AUTHENTICATION TRUST METRIC AND ASSESSMENT FOR FEDERATED IDENTITY MANAGEMENT SYSTEMS

SUMMARY

A formalization of authentication trust is proposed for federated identity management systems. Identity federation facilitates user interaction with Web services that control access, but it is more difficult for a service provider to evaluate the assurance of a user’s identity if the creation and propagation of user authentication assertions involve different authentication authorities and mediators. On the basis of this formal representation, an aggregated trust value is calculated for evaluating the trustworthiness of a user’s identity from the user’s authentication assertions propagated through multiple entities while preventing misbehavior or threats to manipulate the trust value.

Key words: trust metric, identity federation

1. Introduction

Identity federation is a scheme in which an identity provider (IdP) provides a service provider (SP) with an assertion about a user’s personal information such as authentication events or personal attributes beyond security domains [2]–[4]. The SP decides to grant or deny user access to resources on the basis of the assertion obtained from the IdP without directly authenticating him or her. This decision depends on the credibility of the assertion and the trustworthiness of the IdP. Thus, trust plays a crucial role in identity federation as an underlying concept.

This paradigm facilitates user interaction with Web services that control access, but it is more difficult for an SP to evaluate the assurance of a user’s identity if the creation and propagation of user authentication assertions involve different IdPs and intermediaries in different domains. In addition, in recent years many types of authentication methods have been deployed in practical systems and multifactor authentication is also required in response to increasing demands for strong authentication in some environments. Consequently, a trust metric is needed to evaluate propagated authentication assertions for federated identity management (FIM) systems in an open and distributed network.

FIM systems typically focus on the trust relationships between authentication authorities (IdPs) and parties that rely on collaboration (SPs); i.e., they are relationship-focused. In such a system, an online IdP dynamically issues short-term security tokens, i.e., assertions about a user’s identity or attributes upon the user’s request in contrast to a credential-focused system in which long-term cryptographic credentials such as X.509-based ones are issued without involving the original IdP [5]. In relationship-focused systems, an assertion can be transitive on the basis of the relationships between its issuer and recipient; namely, it can be flexibly shared with system entities and reused by them. In contrast, a credential-focused system needs to enforce the non-transitivity of a credential by cryptographic means because of its long lifetime or it will be vulnerable to impersonation attacks.

The transitivity in relationship-focused systems means that the assurance of a user’s identity specified in an assertion depends on the trustworthiness of all entities involved with its creation and propagation. Hence, a trust metric for FIM systems needs to incorporate the notion of transitivity inherent in assertions. However, previous trust metrics do not deal with such a notion, but consider a chain of trust relationships among a hierarchical system of authorities involved in issuing credentials.

In this paper, the formalization of authentication trust is proposed for FIM systems where an authentication assertion is propagated through business partners. On the basis of the trust model, a trust metric is described to quantitatively calculate a trust value for a user’s identity from the user’s multiple authentication assertions using logic-reasoning and graph-based approaches.

The rest of this paper is organized as follows: Section 2 reviews related work. Section 3 describes the trust model and its formal representation. Section 4 examines the metric for deriving authentication trust values. Section 5 describes the application of the proposed authentication trust calculation. Section 6 discusses several issues and Sect. 7 concludes the paper with a summary of the key points.

2. Related Work

There has been much work on trust models, metrics, and formalization in the literature. Prior work by Jøsang et al. [6] on general trust has focused on defining the semantics of trust and modeling trust-based systems. Agudo et al. [7] analyzed a general model of trust based on graph theory. These efforts were too general from a practical viewpoint to provide an access control system for evaluating the trustworthiness of assertions from multiple entities. This motivated me to research the authentication trust semantics and metric for

Copyright © 2012 The Institute of Electronics, Information and Communication Engineers
FIM systems proposed here as well as my observation that a user’s authentication trust transits together with the user’s assertions in FIM systems.

Existing work on trust formalization focuses on assigning numerical values of trustworthiness to paths representing relationships between entities [8]–[11]. Since these efforts described trust for credential-focused systems, they lacked metrics for relationship-focused systems. By contrast, the work described here specifically focuses on authentication trust metric and its evaluation for assertions dynamically established and propagated between entities.

