A LIST OF CHANGES

January 20th, 2016

Paper Number: SCN-15-0766

Paper Title: An Escrow-Free Online/Offline HIBS Scheme for Privacy Protection of People-Centric Sensing

Authors: Peixin Chen, Jinshu Su, Baokang Zhao, Xiaofeng Wang and Ilsun You

Dear Editors,

We would like to take this opportunity to thank you for your handling of our paper as well as thank the reviewers for their careful checking of our paper and very constructive comments. We have carefully read the comments and revised the paper accordingly. We hope that the revised version satisfies the requirement for publication in Security and Communication Networks.

Enclosed please find the detailed responses to the reviewers. Please feel free to let us know if there are any additional concerns. We are looking forward to hearing from you.

Best regards,

Peixin Chen, Jinshu Su, Baokang Zhao, Xiaofeng Wang and Ilsun You

**Response to Reviewer 1’s Comments**

**Reviewer #1:**

In this paper, the authors develop a model to address the key escrow problem in HIBOOS scheme and instantiate the developed model in to a proved escrow-free HIBOOS scheme. The organization of the paper is clear and the presentation is easy to follow. There are following issues that the authors should consider about.

1) It is not entirely clear how the scheme differs from the situation where the user signs the message with a traditional IBS scheme and a conventional PKI, and then uses the combined signature. Here, also he needs the publish his user parameter (=public PKI key), and the receiver can decide whether to check both signatures or only one. It would be useful if the authors discussed the advantages/disadvantages of this setting compared to their proposal.

***Our response:***

This comment is really appreciated. As described by the reviewer, combining the traditional IBS signature and a conventional PKI signature can also achieve the same effect as our scheme. However, it has three disadvantages versus to our scheme:

1. As we described in the first paragraph of section 1, building and operating a PKI are quite burden jobs, which significantly reduce the practicability of the PKI-based scheme and can hardly be applied to the PCS scenario.
2. It has to verify two signatures in other to achieve the escrow-free property, but our scheme need only one signature verification and a user parameter comparison. Apparently, the cost of comparison is trivial comparing to the conventional PKI signature verifying, no matter how efficient the verifying algorithm is.
3. According to such scheme, a user has to maintain two signing keys: an IBS private key and a conventional PKI private key.

2) A more detailed description on the concept of online/offline signature scheme as well as related works is recommended, to oblige with a further understanding for readers.

***Our response:***

Thank you very much for your valuable comments. As a response, we have added a detailed description on the concept of online/offline signature scheme in the third paragraph of the section “1 Introduction”. Other than reviewing the related work of OO signature scheme, we have presented the related work of identity-based online/offline signature schemes.

3) Please add more recent published references, especially those published in the recent three years.

***Our response:***

We thank the reviewer for this valuable comment. After resurvey the previous work related to our work, we have added 4 more recent published references.

4) There are many long equations in the paper, which degrade the readability. Please consider use more concise equation or proofs.

***Our response:***

Thank you very much for this valuable comment. We have modified most of the long equations to make the paper more readability.

**Response to Reviewer 2’s Comments**

**Reviewer #2:**

Paper presents a new research on security and protecting the privacy of PCS (People-Centric Sensing) systems. Authors proposed an escrow-free hierarchical identity-based signature procedure, and using user selected secrets which may be used besides secret keys. Described protocol seems to be resistant for adaptive chosen-message cryptanalysis.

Some remarks towards paper improvements:

1) Section 2 is too short so please extend it or simply join with section 3.

***Our response:***

We thank the reviewer for this valuable comment. Section 2 in the previous version of our manuscript is indeed too short to be an independent section. As suggested, we have merged the previous section 2 and section 3 as a new section “2 OVERVIEW OF OUR ESCROW FREE HIBOOS MODEL”.

2) For identity based signature scheme described in section 3.2 may be placed a simple schema

***Our response:***

We thank the reviewer for this valuable comment. As a response, we have added a schema in section 2.3 to show the generic construction of our HIBOOS scheme.

3) Because presented method use user selected secret for signature generation please also make a reference to the paper:

M. R. Ogiela, U. Ogiela, Linguistic protocols for secure information management and sharing, Computers & Mathematics with Applications 63 (2), (2012), pp. 564-572.

***Our response:***

This comment is really appreciated. As a response, we have appended the following references for “solution to key escrow problem”,

29. M. R. OgielaU. Ogiela, Linguistic protocols for secure information management and sharing, Computers & Mathematics with Applications, vol. 63, no. 2, pp. 564–572, 2012. Elsevier, 2012.

**Response to Reviewer 3’s Comments**

**Reviewer #3:**

1) The problem is interesting and this paper’s research has certain contribution.

***Our response:***

Thank you very much for your approval.

2) There are several syntax and semantics error that must be modified like "Let G be be a cyclic multiplicative group ...", "After publishes the public parameter, user also needs to ask for a PKG signing ...", "... prove the security of our scheme against there attack games.", and "... scheme with other schemes in Table ??.".

***Our response:***

We appreciate the reviewer and apologize for grammatical errors and typing errors in our manuscript. To fix these errors, we have polished our paper in several rounds. In each round, we tried our best to correct lexical errors and send it to some scholars to review and to gain comments for the next round of revision. We have corrected many grammatical and typing errors including the ones pointed by this reviewer and others such as “computation costs” is corrected to “computational costs”, “two technology” is corrected to “two technologies”, and so on.

3) The proposed system is logically correct. Let us know if any parts of the proposed scheme has been implemented.

***Our response:***

Thank you very much for your kindly reminding. Actually, we have implemented the whole HIBOOS scheme and evaluated it. We have added some of the evaluation results in an added section “4.1 Computational Costs”.

4) As the authors have mentioned, efficiency is a key parameter in analyzing an HIBS and escrow-free scheme. There is not a precise performance analysis for the proposed scheme. You must add some information to evaluate the proposed system more precisely.

***Our response:***

Thank you very much for this valuable comment. As mentioned in the response to remark 3, we have added the evaluation results of our HIBOOS scheme as an individual section “4.1 Computational Costs”. In that section, we evaluate the computational costs of algorithms in our scheme, pointing out that our online/offline model is effective.

5) In section 4.1, how SID is selected?

***Our response:***

Thank you very much for pointing out the lack of clarity of the SID selection. Actually, the SID was randomly selected and the word “randomly” was carelessly omitted. We have corrected the error by modified the sentence to “randomly picks as user secret”.

6) The steps in section 3.2 is not clearly categorized. I recommend to provide a pseudo code to illustrate distinction between each step and to determine dependencies among them.

***Our response:***

Thank you very much for pointing out the lack of clarity of section 3.2. Instead of providing a pseudo code, we have added a schema in section 2.3 to show the generic construction of our HIBOOS scheme, which we think is more intuitive to illustrate the distinction between each step and to determine dependencies among them.

7) Do you consider any presumptions for online signing in comparison to offline signing? Exactly there must be a clear distinction between them in view of computations. In Table I, computational time for each of them is almost equivalent. What's the difference between Online and Offline signing in view of computations?

***Our response:***

We appreciate the reviewer and apologize for the typo of Table I. It was a typo that the entries in column “Online Sign Comp.” were filled the same values as the ones in column “Verify Comp.”. Actually in fact, the computational time for online signing was quite shorter than for offline signing, which we had pointed out in section 4.1. We have corrected this mistake. According to Table I, we can find that online signing is much faster than the offline signing.

8) You should provide some graphical images to show how your scheme works. I recommend to add a chart to indicate steps of signing for both offline and online interactively.

***Our response:***

This comment is really appreciated. As mentioned in the response to remark 3, we have added a schema in section 2.3 to show how our scheme works. In an online/offline signature scheme, a user performs offline signing prior to the knowledge of the message to be signed. That is, a user performs the offline phase to obtain an intermediate result. Once the message to be signed is known, user use this result to generate a final signature. The complete signing action is such simple that need not to sign offline and online interactively.