

**Minutes of the Management Committee Meeting**  
**May 31st, 2015**  
**Sibenik, Croatia**

\* The MC Chair opens the MC meeting at 17h35.

**1. Welcome to participants**

\* The Chair mentions that the vice-chair could not attend the meeting for medical reasons.

\* The secretary of the meeting is Pascal Junod (CH).

\* The Chair mentions that the Action's Science Officer is now Luule Mizera, instead of Ralph Stübner.

**2. Adoption of the agenda**

\* The Chair spreads the agenda, which was previously sent by e-mail to MC Members and Substitutes.

\* The Chair asks whether there are new points to be included into the agenda.

\* The Chair announces that a discussion about H2020 calls will happen right after the MC meeting. Denis Trcek (SI) and Peter Kieseberg (AT) will lead the discussion.

\* The Chair welcomes the new representatives. There are 23 new MC Members and Substitutes since the kick-off meeting, and four new countries, namely NO, RO, HU, FI, for a total of 28 participating countries.

\* 19 countries are necessary for the quorum; 18 countries are present, so the MC is not able to vote during the meeting.

\* The Chair recalls that the attendance list must be signed, for reimbursement purposes.

\* The Chair recalls the goals of the CRYPTACUS COST action for people who were not able to attend the meeting in Bruxelles in December 2014 (see slides in Annex 1 for details).

\* Serge Vaudenay asks about the future of funding (w.r.t. announced budget cuts). The Chair did not receive any official news from the COST office so far.

**3. Approval of minutes and matters arising since last meeting**

\* The Chair asks whether there is someone who disapproves the minutes of the meeting that happened in Brussels on Dec 12th, 2014. None disapproves. The minutes are approved.

\* The Chair mentions that the four decisions taken by e-voting in March 2015 will be put in these meeting's minutes. The decisions are the following ones:

**Decision 1:** The vice-leaders of the working groups are:

- WG1 Vice-Leader: Frederik Armknecht,
- WG2 Vice-Leader: Miroslaw Kutylowski,

- WG3 Vice-Leader: Ricardo Chaves,
- WG4 Vice-Leader: Alex Biryukov.

**Decision 2:** The members of the Policy Enforcement Committee are:

- Katerina Mitrokotsa, chair,
- Tsonka Baicheva,
- Amila Akagic,
- Lejla Batina,
- Aggelos Kiayias.

**Decision 3:** The MC delegates to the Action Chair (or, in the case of IC1403, the Vice Chair as the Action Chair is affiliated to the Grant Holder Institution) the task to decide from amongst eligible participants those trainers and trainees who are to be reimbursed to attend the training schools organized by the COST Action IC1403.

**Decision 4:** STSM applicants will be selected with the aim to promote scientific excellence; special attention will be paid to mainstreaming gender equality, development of collaborations with or within inclusiveness countries as defined by the COST Office, and support of Early Career Investigators.

#### **4. Update from the Action Chair**

\* The Chair mentions that any deviation from the W&B plan requires the COST office approval. This explains why the invitations for this meeting were sent later than expected.

\* The Chair mentions that 1 MC+WG meeting and 1 TS were organized so far, but only one STSM grant was awarded up to now. He encourages to apply for such grants, as there is money available. He mentions that the process is rather lightweight.

\* The Chair reviews the “tasks to be done” announced during the last MC Meeting that took place in Brussels on December 12th, 2014. The tasks still in progress include the website and the logo. They will highly likely be done before the next meeting. The website is not set up because the Grant Holder did not receive yet the money from the COST Association.

#### **5. Promotion of gender balance, Early Career Investigator (ECI), and Inclusiveness Countries**

\* The Chair shows the slides of Katerina Mitrokotsa. The Chair suggests to have one meeting in an inclusiveness country and one in a non-inclusiveness country per year, and to colocate the meeting with other scientific events. He mentions it is important to have a good balance between events related to cryptography, security, and privacy. The Chair hopes to attract more external people and companies into the WGs in the short-term future. It is possible to invite people for WGs. It is possible to have up to 4 invited talks per event from non-COST countries.

