Executable Model-Based Risk Assessment Method for Identity Management Systems

Ebenezer Paintsil and Lothar Fritsch
{paintsil, lothar.fritsch}@nr.no

Norwegian Computing Center Oslo, Norway

Abstract. Currently, risk assessment methods for identity management systems (IDMSs) are lacking. This makes it difficult to compare IDMSs based on how they enhance privacy and security of system stakeholders. This article proposes the executable model-based risk assessment method (EM-BRAM) with the aim of addressing this challenge. The EM-BRAM identifies risk factors inherent in IDMSs and uses them as inputs to a colored petri nets (CPNs) model of a targeted IDMS. It then estimates or verifies the system's security and privacy risks using CPNs' state space analysis and queries.

1 Introduction

Identity theft crimes online is ever increasing. In 2010, the total cost of online credit card fraud alone was estimated as 4.2 billion US dollars [1]. Currently, identity related crimes are among the fastest growing crimes in the United Kingdom [2].

Privacy enhance IDMSs have the potential of mitigating these crimes and privacy risks. Privacy enhancing IDMSs can allow end-users to act under pseudonyms, to be unlinkable and control the use and release of their partial identities [3]. However, privacy enhance IDMSs greatly differ in their security mechanisms. They prescribe different security mechanisms and focus on different problem areas. The inconsistent and complex mechanisms make systems' comparisons a daunting task for system stakeholders.

Privacy and security risks assessment methods can be used to compare IDMSs in order to improve their security and also select the appropriate systems for stakeholders. Currently, privacy and security risks assessment methods for IDMSs are lacking [4]. Moreover, the traditional risk assessment approaches such as ISO27005 [5] provide no explicit inputs for risk assessment of IDMSs. For instance, the ISO27005 [5] has no explicit risk model for IDMSs.

Furthermore, the traditional risk assessment approaches rely on the intuitions of risk assessors to estimate risk because of lack of data thereby making the process error prone [7], [8].

This article introduces the executable model-based risk assessment method (EM-BRAM) for IDMSs. The method identifies risk factors inherent in IDMSs and uses them as inputs to a colored petri nets (CPNs) model of a targeted

IDMS to estimate or verify the system's risk. The method has the potential of reducing subjectivity and uncertainty in risk assessment of IDMSs.

2 Executable Model-Based Risk Assessment Method

This section introduces the executable model-based risk assessment method for IDMSs. The method relies of the characteristics of tokens used in IDMSs to estimate a system's risk. The first step in the method is risk identification focusing on the characteristics of tokens that can contribute to privacy and security risks in IDMSs. We focus on tokens used in IDMSs because are personal data sources and gateway to resources. A token is a technical artifact providing assurance about an identity [9]. A token can be an identifier such as username, a claim such as a password, an assertion such as SAML tokens, a credential such as X.509 certificate or combinations of these.

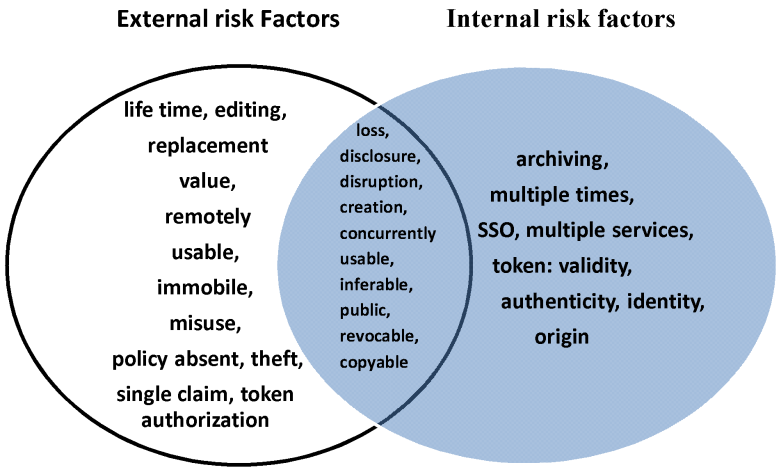

Fig. 1. External and Internal Risk Factors [9]

The characteristics of tokens that contribute to privacy and security risks are identified and categorized into external and internal factors as shown in Figure 1. The internal characteristics serve as the input for the CPNs of the IDMSs.

The second phase of the risk analysis is risk estimation focusing on the internal factors. Internal factors are those under the control of IDMSs while external factors are outside the control of the IDMS. While internal factor are estimated with CPNs modeling, the external factors may be used for policy decision.

We verify or estimate the internal risk through CPNs [10] modeling because it would be difficult to manually verify how tokens flow in IDMSs and which risk state they find themselves. In addition, CPNs is less mathematical and has a

high degree of automation making it relatively easy to use. The automation can potentially reduce cost involved in the risk assessment process and subjectivity in the risk estimation.

The system modeling is followed by the validation of the behavior properties of the system. This enables us to determine the behavioral correctness of the IDMS's model before risk verification or estimation. The validation is automated with CPNTools [10].

Finally, the privacy and security risks are estimated or verified using CPNs queries and ML predicate functions. The queries search through all the execution states of the IDMS model to verify if the risk conditions exist. For example, the following CPNs query can be used to verify whether a token is used for multiple services or single sign-on (SSO). Although SSO reduces human error, it leads to sharing of valuable information across services or domains.

```
fun isMultipleServices()= fn n => isSubstring "bob"
(st_Mark.GoogleSP'ReceivedAssertion 1 n);
```

The query verifies if the alias "'bob"' can be found outside a trusted domain.

3 Conclusion

Lack of risk assessment method for identity management systems (IDMSs) makes it difficult to compare them based on their security and privacy risks levels. This article, proposes the executable model-based risk assessment method for IDMSs. The method can be used to compare IDMSs based on their security and privacy risks levels and has the potential to improve privacy and also reduce the subjectivity inherent in traditional risk assessment methods.

References

[1] Levi, M.: Measuring the cost of cybercrimes. ERCIM News **2012**(90) (2012)
[2] Leyden, J.: Id fraud prevention week fights uk's fastest growing crime (2009)
[3] WP3: D3.1: Structured overview on prototypes and concepts of identity management systems. Deliverable 1.1, Future of Identity in the Information Society (2005)
[4] Cabarcos, P.: Risk assessment for better identity management in pervasive environments. In: Pervasive Computing and Communications Workshops (PERCOM Workshops), 2011 IEEE International Conference on. (2011) 389–390
[5] ISO: Iso 27005 information security risk management. Technical report, International Organization for Standardization (2008)
[6] Aven, T.: A semi-quantitative approach to risk analysis, as an alternative to qras. Reliability Engineering & System Safety **93**(6) (2008) 790 – 797
[7] Campbell, H.: Risk assessment: subjective or objective? ENGINEERING SCIENCE AND EDUCATION JOURNAL (1998)
[8] Paintsil, E.: Evaluation of privacy and security risks analysis construct for identity management systems. Systems Journal, IEEE **PP**(99) (2012) 1
[9] Kurt, J., Lars, K.M.: Colored Petri Nets: Modelling and Validation of Concurrent Systems: Modeling and Validation of Concurrent Systems. Springer-Verlag Berlin Heidelberg (2009) ISBN:978-3-642-00283-0.