Journal of Information Security and Applications 000 (2018) 1–13

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Managing distributed trust relationships for multi-modal authentication

Tim Van hamme, Davy Preuveneers*, Wouter Joosen

imec-DistriNet-KU Leuven, Celestijnenlaan 200A, Heverlee B-3001, Belgium

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Authentication
Behavioral biometrics
Reputation
Trust model
Ontology

ABSTRACT

Multi-modal active authentication schemes fuse decisions of multiple behavioral biometrics (behaviometrics) to reduce identity verification errors. The challenge that we address in this work is the security risk caused by these decision fusion schemes making invalid assumptions, such as a fixed probability of (in)correct recognition and a temporal congruence of behaviometrics. To mitigate this risk, this paper presents a formal trust model that drives the behaviometric selection and composition. Our trust model adopts a hybrid approach combining policy and reputation based knowledge representation techniques. Our model and framework (1) externalizes trust knowledge from the authentication logic to achieve loosely coupled trust management, and (2) formalizes this knowledge in description logic to reason upon and broker complex distributed trust relationships to make risk-adaptive decisions for multi-modal authentication. The evaluation of our proof-of-concept illustrates an acceptable performance overhead while lifting the burden of manual trust and behaviometric management for multi-modal authentication.

1. Introduction

Due to the rapid evolution of cloud computing, Big Data, and the Internet of Things, enterprises rely more and more on context information about the user to improve the delivery, the user convenience and the security of their business applications and services. In multi-modal continuous authentication [1,2], various behaviometrics of a subject are being collected in the background by distributed sensors or other information sources in order to jointly and continuously verify in a user-friendly manner the identity of the subject by establishing and recognizing unique behavioral patterns. The contribution of each behaviometric is usually weighed with a variant of Chair and Varshney's optimal decision fusion rule [3]. While such decision fusion schemes help to reduce the equal error rate (EER) of multi-modal authentication systems, they make assumptions that may jeopardize the trustworthiness of the authentication. For example, (1) decision fusion scheme implementations often mistakenly assume a static probability of correct identification and false alarms for each individual behaviometric; (2) they expect temporal congruence of the different behaviometric data streams; and (3) they ignore security threats of behaviometric sensors (e.g. sensors being temporarily disabled or compromised, and the fact that some behavior data is easily observed in public by adversaries that can use it to spoof a victim's identity).

In the face of risk and uncertainty, behaviometric authentication implementations must be able to understand and reason upon the trustworthiness of the sensors and the information they depend upon. Existing risk and trust models [4–6] proposed in the literature over the past decades, are inadequate due to contextual dependencies and the dynamicity of behaviometrics - i.e. (mis)identification classification probabilities evolving over time - that have an impact on multi-modal continuous authentication. To address this challenge, we propose a trust model and framework that liberate the security architect and the end-user from manually selecting and composing behaviometrics by managing and reasoning upon complex trust relationships for all collaborating systems, sensors and applications for continuous risk-adaptive authentication.

This paper presents a formal representation of a trust model and supporting management framework that enables distributed applications to infer and broker trust relationships. Mainly driven by the requirements of our use case on continuous multi-modal authentication to establish trust in behaviometrics, our model adopts a hybrid approach combining policy and reputation based knowledge representation techniques. The contributions of our trust model and supporting framework are as follows:

1. It externalizes trust knowledge from the authentication logic to augment the core risk model with application-specific

* Corresponding author.
E-mail addresses: tim.vanhamme@cs.kuleuven.be (T. Van hamme), davy.preuveneers@cs.kuleuven.be (D. Preuveneers), wouter.joosen@cs.kuleuven.be (W. Joosen).

https://doi.org/10.1016/j.jisa.2018.01.003
2214-2126/© 2018 Elsevier Ltd. All rights reserved.

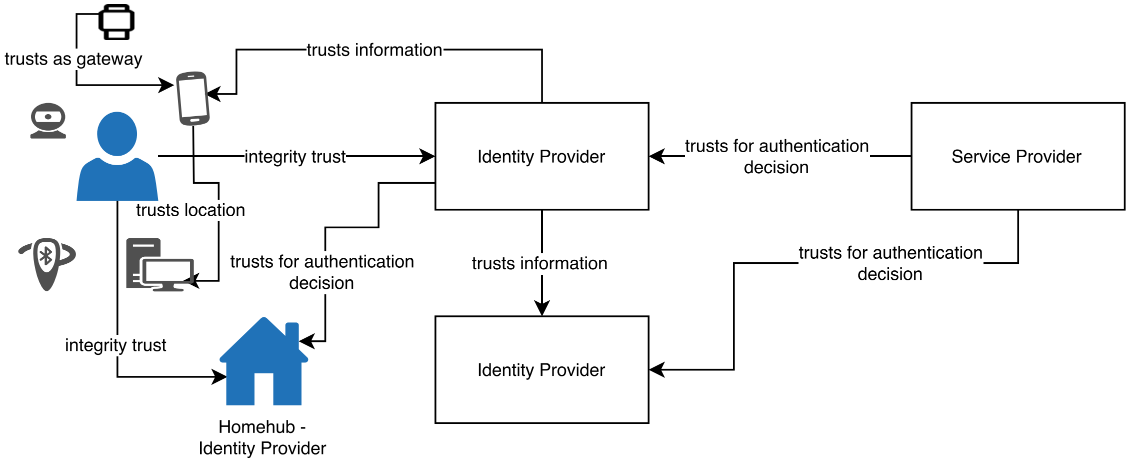

Fig. 1. Trust relationships for local and remote authentication use cases.