#### **6. Update from the Grant Holder**

\* The grant holder mentions that many exchanges between the Grant Holder and the COST Office were needed to launch the Action. Also the eCost application seems to suffer from many bugs. This explains the delays to launch the Action.

\* Many researchers involved in COST Actions believe the budgets of the COST Actions might be cut off in the future. The Chair hopes to keep the budget of Cryptacus unchanged, given the number of countries significantly increased. Serge Vaudenay mentions that there is a petition to be signed by people concerned by budget cuts on the COST website.

## **7. Update from the COST association**

\* No news received from the COST Association.

## **8. Follow-up of MoU objectives**

\* The Chair opens the discussion on the ways to improve the networking activities. Serge Vaudenay (CH) mentions that an earlier program for WGs would help. The Chair says that small groups of people could work on certain topics (homeworks) and the results would be presented at the next WG meeting. Lejla Batina (NL) mentions STSMs. Flavio Garcia (UK) mentions a competition between a building and a cryptanalysis team. He also proposes to make the next meeting in the form of a workshop, where people present their research. Lejla Batina proposes to colocate with CHES. Answering a question from the floor, the Chair mentions that the WG leaders and vice-leaders are free to organize additional WG meetings, but they will not be funded if they are not scheduled in the Work and Budget Plan. The Chair agrees that one important point is to organize the science-related meetings much more in advance.

\* The Chair mentions that it would be nice to have several H2020 projects within the COST participants. The Chair mentions that a project related to a COST Action should probably benefit from a higher acceptance rate than other projects.

## **9. Scientific planning**

\* The Chair looks for locations of meetings for the Grant Period 2. Applicants should contact the Chair of the Scientific Committee, namely Bart Preneel (BE).

## **10. Promotion of the Action**

\* Currently, the website is available at <https://cryptacus.eu>, but it redirects to the COST Action website.

## **11. Requests for new members**

\* The Chair mentions that it is important to promote the action and to have more people joining the action.

## **12. Non-COST applications to the Action**

\* The Chair was contacted by Dong Seong Kim (University of Canterbury, NZ) to join the action. The Chair asked him to send an official letter from the university. Next step will be an e-vote using the eCOST application if such a letter is received.

## **13. AoB**

\* The Chair opens the discussion about Any Other Business. No request from the floor.

#### **14. Location and date of next meeting**

\* The Chair announces a candidate (Crypto School in Sardinia 18-23/10/2015) to organize the next MC+WG Meeting. MC+WG Meeting would be on Oct. 17-18. A disadvantage is that it is not an inclusiveness country. As we cannot vote today, because the quorum is not obtained, the Chair suggests to wait for other candidates the next two weeks (say June 15th, 2015), and then vote. The Chair asks candidates to send an e-mail to Bart Preneel (BE).

\* Lejla Batina asked whether it is possible to reimburse non-MC members when MC Members do not show up. The Chair mentions that it is indeed possible, because such a rule was voted during the meeting 12/12/14: *“Invitations to attend meetings will be sent at least 30 calendar days in advance to Management Committee Members. MC Members and Substitutes who do not confirm their attendance at least 15 calendar days in advance will not be reimbursed. The Chair can decide to use the saved money to reimburse other participants. In such a case, the scientific committee will be requested to provide the Chair with a ranked list of candidates to be reimbursed. The MC delegates its authority to the MC Chair to apply this rule.”*

The Chair says that the rule was not apply for this meeting because the invitations were sent late, but it will be applied next time.

#### **15. Summary of MC decisions**

\* No decisions voted during the MC Meeting.

\* The Chair reviews the list of tasks to be done before the next meeting:

- MC Chair: send STSM call
- MC Chair: send 12/12/14's approved minutes
- MC Chair: send 31/05/15's unapproved minutes
- MC Chair: send GP1's W&B Plan (reminder)
- GH & Website Manager: set up the website
- All: Motivate ECI to apply for STSMs
- All: Spread flyers about Cryptacus
- All: Suggest activities to submit H2020 proposals

#### **16. Closing**

\* The Chair kindly thanks Stjepan Picek and Marin Golub for the organisation of the MC+WG meeting. [applauses]

\* The Chair closes the meeting at 18h50.