Beth et al. [8] presented a formal representation of trust relationships and algorithms for deriving them to estimate the trustworthiness of entities in open networks. A limitation of this solution with respect to the design of an authentication trust metric is that it was vulnerable to manipulation of trust values calculated through the metric by misbehaving entities, which was described in [9]. The present paper uses their calculation method as an underlying technique to further develop algorithms for solving the above problem. Reiter and Stubblebine [10] proposed resilient authentication by using redundant multiple independent trust paths constructed from a trusted certificate authority (CA) to gain increased assurance in the authentication for public key infrastructure (PKI). The drawback is that they did not quantitatively evaluate trust for certificates by implicitly assuming that each certificate has the same level of risk. The work presented here derives a quantified trust value for authentication assertions specifying a user in FIM systems for controlling user access based on authentication trust. Huang and Nicol [11] introduced a formal representation of trust in PKI using logical rule inferences and proposed a mechanism for quantifying trust in certificate chains. Although their work shares this work’s goal of quantifying trust, their trust concept and evaluation were specific to PKI. With respect to the present proposal, their work did not provide a solution for evaluating the trustworthiness of certificates when they are propagated among entities.

Prior work on FIM systems deals with trust issues since trust management is an important building block for identity management. Thomas et al. [12] defined the semantics of the authentication trust level and provided a method for combining two trust levels to express the effect of multifactor authentication in a FIM environment. Although the present proposal is related in that it examines the authentication trust level, it focuses on evaluating the aggregated authentication level when multiple types of authentication assertions are available, by analyzing the similarity of the assertions. Alenárez et al. [13] analyzed the existing identity federation frameworks and identified the drawbacks for deployment in dynamic open environments. They also proposed a SAML [2] extension for dynamic federation that dynamically establishes trust between entities. Although their work remained a design concept for integrating trust-based functionality, the work presented here provides algorithms for evaluating a user’s authentication trust to be deployed in FIM systems.

3. Formal Representation of Authentication Trust

This section describes the formal representation of authentication trust for FIM systems. This paper gives trust specific definitions from the practical viewpoint of FIM. The concept of identity is introduced into a trust model, which consists of entities that exchange a user’s assertion with other entities.

3.1 Trust Semantics

The model’s trust relationships are defined as follows.

Definition 1 (Identity Trust) Identity trust is the certainty that the identity of an entity is identical to the identity claimed by the entity itself or by other parties regarding the entity on the basis of the authentication context.

In the above definition, the authentication context [14] is the information that the SP may require before it makes an entitlement decision with respect to an authentication assertion, such as an authentication method (e.g., password) and transport protocol (e.g., Secure Sockets Layer (SSL)). Identity trust is a foundation for authorizing an interacting entity to access restricted resources or for regulating interactions with the entity in trust-based systems including FIM systems. Identity trust in an entity is established as a result of authentication procedures in which the entity presents a credential such as a password or an X.509 certificate proclaiming its identity to an authenticating entity using a predefined authentication protocol. The authenticating entity verifies the presented credential and determines the trustworthiness of the entity with some level of certainty depending on the above authentication method.

Accordingly, the semantics of identity trust can be defined as follows:

\[ \text{trust}_{\text{id}}(x) \equiv \text{authn}(p, q, x), \quad x \in AC \quad (1) \]

where AC stands for a set of authentication context information, \( \text{trust}_{\text{id}}(x) \) expresses that entity \( p \) has identity trust in entity \( q \) on the basis of a specific authentication context \( x \), and \( \text{authn}(p, q, x) \) means that entity \( p \) authenticates entity \( q \) using authentication context \( x \). This axiom plays the role of a practical procedure for entity authentication in FIM systems associated with the identity trust relationship in this trust model.

Many metrics for evaluating this trust relationship have already been proposed. For example, many PKI trust models focus on the relationships among certification authorities for X.509 certificates. Instead, the proposed trust model focuses on the chain of user authentication context that comprises a certification trust evaluation.

The following definitions are related to the identity-trust-derived capabilities that are specific to FIM systems.

Definition 2 (Attestation Trust) Attestation trust is the
certainty about the entity’s capability to accurately create and assert information necessary for a recipient in a format appropriate for the recipient and to securely transmit the information to the recipient.

