Huan-feng PENG, Zhi-qiu HUANG, Lin-yuan LIU, Yong LI, Da-juan FAN, Yu-qing WANG, 2018. Preserving privacy information flow security in composite service evolution. *Frontiers of Information Technology & Electronic Engineering*, 19(5):626-638. https://doi.org/10.1631/FITEE.1700359

Preserving privacy information flow security in composite service evolution

Key words: Composite service, Privacy information flow security, Service evolution, Petri net

Corresponding author: Zhi-qiu HUANG
E-mail: zqhuang@nuaa.edu.cn
ORCID: http://orcid.org/0000-0001-6843-1892

Motivations

1. The usage of the information flow control (IFC) technology by composite service providers will increase users' confidence so that their privacy data are correctly used.

2. User privacy requirement and trust levels of component services may change after a composite service is deployed. Preserving privacy information flow security in a composite service becomes an important evolutionary requirement.

3. In this study, we focus on how to preserve privacy information flow security in a composite service when user privacy requirements and trust levels of component services change.

Main ideas

1. To address this issue, a possible approach is to re-verify the entire composite service. However, this approach incurs great evolutionary cost. To avoid the complex re-verification process and decrease the evolutionary cost, a better approach is used to identify the impact of the changes, and then enforce the evolution according to the impact identified.

2. When we initially verify the privacy information flow security, the underlying data for the subsequent evolution is recorded. Based on the underlying data, we propose evolution operations that can preserve privacy information flow security.

Methods

1. A privacy data item dependency analysis method based on a Petri net model is presented.
2. The set of privacy data items collected by each component service is derived through a privacy data item dependency graph, and the security scope of each component service is calculated.
3. The evolution operations that preserve privacy information flow security are defined.

Major results

1. We illustrate the effectiveness of our approach through a case study.

2. The experimental results indicate that our approach has high evolution efficiency and can greatly reduce the cost of evolution compared with re-verifying the entire composite service.

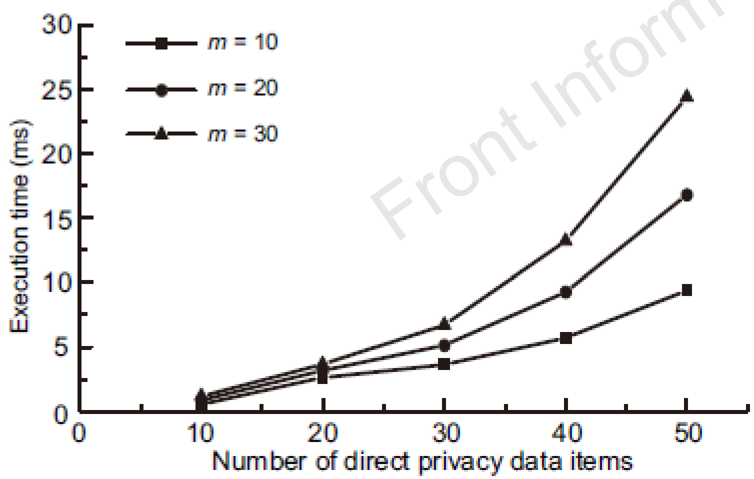

Fig. 6 Time cost of Evolution operation 2.1

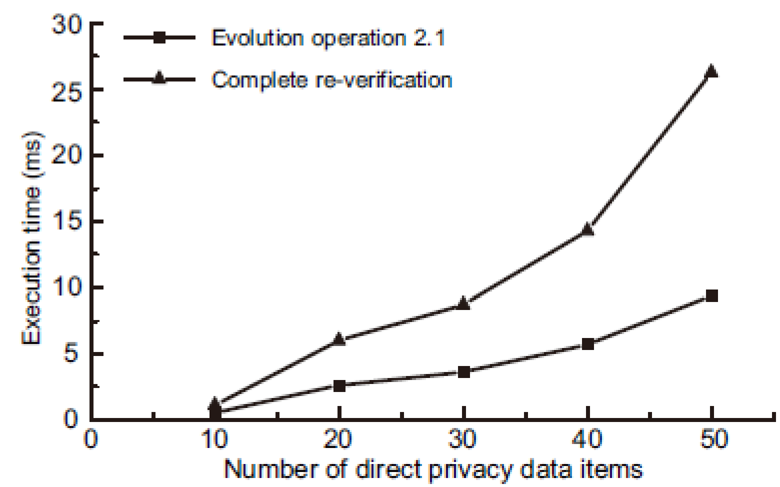

Fig. 7 Time cost by Evolution operation 2.1 and complete re-verification ($m = 10$)

Conclusions

1. We investigated how to preserve privacy information flow security in a composite service, when the trust levels of component services and user requirements changed. Based on the underlying data recorded during the static verification, evolution operations that preserved privacy information flow security have been proposed.

2. We have illustrated the effectiveness of our approach through a case study. Compared with re-verifying the entire composite service, we have also shown through simulation experiments that our approach could reduce the evolution cost more effectively.

Conclusions (Cont'd)

3. In the scenario of online evolution, too long verification time was generally unacceptable. Through our approach, the complicated re-verification process could be avoided, and the evolution efficiency could be greatly improved.