trust concepts while minimizing the impact on the authentication logic.

2. It formalizes risk, trust and context concepts in description logic to automate context-aware inference and brokerage of trust relationships.
3. The trust management framework has an acceptable low computational overhead to infer and broker these relationships.

While we will demonstrate and evaluate the feasibility, applicability and performance of our hybrid trust model with our authentication use case, its design should make it suitable for other distributed risk-adaptive applications.

The paper is structured as follows. We carry out a requirements and gap analysis on trust models for our motivating scenario on multi-modal authentication in Section 2. Section 3 describes the design and implementation of our trust management solution. We evaluate the feasibility of modeling and reasoning upon distributed trust relationships in Section 4. We discuss and compare our work in Section 6 with related work on multi-modal authentication and policy-based and reputation-based trust models. We conclude with some final thoughts and directions for further research in Section 7.

2. Trustworthy continuous multi-modal authentication

In this section, we describe the trends that have lead to our motivating scenario on multi-modal authentication and briefly highlight how trust plays a role. Later on, we will discuss which challenges are not addressed by existing solutions and the state-of-the-art, and which trust relationships must be considered to bridge this gap.

2.1. Trends and trust challenges for multi-modal authentication

Fig. 1 depicts our high-level motivating scenario that we will use to illustrate the authentication related trends and trust challenges.

2.1.1. Federated single sign on

In federated Single Sign On (SSO), an identity provider (IdP) is taxed with authenticating users on behalf of a service provider (SP). The SP needs to trust the IdP to do a secure job of authenticating the user. The other way around, the user trusts the IdP with his credentials. The IdP itself is part of a federation and trusts the authentication assertions from the other IdP members in the circle of trust of IdPs and SPs. The trust in an IdP that offers multi-factor authentication (MFA) - i.e. combining factors representing something (1) you *know*, (2) you *own*, and/or (3) you *are* - will be higher than in one that only provides login/password authentication.

2.1.2. Risk-adaptive authentication

Contemporary authentication systems tap into the context of a user or service interaction [7–9] to ascertain the risk of a security threat. For example, online payments executed in the home country of a user are generally perceived as more safe than the same payment executed abroad. Wiring a small amount of money is less risky than a high amount. Risk-adaptive authentication schemes will verify additional non-intrusive context factors to offer a frictionless authentication experience in low-risk situations. This implies that trust relationships are context-dependent.

2.1.3. Multi-modal authentication with behavioral biometrics

Behavioral biometrics add a 4*th* authentication factor based on something you *do* to multi-factor authentication systems. Typical examples are mouse and keystroke dynamics [10–13], websites browsed and network traffic [14], stylometry [7], ambient sound [15] and gait recognition [16,17]. While such behaviometrics are user friendlier, they have higher false acceptance rates (FAR) or false rejection rates (FRR) compared to iris scans or fingerprint biometrics. That is why multiple features or decisions are fused in multi-modal authentication [18] to obtain acceptable equal error rates (EER). Consider the example of a smart assistant homehub in Fig. 1, which uses built-in voice recognition and identification to continuously authenticate users. On top of that it assesses the presence of wearable devices that use gait recognition to identify their bearer. It trusts these wearables to tell if they are currently being worn by the user or not.

To provide an accurate joint assessment of the identity of the subject, the contribution of each behaviometric will depend on its accuracy. Chair and Varshney's optimal decision fusion rule [3] assumes a static probability of correct identification and false alarms for each individual behaviometric. Each of the n behaviometrics makes a local binary decision $u_i = \{-1, +1\}$ depending on whether it is in favor of the hypothesis H_0 or H_1 that either rejects or confirms the claimed identity of the subject. The optimal decision fusion rule states that:

$$f(u_1, ..., u_n) = +1 \qquad \text{if} \quad a_0 + \sum_{i=1}^{n} a_i u_i > 0 \tag{1}$$

$$f(u_1, ..., u_n) = -1 \qquad \text{otherwise} \tag{2}$$

Please cite this article as: T. Van hamme et al., Managing distributed trust relationships for multi-modal authentication, Journal of Information Security and Applications (2018), https://doi.org/10.1016/j.jisa.2018.01.003