Based on the above definition, if $trust^{a}_{pq}(x)$ designates the attestation trust of trustor $p$ for trustee $q$ regarding information $x$, its semantics is given in first-order logic as

$$trust^{a}_{pq}(x) \equiv assert(q, x) \Rightarrow accept(p, x), \quad (2)$$

where $assert(q, x)$ means that $q$ creates an assertion containing information $x$ and $accept(p, x)$ represents that $p$ accepts that $x$ is true. The $\Rightarrow$ operator designates the implication that whenever the antecedent (expression to the left of the operator) is true, the consequent (expression to the right of the operator) is true.

For example, if an authentication authority issues an assertion in a format such as SAML [2] or OpenID [3] stipulating that it authenticated a user by using a particular authentication method at a specified time, then an SP with attestation trust in that authority accepts the information represented in the assertion format as credible.

The functionalities required for attesting in FIM systems include not only selective information encoding but also identity mapping. An attesting entity specifies a user in attested information using a corresponding identifier for a recipient associated with the user’s local identifier in the attesting entity. This functionality is important from the viewpoint of privacy because the recipient’s identifier may differ from the local one and be unique to the pair of recipient and attesting entity.

**Definition 3 (Mediation Trust)** Mediation trust is the certainty about the entity’s capability to verify the accuracy and reliability of information created by another entity and securely transmit the information to the recipient without modification.

Let $trust^{m}_{pq}(x)$ denote the mediation trust of trustor $p$ in trustee $q$ regarding information $x$. Its semantics is formally expressed as

$$trust^{m}_{pq}(x) \equiv accept(q, x) \Rightarrow accept(p, x). \quad (3)$$

This axiom means that if $q$ accepts that information $x$ is true, then $p$ also accepts that $x$ is true.

For example, a “proxying IdP” in SAML can act as a “trust mediating” entity. If it receives an authentication request regarding a user from an SP and cannot directly authenticate the user, it asks another IdP to authenticate the user and then returns the authentication assertion obtained from the authenticating IdP to the SP.

Note that in the above definition a trust mediating entity does not create an assertion by itself, but forwards it, though the entity shares responsibility for its trustworthiness with the entity providing it. In the above example, if the proxying IdP produces a new assertion by transforming identifiers used in the original information obtained from another IdP into the ones for the SP, then the proxying IdP corresponds to a “trust attesting” entity described in Definition 2.

### 3.2 Inference Rules

On the basis of the above trust semantics, the following inference rules for attestation and mediation trust are introduced using modus ponens to applied Axioms (2) and (3).

$$accept(p, x) \equiv trust^{a}_{pq}(x) \land assert(q, x), \quad (4)$$

$$accept(p, x) \equiv trust^{m}_{pq}(x) \land accept(q, x). \quad (5)$$

These logical rules enable information asserted by an entity to propagate via trusted entities in a network. Specifically, once an authentication authority has authenticated a user and asserted that the authentication context about the user is true, the asserted information can propagate among trusted entities in FIM systems.

### 3.3 Direct Trust and Propagation Trust for Authentication

For entity authentication, there are two types of trust: direct trust and propagation trust. To trust an entity directly means to confirm its identity. This means that direct trust for authentication corresponds to identity trust in Axiom (1), which is represented by $trust^{i}_{pq}(x)$ for trustor $p$, trustee $q$, and authentication context $x$. A case of direct trust is shown in Fig. 1; here, entity $p$ directly authenticates entity $q$, as indicated by the solid line from $p$ to $q$. In the remainder of this paper, this relationship is represented by symbol $p \to q$. Propagation trust expresses the certainty with which an entity accepts as trustworthy the information propagated from another entity having that information. The information refers to an entity other than the ones sending and receiving it. The trustworthiness of the information for its receiver depends on the trustworthiness of its sender because the sender holds and accepts the information. Propagation trust is categorized into two modes: attestation mode and mediation mode.

In the attestation mode of the propagation trust relationship between trustor $p$ and trustee $q$, it is $q$ that produces the information propagated to $p$. An attestation mode example of propagation trust is illustrated in Fig. 2; here, entity $p$ has propagation trust in entity $q$, which is represented by the dotted line from $p$ to $q$, while $q$ has direct trust in entity $r$. In the remainder of this paper, this propagation trust relationship is represented by $p \sim q$. In Fig. 2, trustee $q$ directly authenticates the other entity $r$ and produces an authentication

![Fig. 1](direct-trust.png) Direct trust for authentication ($p \to q$).

![Fig. 2](propagation-trust.png) Propagation trust in attesting entity ($p \sim q$).
The case shown.

to derive rules, which are general rules that are not specific to

is for the reader’s intuitional understanding of the de-

through entities is accurate.

propagated information such as an authentication result

principle [6], which leads to an inference about whether

3.4 Derivation of Direct Trust and Propagation Trust

In this axiom, \( \text{trust}_{pq}^{(a)}(x) \) denotes the attestation mode of

In this axiom, \( \text{trust}_{pq}^{(a)}(x) \) denotes the attestation mode of

In the mediation mode of propagation trust, a mediat-

In this section describes a formal algorithm for trust aggrega-

Rule 1 (Direct Trust Derivation)

This rule means that \( p \) has assurance in authentication context

Rule 2 (Propagation Trust Derivation for Attestation)

The derivation for mediation is similar to that for attes-

Rule 3 (Propagation Trust Derivation for Mediation)

These rules enable us to logically derive aggregated di-

4. Authentication Trust Quantification

This section describes a formal algorithm for trust aggrega-


4.1 Authentication Trust Value

A direct authentication occurs if an entity authenticates a user using an authentication context. The value of entity $p$'s direct authentication trust in entity $q$ with authentication context $x$, $v_{pq}^{(i)}(x)$, is defined on the basis of the semantics of Axiom (1) as

$$v_{pq}^{(i)}(x) = \Pr(\text{authn}(p, q, x)). \quad (11)$$

This trust value can be a probability derived from the data accumulated in transactions between $p$ and $q$. Alternatively, $p$'s administrator can set a value as a subjective probability or give a value as an assurance level in the range $[0, 1]$. For example, NIST Special Publication 800-63 (NIST: National Institute of Standards and Technology) [15] describes four assurance levels for the certainty values associated with an identity assertion according to the types of authentication mechanisms.

For propagation authentication trust, the acceptance of propagated information depends on the authentication of the entity propagating the information. On the basis of the relationship between probability and conditionals and the semantics of Axioms (2) and (3), the following values of authentication trust for attestation and mediation are defined.

$$v_{pq}^{(i)}(x) = \Pr(\text{accept}(p, x) | \text{assert}(q, x) \land \text{authn}(p, q, y)), \quad (12)$$

$$v_{pq}^{(i)}(x) = \Pr(\text{accept}(p, x) | \text{accept}(q, x) \land \text{authn}(p, q, y)). \quad (13)$$

Let $v_{pq}^{(i,a)}(x)$ and $v_{pq}^{(i,m)}(x)$ be the authentication trust values for $\text{trust}_{pq}^{(i,a)}(x)$ and $\text{trust}_{pq}^{(i,m)}(x)$, respectively, in Axioms (6) and (7). For simplicity, suppose that $v_{pq}^{(i)}$ is used to denote $v_{pq}^{(i,a)}(x)$ by omitting $x$ since $x$ is authentication result information and it is common to all axioms in this context. Then, the following equations are obtained:

$$v_{pq}^{(i,a)} = v_{pq}^{(i)} \cdot v_{pq}^{(a)}, \quad (14)$$

$$v_{pq}^{(i,m)} = v_{pq}^{(i)} \cdot v_{pq}^{(m)}. \quad (15)$$

4.2 Trust Value Calculation

On the basis of the above definitions of authentication trust values, the Beth-Borcherding-Klein (BBK) metric [8] is applied to calculate the values of direct and propagation trust (Fig. 5). In an aggregated trust value, the BBK metric reflects the direct trust value more than the propagation value when the two aggregated values are located sequentially in the trust chain.

4.2.1 Serial Trust Aggregation

Serial trust aggregation creates a new trust relationship from two existing trust relationships and assigns it a new trust value. If there is a path $p \leadsto \cdots \leadsto q$ with propagation value $v_{pq}^{(i,a)}$ and a direct edge $q \rightarrow r$ with value $v_{qr}^{(i)}$, then the direct trust value for the path $p \leadsto \cdots \leadsto q \rightarrow r$ is expressed using Eqs. (11) and (14) as follows (see Fig. 5 (a)).

$$v_{pr}^{(i)} = 1 - (1 - v_{qr}^{(i)}) v_{pq}^{(i,a)}. \quad (16)$$

If there is a path $p \leadsto \cdots \leadsto q$ with propagation trust value $v_{pq}^{(i,m)}$ and a propagation edge $q \leadsto r$, then the propagation trust value for path $p \leadsto \cdots \leadsto q \leadsto r$ is expressed using Eqs. (14) and (15) as follows (see Fig. 5 (b)).

$$v_{pr}^{(i,a)} = v_{pq}^{(i,m)} \cdot v_{qr}^{(i,a)}. \quad (17)$$

$$v_{pr}^{(i,m)} = v_{pq}^{(i,m)} \cdot v_{qr}^{(i,m)}. \quad (18)$$

Thus, if, in general, there are propagation paths $p \leadsto q$ and $q \leadsto r$, then the aggregated trust value $v_{pr}$ is obtained from Eqs. (16), (17), and (18) as

$$v_{pr} = \begin{cases} v_{pr}^{(i,a)} & \text{for attester } q, \\ v_{pr}^{(i,m)} & \text{for mediators } q \text{ and } r, \\ v_{pr}^{(i,m)} & \text{for mediator } q \text{ and attester } r. \end{cases} \quad (19)$$

4.2.2 Parallel Trust Aggregation

If, in general, there are multiple propagation paths, there will be multiple (aggregated) direct trust values as a result of serial trust aggregations. Parallel trust aggregation derives a new trust value for a path between two entities when there are multiple direct trust values for the path. The case where there are $K$ direct trust values for path $p$ and $q$ and the $k$-th path has trust value $v_{pq,k}$ is illustrated in Fig. 6.

Note that an SP (e.g., entity $p$ in Fig. 6) has a function that provides identity mapping between the identifiers of a user (e.g., entity $q$ in Fig. 6) shared with IdPs and the user’s local identifier at the SP for parallel trust aggregation. In FIM systems, different pseudonyms are often used for a user’s identifiers effective only for each pair of an SP and an IdP to protect the user’s privacy. In the case of Fig. 6, $p$ may receive multiple assertions each of which contains authentication context $x_k (1 \leq k \leq K)$ specifying the same user represented by identifier $id_k (1 \leq k \leq K)$. $p$ can identify that each different identifier $id_k$ indicates the same user whose identifier is $id$ by means of the identity mapping function.

Here, consider calculating a combined trust value from all the existing (aggregated) direct trust relationships and
their assigned trust values using the weighted aggregation approach. If $w_k$ denotes the positive weight for trust value $v_{pq,k}(1 \leq k \leq K)$, then aggregated direct trust value $v_{pq}$ is given by

$$v_{pq} = \sum_{k=1}^{K} w_k \cdot v_{pq,k}. \quad (20)$$

However, the above trust aggregation has sensitivity to misbehavior or threats that attempt to manipulate the output of trust values to increase the user’s identity assurance [9]. This sensitivity issue is illustrated as an example in Fig. 7. Entity $p$ has a mediation mode of propagation trust paths with entities $q$, $r$, and $s$ that have an attestation mode of propagation trust for entity $t$. Here, $t$ is the only attesting entity for $q$, $r$, and $s$ that directly authenticates $u$, but $q$, $r$, and $s$ receive the same authentication information from $t$: the aggregation approach sums up the values. In addition, entities $h_1$, $h_2$, and $h_3$ correspond to the same attesting entity $h$ but have different authentication events. Attesting entity $h$ can inflate its aggregated propagation trust value for $g \rightarrow u$ by increasing the number of authentication events if the weight values for the corresponding trust paths relatively increase in Eq. (20). Note that the trust value will also be sensitive when $h$ issues an excessive number of assertions for a single authentication event without any intention of making threats or attacks.

As a solution to the sensitivity problem, the approach of discovering similar authentication trust paths is proposed as an extension of the weighted aggregation. How much value is assigned to each weight depends on its parallel aggregation policy. The following policies are introduced according to what kind of factor takes precedence:

- (P1): Arithmetic mean of the values. This is simple as a basic policy although it is not resilient to inflation of the number of assertions. The weight $w_k$ is given by $w_k = 1/K$ for $k = 1, \ldots, K$.
- (P2): Mean of the $M$ highest values. $w_k = 1/M$ for $k = 1, \ldots, M$ and $w_k = 0$ for $k = K - M + 1, \ldots, K(0 \leq M \leq K)$ if $v_{pq,k}$ is sorted in reverse numerical order.
- (P3): Geometric distribution for the $M$ highest values, $w_k = \alpha(1-\alpha)^k$ for $k = 1, \ldots, M$ and $w_k = 0$ for $k = K - M + 1, \ldots, K(0 \leq M \leq K)$ if $v_{pq,k}$ is sorted in reverse numerical order, where $\alpha$ is the common ratio

$(0 < \alpha < 1)$ and $c$ is a normalized value given by $c = 1/(1-(1-\alpha)^K)$.

If we let $V_{pq} = \{v_{pq,k}|1 \leq k \leq K\}$ denote the set of $v_{pq,k}$, the aggregated trust value for policy $pol$, $v_{pq}(V_{pq}, pol)$, is given by

$$v_{pq}(V_{pq}, pol) = \sum_{k=1}^{K} w_k(pol) \cdot v_{pq,k}. \quad (21)$$

4.2.3 Aggregation Algorithm

A direct acyclic graph (DAG) is considered to aggregate a trust value between two entities using the above metric. Algorithm 1 shows a procedure for calculating the aggregated direct trust between SP $p$ and user $u (p \rightarrow u)$ in DAG $G$ that recursively simplifies its graph by replacing multiple paths with a single trust path labeled with a new trust value. Note that $p$ knows the trust paths through which individual assertions propagate and the authentication events attested in them. Let $E$ and $A$ denote entities and arcs in $G$, respectively. Note that each entity may be represented by multiple nodes, which are identified by the authentication event.

$N(u)$ denotes $u$’s neighbors that have direct trust relationships with $u$ (step 1). If path $(p, u)$ is the only path from $p$ to $u$ in $G$, nothing is done (steps 2–3). reachable$(p, q)$ denotes a utility function that returns true if there is path $p \rightarrow q$. Step 4 checks whether $p$ has only one path to $u$. If this holds true, then serial aggregation is executed; the last arc is deleted and a new trust path with its trust value is added to $G$ (steps 5–6). Step 7 checks whether $p$ has multiple nonintersecting paths to $u$. If this is true, parallel aggregation is performed; the aggregated trust value is calculated using the weighted aggregation approach in calcWeightedTrustValue (described later in Alg. 2) with an aggregation policy for discovering the similarity of trust paths (step 8), the last arcs in all paths from $p$ to $u$ are deleted (steps 9–11) and a new aggregated trust path with its trust

![Graph example.](image-url)
value is added to \( G \) (step 12). Otherwise, the above procedure is recursively called for each sub-graph (steps 13–17). Finally, this procedure is completed (step 18).

Algorithm 2 describes the procedure for calculating a weighted aggregated trust value depending on its aggregation policy. Step 1 excludes entities mediating or attesting assertions that have expired authentication events by referring to the authentication time, current time, and fixed authentication validity period. If the aggregation policy \( \text{pol} \) is P1, the arithmetic mean of the values involving the elements of \( E \) is returned (steps 2–4). Steps 5–13 produces the meta-set \( VS \) that consists of the value sets \( Vs \) containing aggregated trust values indexed by the identifier of an entity \( (e,i,d) \) for policies P2 and P3. Function \( \text{getValues} \) obtains value set \( V \) corresponding to the entity identifier from \( VS \) and function \( \text{putValues} \) registers \( V \) in \( VS \) by using the entity identifier as a key. As a result, each \( V \) in \( VS \) has aggregated trust values from the same entity. In steps 14–18, for each value set, a weighted aggregation trust value is calculated according to its policy. Function \( \text{sortReverseOrder} \) transforms a value set into one that has values in reverse order and \( \text{putValue} \) registers the calculated value by using the index number in value list \( VL \). This list contains trust values from different entities. Using the reverse-sorted list, the weighted aggregated value is finally calculated and returned (steps 19–20).

### 4.2.4 Trust Aggregation Example

The example shown in Figs. 8 and 9 demonstrates the trust aggregation procedure starting with the trust relationships shown in Fig. 7. The procedure applies Alg. 1 to obtain the aggregated direct trust value of \( p \rightarrow u \). In Fig. 7, \( u \) has neighbors \( t, h_1, h_2, \) and \( h_3 \).

The result of parallel aggregation between \( p \) and \( t \) is shown in Fig. 8 (a). Since \( t \)'s neighbors \( q, r, \) and \( s \) have one neighbor \( p \), parallel aggregation is applied for the sub-graph of \( G \) with \( p \) as the source and \( t \) as the sink. The aggregated trust \( p \rightarrow t \) is created and combined from three serial trust aggregations \( p \rightarrow q \rightarrow t, p \rightarrow r \rightarrow t, \) and \( p \rightarrow s \rightarrow t \). After the combination, arcs \( q \rightarrow t, r \rightarrow t, \) and \( s \rightarrow t \) are removed, and arc \( p \rightarrow t \) is added with its aggregated trust value.

The result of serial aggregations for the sub-graphs \( p \rightarrow q \rightarrow h_1, p \rightarrow q \rightarrow h_2, \) and \( p \rightarrow q \rightarrow h_3 \) are shown in Fig. 8 (b). In Fig. 8 (a), \( q \) is a mediating entity of \( p \) that has trust relationships with \( h_1, h_2, \) and \( h_3 \), each of which actually represents the same attesting entity \( h \), but is identified by its distinct authentication context. Three aggregated trust relationships \( p \rightarrow h_1, p \rightarrow h_2, \) and \( p \rightarrow h_3 \) are created and arcs \( q \rightarrow h_1, q \rightarrow h_2, \) and \( q \rightarrow h_3 \) are removed. Now \( u \) has four neighbors \( (t, h_1, h_2, \) and \( h_3) \), each of which has only one neighbor \( p \).

The result of parallel aggregation between \( p \) and \( u \) is shown in Fig. 9. After four serial trust aggregations \( p \rightarrow t \rightarrow u, p \rightarrow h_1 \rightarrow u, p \rightarrow h_2 \rightarrow u, \) and \( p \rightarrow h_3 \rightarrow u \), aggregated direct trust \( p \rightarrow u \) and its trust value are added, and arcs \( t \rightarrow u, h_1 \rightarrow u, h_2 \rightarrow u, \) and \( h_3 \rightarrow u \) are removed. As a result, the aggregated direct trust value for \( p \rightarrow u \) is obtained.
5. Authentication Trust Assessment

This section shows how the derived trust values are used to assess the authentication trust of a user in several use cases.

Access Control Using Multifactor Assertions. If an IdP has multiple types of authentication methods and issues authentication assertions about a user to an SP, the SP can assess the user’s identity trust by deriving the trust value and decide whether to grant the user access to a particular resource by comparing the value with a predefined threshold.

A use case in which IdP h provides SP p with authentication assertions about user u by means of two authentication methods—a basic authentication (using a password) and biometric authentication (using a fingerprint)—is shown in Fig. 10 (a). Since different authentication methods are provided by the same entity, the figure represents the IdP as two different attesting entities h1 and h2. The value allocated to each path represents the trust value for that path. Namely, \( v_{ph1}^{i} \), \( v_{ph2}^{i} \), and \( v_{hu}^{i} \) are equal to 0.9, 0.9, 0.6, and 0.9, respectively. Although these trust values are assumed to be given here to demonstrate the proposed trust assessment, they can be obtained by using the NIST publication or measured with the frequency rate of the trustor’s positive experiences among all encounters with the trustee [11]. In this case, since biometric authentication is known as a stronger authentication method than the basic authentication, \( v_{h2,u}^{i} \) is larger than \( v_{h1,u}^{i} \) whereas the trust values for attestation are the same. From Eq. (16), the aggregated trust value \( v_{pu,k}^{i} \) for \( k = 1, 2 \) is obtained as \( v_{pu,k}^{i} = 1 - (1 - v_{ph1}^{i}) v_{ph2}^{i} \). In applying Eq. (21) for P1, \( (w_{1}, w_{2}) = (0.5, 0.5) \), then the aggregated trust value \( v_{pu} \) is obtained as

\[
v_{pu} = w_{1} \cdot v_{pu,1}^{i} + w_{2} \cdot v_{pu,2}^{i} = 0.5 \cdot (1 - (1 - 0.6)^{0.9}) + 0.5 \cdot (1 - (1 - 0.9)^{0.9}) = 0.56 + 0.87 = 0.72.
\]

Consider that p’s administrator sets threshold values to 0.5 and 0.7 in u’s profile information to grant u permission to “read” and “write”, respectively. In this case, u is denied permission to update u’s profile if p has only an authentication assertion about u from h1 whereas u is granted permission to do so if p additionally obtains another authentication assertion from h2.

