Jia-xin JIANG, Zhi-qiu HUANG, Wei-wei MA, Yan CAO, 2018. Using information flow analysis to detect implicit information leaks for web service composition. *Frontiers of Information Technology & Electronic Engineering*, 19(4):494-502. https://doi.org/10.1631/FITEE.1601371

Using information flow analysis to detect implicit information leaks for web service composition

Key words: Information flow analysis; Business process execution language; Petri net; Interference

Corresponding author: Jia-xin JIANG
E-mail: jiangjiaxin@nuaa.edu.cn
ORCID: http://orcid.org/0000-0001-6185-4438

Motivation

1. Users usually have to submit some personal information, which is sensitive information, to service providers to carry out necessary business processes when using web service composition.

2. Access control mechanisms only monitor a particular transmission channel between a classified subject and a public subject, whereas so called ‘covert channels’ are neglected.

3. Information flow analysis can capture security violations that lie beyond the scope of an access control mechanism, such as the information leaks that take place over covert channels.

Main idea

1. In information flow analysis, the criterion for the security of a system is based on the notion of noninterference.

2. A Petri net is a well-founded process-modeling technique that has formal semantics. It has been used to model and analyze several types of processes including protocols, manufacturing systems, and business processes.

3. Place-based noninterference (PBNI) is an approach for reasoning through the structural noninterference in Petri nets.

Method

1. BPEL workflow is transformed into a labeled Petri net. The transformation includes two steps:

   (1) the BPEL model is mapped into an equivalent Petri net model using an existing transformation tool—BPEL2oWFN;

   (2) the resultant Petri net is unfolded into a labeled Petri net, to which is added the security class, to model concurrently running instances and their access to shared resources.

2. Using Petri net reachability graph to estimate Petri net interference and thereby detect implicit information leaks in web service composition.

Major results

1. A labeled Petri net to describe the case study of update patient record workflow.

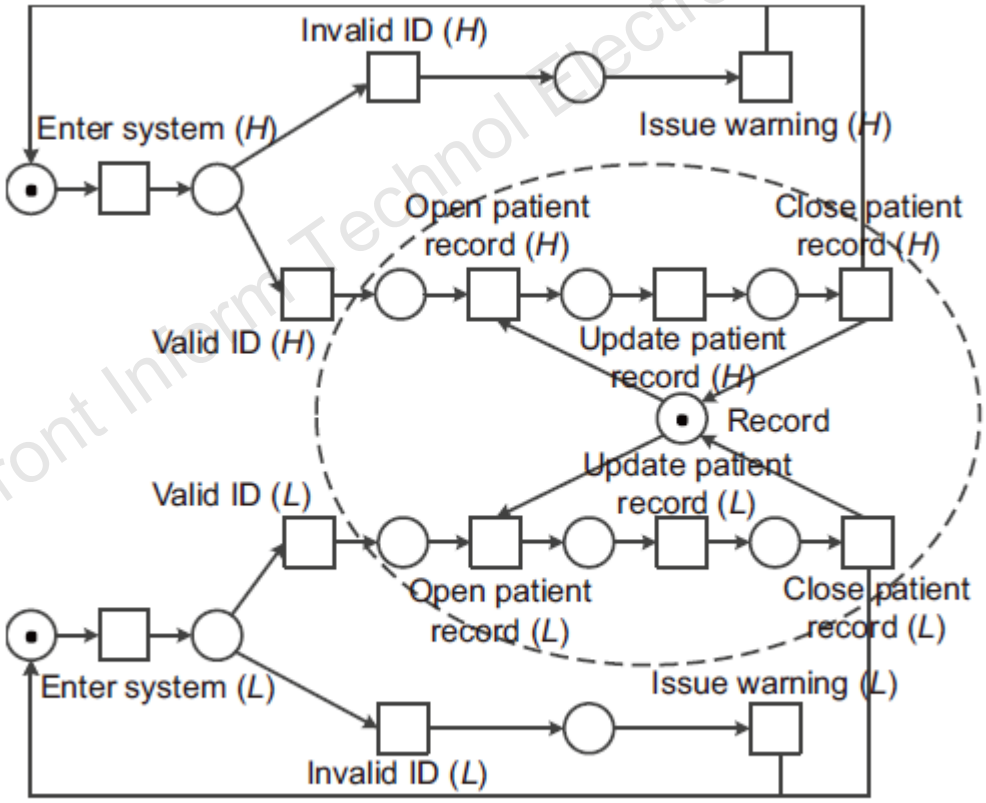

Fig. 8 Labeled Petri net of the workflow

Major results

2. We transform the labeled Petri net to a reachability graph (Fig. 10) to describe the running states of the Petri net.

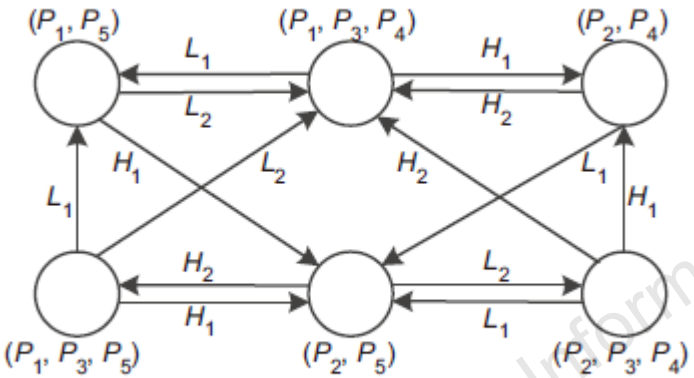

Fig. 10 Reachability graph of the partial workflow

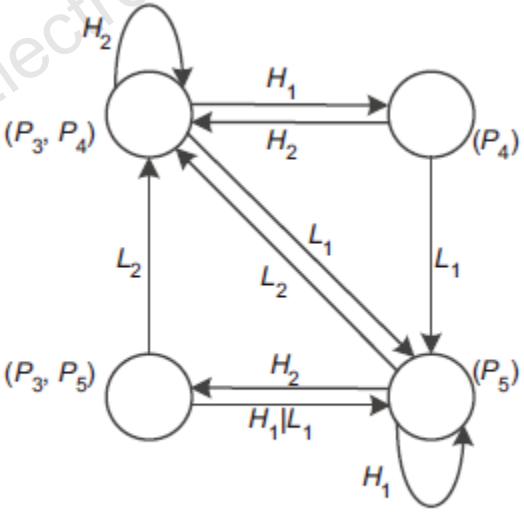

Fig. 11 *L*-reachability graph of the partial workflow

3. In Fig. 11, we discover that the state (P_3, P_4) can convert to state (P_4) by H_1, which means that the Petri net has an interference property.

Conclusions

1. We present an approach for information flow analysis of BPEL specifications to detect implicit information leaks for web service composition and demonstrate its applicability in a case study.

2. Overall, the static detection of information flows for BPEL is a novel promising research direction to ensure formally founded security guarantees for web service composition.