A LIST OF CHANGES

June 26th, 2013

Paper Number: WIRE-D-13-00107
Paper Title: Generating Lightweight Behavioral Signature for Malware Detection in People-Centric Sensing
Authors: Huabiao Lu, Baokang Zhao, Jinshu Su and Peidai Xie

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 Wireless Personal Communications.

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,
Huabiao Lu, Baokang Zhao, Jinshu Su and Peidai Xie

Response to the Associate Editor

Comments to the Author:
Based on the advice received, I have decided that your manuscript can be accepted for publication after you have carried out the corrections as suggested by the reviewer(s).

Our Response: We appreciate the comments and minor revision recommendation by the editor. We have revised the original manuscript according to the comments and suggestions made by the three reviewers. We also simplified the title of the paper by changing the ambiguous title "Simple yet Effective Malware Behavioral Signature Generation for People-Centric Sensing" to a more clear title "Generating Lightweight Behavioral Signature for Malware Detection in People-Centric Sensing". In the rest part of this revision document, we provide the detailed revisions made in response to each of the three reviews.

Response to Reviewer 4's Comments

Reviewer #4:

As the Behavior-Graph-based signature is too complicated for PCS, this paper proposes a simple yet effective signature generation system, SimBehavior. To be more lightweight, SimBehavior is based on syscall sequence rather than behavior graph. Further more, the paper proposes Resource Differentiation scheme, Iterative Sequence Alignment (ISA) and Signature Refinement to generate a simple but still accurate signature. The experimental results validate the effectiveness and accuracy of SimBehavior.

1) Since the authors announce SimBehavior is more simple than Behavior Graph-based system, comparing with Hamsa (network-based) is not enough to validate it.

Our response:

We thank the reviewer for this valuable comment. Really, with the exception of the newest behavior graph, Hamsa (in Proceedings of the 2006 IEEE Symposium on Security and Privacy) is one of the state-of-the-art signature generation systems for both network-based and behavior-based systems. Therefore, in our experimental part, we have revised Hamsa as a behavior-based signature generation system, and make it generate behavioral signature consisting of syscall tokens. After that, our revised Hamsa becomes a good choice to comparing with new approaches. Therefore, we choose to compare our proposed SimBehavior with Hamsa. In the future, we will build new behavior graph systems and comparing SimBehavior and these systems.

2) Although syscall-sequence-based signature may be more simple than behavior-graph-based, its efficiency for PCS needs to be validated.

Our response:

As an emerging sensing system, PCS only applies for simple application and rarely exists in real life. Thus, it is difficult to validate the efficiency of our SimBehavior in PCS straightforwardly. Fortunately, because of rich connectivity and sociality in PCS, the behavior model of malwares in PCS intrinsically is the same with those in online social network (OSN). Therefore, in our experiments, we generate the signatures of malwares and detecting new malwares using similar approaches in OSN. By this way, the efficiency of our SimBehavior in PCS is validated.

Response to Reviewer 5's Comments

Reviewer #5:

Because in people-centric sensing network, the worse, attackers usually obfuscate their mal-wares, this article proposes a resource differentiation based, anti-obfuscation, simple but effective malware behavioral signature generation system. The resource differentiation scheme generalizes syscall sequence by classifying resources for hiding the differences introduced by different executing environment or random tactics used by malware. The Iterative Sequence Alignment can defeat obfuscation and gain sub-signature set from generalized syscall sequences. The performance of this system is evaluated in the experiment and the presentation of this paper is well.
Following improvements should be made on this paper before publishing:

1) The position of reference [2] and [3] should be changed each other;

Our response:

Thank you very much for pointing out the mistakes within the references. We really appreciate your valuable comments, and it is definitely a good writing style to keep the No. of references sequentially increment according to the first appearances of those references in manuscript.

We have changed the No. of reference [2] and [3] in our original manuscript to [3] and [2] in our revised manuscript. And the No. of references "Abhinav Srivastava, Andrea Lanzi, Jonathon Giffin (2008). System Call API Obfuscation (Extended Abstract). In RAID'08." and "Matt Fredrikson, Somesh Jha, Mihai Christodorescu, et al. (2010). Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors. In Proceedings of the 2010 IEEE Symposium on Security and Privacy." are also exchanged in our revised manuscript.

