH
- Update from COST
- Gender Balance
- MoU Objectives
- Scientific Planning
- Promotion
- AoB
- Next Meeting
- Decisions
- Closing



Approval of Minutes and Decisions

- Approval of the minutes of Haifa meeting (29/03/16)
- Decision that will be included in the minutes of this meeting: Montenegro becomes a member of Cryptacus (Approved: Unanimity)

Update from the Action Chair

- MC Chair sends a W&B plan proposal for discussion.
- MC Chair sends the (unapproved) minutes of Haifa's meeting.
- MC Chair puts on the website the official acknowledgment to be included in published articles.
- Put the slide of the MC Meeting on the website.
- Create a newsletter
  - cryptacus@irisa.fr
  - cryptacus.newsletter@irisa.fr
- Create flyers.

Update from the Action Chair

"This article is based upon work from COST Action CRYPTACUS, supported by COST (European Cooperation in Science and Technology)".

Note also that "COST must also orally be acknowledged during all news media interviews, conferences and events where COST Action representatives give a public presentation or participate to a session or panel."

Update from the Grant Holder

- Grant Holder: INSA Rennes, France
- GH Administrative Manager: Isabelle Mesguen
- GH Scientific Representative: Gildas Avoine
- Difficulties to launch the new GP because:
  - Too long to decide about next location.
  - Several STSM canceled.
  - Invitations sent earlier than last time.
  - Several people invited to attend the WG meetings with the remainig budget.

Budget Plans

COST Action IC1403 Cryptacus						
Grant Period		Allocated budget	Reimbursement		STSM	Final Grant amount
			MC meeting participants	Training School participants		
1	2015-03-01 / 2015-09-30	70,344.35 €	26	15	1	38,126.21 €
2	2015-10-01 / 2016-04-30	121,590.33 €	17	14	5	94,982.00 €
3	2016-05-01 / 2017-04-30	139,495.00 €	33	-	1	

Update from the COST Association

- No message received

Promotion of Gender Balance,…

- Three important criteria for the COST Association:
  - Promotion of gender balance
    - 4 STSMs (female)
  - Promotion of Early Career Investigator (ECI)
    - 7 STSMs paid or accepted
  - Promotion of Inclusiveness Countries
    - MC/WG/TS Meeting in Croatia
    - 3 WG vice-leaders (among 4) are from IC.

Promotion of Gender Balance,…

Applicant	Home	Host	Contact person in Host university	STSM Topic	Duration (days)	Grant
Clémentine MAURICE	Sophia-Antipolis	Graz	Mangard	Bringing together techniques from physical side-channel attacks to cache-based side-channel attacks	13	1,050.00 €
Eduard MARIN	Leuven	Birmingham	Garcia	Security and privacy analysis of a pacemaker	14	1,525.00 €
Atul LUYKX	Leuven	Lyngby	Bogdanov	Collaboration on Authenticated Encryption	7	850.00 €
Veelasha MOONSAMY	Nijmegen	Leuven	Preneel	Application of side channel analysis to smartphone's power consumption Android malware classification	10	1,050.00 €
Qinju WANG	Leuven	Graz	Mendel	Cryptanalytic techniques of symmetric-key primitives	11	1,100.00 €
Sohail UL HASSAN	Tampere	Bristol	Page	Side Channel Analysis of Complex Embedded Systems	5	950.00 €
Bei LANG	Gothenburg	Zurich	Perrig	erificable delegation of computation	21	2,500.00 €

Follow-up of the MoU Objectives

- Third scientific meeting
- Use Cryptacus to find partners to set up H2020 consortia.
- Andrey suggested to work on guidelines about lightweight cryptography. This would be a traversal axis.
- Publish STSMs proposals in the newsletter.

Scientific Planning

Workshop during Grant Period 3. Proposal to be discussed, now:

- 2- or 3- day workshop
- Submitted talk: abstract (1 page), informal booklet of the abstracts.
- Up to 4 invited speakers (outside COST countries).
- Accepted speakers from COST countries: expenses will be reimbursed. Up to 10 or 15 speakers should be ok (to be checked).
- LOS: 20 € / day / participant (e.g., 2400 €)

Promotion of the Action

- Website
  - Website Manager is Pascal Junod (CH)
  - Website is up. Comments are welcome
- Flyers
  - MC Chair should create flyers (spread in conferences)
  - Mailing list for the Action (not only MC Members).
    - cryptacus@irisa.fr
    - cryptacus.newsletter@irisa.fr

Any other Business

Agenda
Welcome
Minutes
Update from Chair
Update from GH
Update from COST
Gender Balance
MoU Objectives
Scientific Planning
Promotion
AoB
Next Meeting
Decisions
Closing

- Floor is open for discussion

Location of Next Meeting

- Next location should be announced before Xmas.
- Approval will be requested early in December.

Summary of MC Decisions

- Decisions:
  - Quorum not obtained
- Tasks:
  - MC Chair sends the (unapproved) minutes of Sophia-Antipolis' meeting.
  - MC Chair creates flyers.
  - MC Chair and Scientific Committee Chair wait for pre-proposals for the workshop organization until Nov 15.

Closing

- Thanks for coming.
- Big thanks to Aurélien Francillon and the local staff for the organization of the MC+WG Meeting in Haifa.