**Response to the Handling Editor and Reviewers**

**Submission No.:** MONE-D-16-00333

**Title:** Offline Mode for Corporate Mobile Client Security Architecture

**SM 188 – Sustainable Computing Techniques for Mobile Networks**

**Mobile Networks and Applications**

Dear Editor-in-Chief and reviewers,

The authors would like to thank the Associate Editor-in-Chief and the Reviewers for volunteering their time in reviewing our manuscript and providing us with valuable comments which allowed us to significantly improve the paper. We have carefully revised the manuscript based on the comments and suggestions. All changes in the paper have been marked with a color. The following is our point-by-point responses to the raised comments.

Kind regards,

The authors.

1. **EDITOR**
   1. **COMMENT: *Based on the advice received, your manuscript could be reconsidered for publication should you be prepared to incorporate major revisions.***
      1. **REPLY:** We thank the Editor for the time, work, and positive evaluation of our paper.
2. **REVIEWER #1**
   1. **COMMENT: *The paper presents a reasonable approach to offline mode for reading secure documents on mobile clients without consuming much of the device resources under a restricted adversary model.***
      1. **REPLY:** We thank this reviewer for the stimulating comments and for appreciating the contribution of our paper, as well as for the suggestions.
   2. **COMMENT: *The adversary model seems not complete. (1) The adversary model mentioned in Subsection 6.1 is not clear because affirmative statements are mixed with negative statements. (2) May the adversary disable the TIM?***
      1. **REPLY:** We arethankful for the constructive observations. We updated the adversary model description and separate positive and negative statements in order to clarify the assumptions. The TIM is an internal module of the mobile client that implements offline anomaly detection through signal processing techniques. Therefore, the TIM can not be disabled while the mobile client is running.

(?)

* 1. **COMMENT: *In Subsection 5.2, the description of ABE components is unclear: (1) typo of redundant double prime('') in PK, (2) no description of basic properties of bilinear paring function, (3) no description of the meanings of the notations w and s. (4) bad-form notation "for all i in {t\_i}\_M" (because "i" cannot belong to the set).***
     1. **REPLY:** We thank the reviewer for suggesting valuable corrections. We have corrected the cited typos (1) and made a review for similar errors. We complemented the text with a description of basic properties of bilinear paring function (2), added the description of *w* and *s* (3) and corrected the highlighted notation (4).

(?)

* 1. **COMMENT: *In Subsection 5.3, the description of SSS (modular secret sharing) is unclear: (1) Di is a typo, (2) the notation based on Chinese Remainder Theory (CRT) is not well presented, (3) the meanings of d, S, p\_0, and p\_1 are not clear, (4) What are the reasons for S being equivalent to s and s\_1 in modulo p\_0 and p\_1, respectively?***
     1. **REPLY:** We are thankful for the constructive observations. We have done modifications in onder to clarity the highlighted points. Following we present the changes.

(?)

* 1. **COMMENT: *In Subsection 6.2, it may be better to change "operations 1)-7)" to "actions 1)-7) (as mentioned in the offline mode)".***
     1. **REPLY:** We would like to thank the reviewer for this observation and communicate that we made the suggested modification.

(?)

* 1. **COMMENT: *There is little description about how to retrieve the logs from the Galaxy mobile devices and the correctness of anomaly detection in the experiments.***
     1. **REPLY:** We thank the reviewer for this constructive comment. We have improved the description of the User Activity Logging (UAL), which is responsible for the incremental logging of activities of the mobile client. The selected features monitored by the UAL for the evaluation of our proposal are described in subsection 6.1.4. The selected features are: File Access (Time and File System Location); File Update (Time and File System Location); File Download (Start Time, End Time and File System Location) and File Upload (Start Time, End Time and File System Location). The monitored features represents events of the user operating the mobile client. Therefore, the UAL, which is an internal module of the mobile client, can monitor and log the desired events for further analysis.

(?)

1. **REVIEWER #3**
   1. **COMMENT: *In the related work, these following references need to be considered to enhance the completeness of the work. Heydari, Mohammad, et al. "An efficient password-based authenticated key exchange protocol with provable security for mobile client-client networks." Wireless Personal Communications 88.2 (2016). Mayrhofer, René. "An architecture for secure mobile devices." Security and Communication Networks 8.10 (2015): 1958-1970. Shila, Devu Manikantan, et al. "AMCloud: Towards a Secure Autonomic Mobile Ad Hoc Cloud Computing System." IEEE Wireless Communications(2016). Chang, Hyunseok, et al. "Design and Architecture of a Software Defined Proximity Cloud." Advances in Mobile Cloud Computing Systems (2015): 123. Xia, Yubin, et al. "TinMan: eliminating confidential mobile data exposure with security oriented offloading." Proceedings of the Tenth European Conference on Computer Systems. ACM, 2015. Kulkarni, Pallavi, and Rajashri Khanai. "Addressing mobile Cloud Computing security issues: a survey." Communications and Signal Processing (ICCSP), 2015 International Conference on. IEEE, 2015.***
      1. **REPLY:** We are thankful for the valuable suggestion to enhance the completeness of the proposed work.

(?)

Pedir o livro pra alguém

* 1. **COMMENT: *More discussions on the figure 1 and 2 should be added. The current version is not easy to understand.***

## **REPLY:** We thank this reviewer for the observation. Figure 1 describes the mobile client protection both in online and offline mode. In online mode, the client has the possibility to connect to the server and the security of the client is enhanced by the server-backed up mechanisms. On the other hand, in offline mode the client’s security is supported by the standalone mechanisms. Additionally, the mobile client protection is enhanced by the threat intelligence unit providing the constant monitoring and analysis. Figure 2 depicts the client-side protection mechanisms. The client should support 4 subsystems: i) encryption subsystem that contains the procedures of encryption and decryption; ii) storage subsystem that provides the downloaded shares and key storage protection; iii) threat intelligence unit that provides the constant monitoring, and iv) the communication subsystem. In short, all security procedures are connected to 4 groups of operations: file request and receiving; encryption and decryption; file and key storing; monitoring and analysis.

* 1. **COMMENT: *The figure 8 should be explained more in detail.***

## **REPLY:** Tanya.

* 1. **COMMENT: *The formula 5 should be discussed more, the related sentence should be introduced with more theoretical support. The set of obtained vectors y(q)m composes the zero mean matrix Y(q), then the zero mean covariance ma-trix ^R(q)=yy can be calculated as follows.***

## **REPLY:** We thank the reviewer for this constructive comment to clarify the proposed work. Thiago.