Fw: FROM Ilsun) wd: Security and Communication Networks - Decision on Manuscript ID SCN-15-0766

"bkzhao@139.com" <bkzhao@139.com>
收件人：cpx612 <cpx612@163.com>
时　间：2015-12-19 18:28:07
附　件：

培鑫，
　　请查看意见，并抓紧时间修改，

祝好，
宝康

From: Ilsun You
Date: 2015-12-19 11:46
To: bkzhao@139.com
Subject: FROM Ilsun) wd: Security and Communication Networks - Decision on Manuscript ID SCN-15-0766

Dear Baokang,

Please timely prepare for the revised version according the review comments.

Best,
Ilsun

---------- Forwarded message ----------
From: <francesco.chiti@unifi.it>
Date: Sat, Dec 19, 2015 at 12:43 AM
Subject: Security and Communication Networks - Decision on Manuscript ID SCN-15-0766
To: chenpeixin@nudt.edu.cn, sjs@nudt.edu.cn, bkzhao@nudt.edu.cn, wang@nudt.edu.cn, ilsunu@gmail.com

18-Dec-2015

Dear Mr You,

Manuscript ID SCN-15-0766 entitled "An Escrow-Free Online/Offline HIBS Scheme for Privacy Protection of People-Centric Sensing" which you submitted to Security and Communication Networks has been reviewed. The comments of the referee(s) are included at the bottom of this letter.

A revised version of your manuscript that takes into account the comments of the referee(s) will be reconsidered for publication. The revision is due in two months.

Please note that submitting a revision of your manuscript does not guarantee eventual acceptance, and that your revision may be subject to re-review by the referee(s) before a decision is rendered.

You can upload your revised manuscript and submit it through your Author Center. Log into https://mc.manuscriptcentral.com/scn and enter your Author Center, where you will find your manuscript title listed under "Manuscripts with Decisions".

When submitting your revised manuscript, you will be able to respond to the comments made by the referee(s) in the space provided. You can use this space to document any changes you make to the original manuscript.

Once again, thank you for submitting your manuscript to Security and Communication Networks and I look forward to receiving your revision.

Sincerely,

Dr Francesco Chiti
Security and Communication Networks
francesco.chiti@unifi.it, francesco.chiti@gmail.com

Referee(s)' Comments to Author:

Reviewing: 1

Comments to the Author
In this paper,the authors develop a model to address the key escrow problem in HIBOOS scheme and instantiate the developed model in to an 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. (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. (3) Please add more recent published references, especially those published in the recent

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

Reviewing: 2

Comments to the Author
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.
2. For identity based signature scheme described in section 3.2 may be placed a simple schema
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.

Reviewing: 3

Comments to the Author
1. The problem is interesting and this paper’ s research has certain contribution.
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 ??.".
3. The proposed system is logically correct. Let us know if any parts of the proposed scheme has been implemented.
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.
5. In section 4.1, how SID is selected?
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.
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?
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.

不加了。-许同梦

--
+ Ilsun You, Ph.D., IET Fellow, SMIEEE
+ EiC of JoWUA (http://www.jowua.org) indexed by Scopus.
+ Associate Professor, Department of Information Security Engineering
+ Soonchunhyang University
+ Asan-si, Republic of Korea
+ E-mail: ilsunu@gmail.com
+ Home: http://ilsunu.googlepages.com