Access Control Using Assertions from Multiple Authorities. Figure 10 (b) shows different IdPs q, r, and s issuing authentication assertions about user u to SP p using the aforementioned basic and biometric authentication methods, respectively. The trust values \( v_{pq}^{i}, v_{pr}^{i}, v_{ps}^{i}, v_{pu}^{i}, v_{qu}^{i}, v_{qu}^{i} \), and \( v_{qs}^{i} \) are 0.9, 0.6, 0.9, 0.6, 0.9, and 0.9, respectively. With these assumptions, and in the same way as for the above use case, the aggregated trust value \( v_{pu,s}^{i} \) for \( s = q, r, s \) is obtained as \( v_{pu,s}^{i} = 1 - (1 - v_{pu}^{i}) v_{su}^{i} \). If the aggregation policy is P1, then the aggregated trust value \( v_{pu} \) for this use case is obtained as

\[
v_{pu} = w_{q} \cdot v_{pu,q}^{i} + w_{r} \cdot v_{pu,r}^{i} + w_{s} \cdot v_{pu,s}^{i} = 1/3 \cdot (1 - (1 - 0.6)^{0.9}) + 1/3 \cdot (1 - (1 - 0.9)^{0.9})
\]

\[
= 0.56 + 0.75 = 0.87
\]

where \( (w_{q}, w_{r}, w_{s}) = (1/3, 1/3, 1/3) \). If policy P3 (\( M = 2, \alpha = 0.75 \)) is applied, then the aggregated trust value \( v_{pu} \) for this case is obtained as

\[
v_{pu} = 0.56 \cdot 0.2 + 0.75 + 0.8 \cdot 0.87 = 0.85
\]

where \( (w_{q}, w_{r}, w_{s}) = (0, 0.2, 0.8) \). Like in the above use case, an SP can determine its access control decision for a user on the basis of a quantitative evaluation of authentication trust for the case in which multiple authentication authorities are involved.

Although the above two use cases are very simple because there are two or three attesting entities, it is possible to treat more complicated cases having multiple mediating entities and the combination of those entities.

Selection of Authentication Authority and Method. By means of the proposed trust value calculation, when an SP needs to authenticate a user, it can simulate and evaluate the aggregated trust values for possible authentication methods and authorities and choose appropriate ones among them in order to obtain a trust value that exceeds a threshold value. This cost is effective in FIM systems because an SP can selectively depend on an IdP for authentication of appropriate strength even if the SP itself does not have that capability.

6. Discussion

The proposed trust metric reflects the characteristics of relationship-focused systems and thus introduces entity-to-entity relations to quantitatively evaluate the identity trust of an entity. In some cases, it is necessary to combine the proposed trust metric and the one for credential-focused systems. For example, when an SP receives an assertion signed by an attester from a mediator, the SP can evaluate the integrity of the assertion by verifying the signature as well as
the mediation and attestation trust. Although the mediating trust is still needed because the mediator needs to associate between the identifier in the received assertion and the accessing subject, the signature verification involves discovering the trust chain of the attester’s signature key.

Other topics for future work include assigning appropriate trust values and establishing weights for trust aggregation with possible aggregation policies from a practical viewpoint. Furthermore, a feasibility study of the proposed trust value calculation still needs to be performed.

7. Conclusion and Future Work

This paper defined the semantics of authentication trust and described formal rules for deriving authentication trust using a trust reasoning approach for FIM systems. In addition, on the basis of the proposed representation, it quantitatively derived aggregated trust from a user’s authentication assertions propagated through multiple entities in order to evaluate the trustworthiness of the user’s identity. Future work includes incorporating the proposed metric with a traditional credential-based one and establishing a method for assigning appropriate values and weights for trust aggregation with its policies.

References


Hidehito Gomi received the B.Eng. degree from the Department of Applied Mathematics and Physics and the M.Eng. degree from the Division of Applied Systems Science, Faculty of Engineering, Kyoto University, Kyoto, Japan, in 1994 and 1996, respectively. From 1996 to 2007, he was a researcher in the laboratories of NEC Corporation. From 2001 to 2003, he was a visiting researcher in the Computer Science Department of Stanford University, CA, U.S.A. In 2007, he joined Yahoo! JAPAN Research, where he is continuing his research on security architecture, identity management, and trust management. He is a member of the IEEE-CS, ACM, and IPSJ.