2) In section 5.1, please give some references which talking about traditional sequence alignment.

Our response:

This comment is really appreciated. As a response, we have appended the following references for "traditional sequence alignment",

[18] wikipedia. Sequence alignment [Online]. Available: http://en.wikipedia.org/wiki/Sequence_alignment, May, 2013.
[19] Yong Tang, Bin Xiao and Xicheng Lu (2009). Using a Bioinformatics Approach to Generate Accurate Exploit-based Signatures for Polymorphic Worms. Computers & Security, Vol 28, pp. 827-842.
[20] Saul B. Needleman, Christian D. Wunsch (1970). A general method applicable to the search for similarities in the amino acid sequence of two proteins. Journal of Molecular Biology, Vol 48, Issue 3, pp. 443-453.
[21] Cédric Notredame, Desmond G Higgins, Jaap Heringa (2000). T-coffee: a novel method for fast and accurate multiple sequence alignment. Journal of Molecular Biology, Vol 302, Issue 1, pp. 205-217.

3) In section 7.2, the consumed time of SimBehavior should also be introduced and analyzed.

Our response:

In the revised manuscript, we have conducted extensive experiments according to this valuable comment. In our new experiments, some related metrics, including the time of our SimBehavior to generate signatures for each family and the time of matching generated signatures against testing set of each family, are computed and compared in details. From the perspective of the time consumption, our SimBehavior is appropriate for behavioral analysis and detection of malwares in PCS.

Response to Reviewer 6's Comments

Reviewer #6:

Currently, there are increasing requirements for detecting malwares in handheld computers, i.e., mobile phones, especially for PCS. Providing such mechanisms is critical and challenging. In this paper, the authors proposed SimBehavior, an novel approach to provide a simple and efficient solution to handle with this issue. The contribution of this paper is significant. Yet, the presentation and organization of this paper should be improved. My detailed comments can be summarized

as follows,

1) The presentation of this paper should be polished. I have found some grammatical errors and typing errors can be found in the paper, for instance, "Our experiment results" should be "Our experimental results".

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 one pointed by this reviewer and others such as “Our experiment results” is corrected to “Our experimental results”, “rreceived” is corrected to “received”, and so on.

2) The title of this paper can be improved. I suggest the authors to have a better title.

Our response:

Thank you very much for suggesting us to improve the title. We change the ambiguous title “Simple yet Effective Malware Behavioral Signature Generation for People-Centric Sensing” to a more clear title “Generating Lightweight Behavioral Signature for Malware Detection in People-Centric Sensing”.

3) Some figures is not very clear. For instance, the font problem in Fig.2.

Our response:

Thank you for pointing out the lack of clarity in some figures. We have change the font of Fig.2 form Song to Times New Roman, and font size from 12 pt to 10 pt to make Fig.2 look much clearer.

4) In the experimental part, the results can be more significant using figures instead of tables.

Our response:

It is a good idea to use figures instead of tables to present the results of experiments. However, due to lacking of experimental data and comparative algorithms in malware, It is very difficult to have enough experimental points of data to depict a good figure in our manuscript. We are very sorry and were forced to use tables to present our experimental results.

5) More recent reference literatures should be cited. Such as,
[1] Matthew Fredrikson, Mihai Christodorescu, Somesh Jha, Dynamic behavior matching: a complexity analysis and new approximation algorithms, 23rd international conference on Automated deduction (2011), pp.252-267.

Our response:

We appreciate the comment made by this reviewer. We have added the following reference literatures additionally in our revised manuscript:

Symantec Corporation (2013). Internet Security Threat Report--2012 Trends Vulume 18. Available: http://www.symantec.com/threatreport/.

Matthew Fredrikson, Mihai Christodorescu, and Somesh Jha (2011). Dynamic Behavior Matching: A Complexity Analysis and New Approximation Algorithms. In 23rd international conference on Automated deduction, LNAI 6803, pp. 252–267.

Vaibhav Rastogi, Yan Chen, and Xuxian Jiang (2013). DroidChameleon: Evaluating Android Anti-malware against Transformation Attacks. Short Paper, in the Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS).