Establishing Authentication Trust in Open Environment Using Social Approach

Hidehito Gomi
Yahoo! JAPAN Research
Yahoo! Japan Corporation
Tokyo, Japan
hgomi@yahoo-corp.jp

***Abstract*—A trust metric is described for a user to ensure the authenticity of another user who is not known to system entities in an open environment. On the basis of the metric, an identity federation framework is proposed for propagating an authentication assertion for an unknown user across system entities. The unknown user directly interacts with an authenticating user with the support of an entity mediating the authentication. By use of the proposed framework, an entity receiving an authentication assertion can derive and evaluate the trust value of its corresponding user in a quantitative fashion to flexibly control his or her access.**

***Keywords*-trust metric;identity federation;delegation**

I. Introduction

Conventional security systems usually need to authenticate users to control their accesses to restricted services. For this, the users are required to register their personal information and obtain credentials to be used for authentication. This is a common procedure and is a convenient way to clarify which entity is responsible for authorizing accesses. However, a user who would like to use a service but cannot be authenticated by the service often becomes unwilling to use the service because the process of registering personal information is troublesome or time-consuming. Namely, there is a trade-off between flexible service provisioning and secure access control.

A use case requiring flexible service provisioning is delegation, in which a user provides all or some of his or her privileges to another user to perform tasks. In delegation, the complexity of the system increases because the user attempting to execute a task (delegatee) is different from the user who already has privileges to perform the task (delegator) but who delegates the task. When a service provider (SP) does not have any information about the delegatee, access control based on his or her identity becomes impossible even if the SP knows about the delegator delegating the task to the delegatee. This situation occurs in many scenarios for open and distributed applications. If the SP obtains a certificate containing information about the delegatee issued by a trusted entity, the SP may possibly grant the delegated access by evaluating the trustworthiness of the delegatee's identity.

Much work on the exchange of security- and privacy-related information in terms of identity management has been conducted. Recently emerging technical specifications [1]–[3] provide a framework for federated identity management (FIM) systems. In this framework, an identity provider (IdP) authenticates a user by means of particular authentication methods and issues an authentication assertion about the user to an SP that provides a restricted service to authorized users. Although this framework enables propagation of information about an authenticated user based on trust between an IdP and SP, it still cannot propagate information about a user who has not been registered at the IdP, which is the same as in conventional security systems. In many delegation scenarios, a delegator trusts in a delegatee and can recognize his or her identity based on many criteria. Therefore, the information that a delegator has on a delegatee can effectively be shared for an SP to authorize the delegatee's access even if an IdP cannot authenticate him or her directly.

A trust metric for a user to authenticate another user who has not been registered in the system is proposed, as is the metric's framework for propagating the authentication information among the system entities, based on the author's previous work on FIM systems [4]. The framework introduces a specific authentication federation method by which a direct interaction between the two users can be reflected in the authentication assertion with the support of an entity that mediates the authentication. With the framework, an SP receiving the assertion about the unregistered user can flexibly control his or her access in a quantitative fashion.

The rest of this paper is organized as follows. Section II reviews related work. Section III introduces an authentication trust metric for FIM systems. Section IV proposes a user-centric authentication federation scheme. Section V describes the derivation of the authentication trust value for an entity calling a resource on behalf of its owner. Section VII concludes the paper and presents future work.

II. Related Work

Trust models, metrics, and formalization have been frequently researched. Prior work on general trust has focused on defining the semantics of trust and modeling trust-based systems. A variety of trust classes, trust types, and reputation systems [5] has been investigated.

Existing work on trust formalization focuses on assigning numerical values of trustworthiness to paths representing relationships between entities [6]–[8]. Beth et al. [6] presented a formal representation of trust relationships and the algorithms for deriving them to estimate the trustworthiness of entities in open networks. Reiter and Stubblebine [7] presented a set of guiding principles for the design of authentication metrics. Huang and Nicol [8] introduced a formal representation of trust in a public key infrastructure (PKI) and proposed a mechanism for quantifying trust in certificate chains. However, their models focused on general trust and do not deal with user-to-user authentication.

Work related to identity and trust management can also be found in the literature [9]. Thomas et al. [10] defined the semantics of the authentication trust level and provided a method for combining two trust levels of a multifactor authentication in a FIM environment. Although their work shares the author's goal of flexible and quantitative access control, it did not consider a social authentication approach as proposed in this work. Gomi [4] proposed an authentication trust metric for FIM systems. The author enhances his approach for propagating the trust level of a person to a more general framework for controlling access by an unregistered user by using social authentication in an open environment.

Another related line of research is end-to-end trust establishment methods in limited network environments. Seigneur et al. [11] proposed an entity recognition approach in which dynamic enrollment enables spontaneous interactions with unknown entities in pervasive computing environments. Theodorakopoulos and Baras [12] proposed a method for evaluating trust between entities in ad-hoc networks. The limitation of these methods is that they do not support the derivation of authentication results among entities.

III. Authentication Trust for Identity Federation

This section describes the semantics and the formal representation of authentication trust for FIM systems [4].

A. 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 statement, *authentication context* [13] denotes the information about the characteristics of the mechanisms and processes by which the authentication confirms the entity's identity. For example, the information includes authentication methods such as presentation of a password over a protected transport channel and verification of a digital signature using an X.509 certificate. The authenticating entity validates the presented credential and determines the trustworthiness of the entity with some level of certainty depending on the above authentication context.

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

$$trust^{(i)}_{pq}(x) \equiv authn(p,q,x) \qquad x \in AC, \tag{1}$$

where AC stands for a set of information about the authentication context, $trust^{(i)}_{pq}(x)$ expresses that entity p has identity trust in entity q on the basis of a specific authentication context x, and $authn(p,q,x)$ means that entity p authenticates entity q by means of an authentication method represented in an authentication context x. This axiom represents 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. In such a *credential-focused* system, long-term, non-transitive cryptographic credentials such as X.509 are issued without involving an IdP [14].

In contrast, FIM systems are *relationship-focused* ones in which an online IdP dynamically issues short-term security tokens while restricting its transitivity on the basis of the relationships between the issuer (IdP) and recipient (SP). In this paper, a formal representation of authentication trust by introducing the above trust relationship is examined. The following definitions are related to the identity-trust-deriving capabilities that are specific to FIM systems.

Definition 2 (Attestation Trust). *Attestation trust is the certainty about an 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.*

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

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

where $assert(q,x)$ means that q creates an assertion containing information x and $accept(p,x)$ represents p accepting that x is true. The ⇒ 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.

In the above axiom, x is general propagated information. However, if x corresponds to an authentication context, the

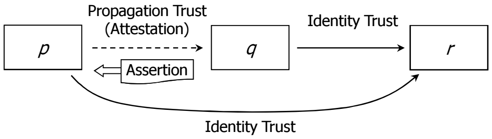


Figure 1. Authentication trust transitivity.

axiom specifically denotes that the authentication context is propagated from q to p in a particular encoded format. This leads to the establishment of authentication trust as a basic principle in FIM systems.

B. Authentication Trust Derivation

For derivation of user authentication, *propagation trust* is defined as follows.

$$trust_{pq}^{(i,a)}(x) \equiv trust_{pq}^{(i)}(y) \wedge trust_{pq}^{(a)}(x). \qquad (3)$$

In this axiom, $trust_{pq}^{(i,a)}(x)$ denotes the attestation mode of propagation trust from p to q regarding information x that q propagates to p. This means that p has attestation trust in q regarding information x and p also has identity trust in q. Note that the authentication context propagated to p is not q's authentication context y but x.

The basic principles of trust-based systems are described in previous literature [5]. In general, trust transits from entity to entity. The idea behind *trust transitivity* is that when Alice trusts Bob, and Bob trusts Charlie, and Bob refers Charlie to Alice, then Alice can derive a measure of trust in Charlie based on Bob's referral combined with her trust in Bob. Although this principle holds true for authentication trust in FIM systems, it additionally involves end-to-end authentication procedures for deriving trustworthy information about the authenticity of an entity as well as the attesting capability of an entity propagating the information. This is illustrated in Figure 1. The solid and dashed lines indicate identity trust and propagation trust, respectively, from the viewpoint of r's authentication.

From this observation, the following rule is obtained.

Rule 1 (Authentication Trust Derivation).

$$trust_{pr}^{(i)}(x) \Leftarrow trust_{pq}^{(i,a)}(x) \wedge trust_{qr}^{(i)}(x). \qquad (4)$$

This rule means that p has assurance in an authentication assertion containing x regarding r attested by q since p trusts in q's identity and attestation capability. It clearly explains a typical identity federation scenario in which p, q, and r correspond to an SP, an IdP, and a user, respectively, in FIM systems. The authentication trust in r transits from q to p in the opposite direction of the propagation of the assertion encapsulating x.

IV. User-managed Authentication

This section proposes a new scheme for obtaining authentication trust within the scope of the trust model described in Section III.

A. User-managed Authentication Trust

First, a definition for a trust semantic is given.

Definition 3 (User-managed Authentication Trust). *User-managed authentication trust is the certainty about a user's capability to authenticate another user within a particular authentication context with the support of an entity mediating the authentication (authentication mediator).*

In the above statement, "user-managed authentication" (UA) means an authentication procedure in which a user (trustor) him or herself directly authenticates another user (trustee) online. The trustor has some capability of identifying the trustee, and confirming the identity of the trustee by means of an authentication method and procedure. However, the trustor does not have any capability for attestation as defined in Definition 2, so he or she needs assistance in performing the authentication and in demonstrating the trustworthiness of the authentication results.

The authentication mediator (AM) mediates UA by providing an infrastructure for the above assistance to a trustor. The AM can provide a secure transport channel for interactions with and between a trustor and a trustee, and can monitor the interactions so that the validity of the authentication procedure between the trustor and trustee is ensured. Since the AM has some capability for attestation, it can produce and issue an assertion stipulating an authentication event within a specific authentication context regarding UA. With this scheme, an entity receiving an assertion of UA can evaluate the trustworthiness of a trustee's identity within the scope of FIM systems described in Section III.

Various types of authentication contexts for UA can be considered. Following are some examples.

Examples (User-managed Authentication Contexts).

- Secret code sharing. A trustor provides a trustee with a secret code unique to the trustee as a password that the trustee needs to present during authentication in a secure way such that it is not disclosed to other users.
- Secret questions. A trustor asks a trustee questions about information that is shared only with the trustee as a means of authenticating the trustee in a secure communication mediated by an AM. If the trustor receives answers from the trustee and accepts them as appropriate, the authentication successfully ends, with the trustor having confidence in the trustee's identity.
- Context validation. A trustor specifies the type of a trustee's context (e.g., geo-location) to an AM and then validates the appropriateness of the context information obtained by the AM using its functionality (e.g., GPS). For example, if the trustor is close to the trustee, the geo-location should indicate that the trustee is within a short distance from the trustor's current location.

As shown in the above examples, there are variations about which entity (trustor or AM) has the knowledge and

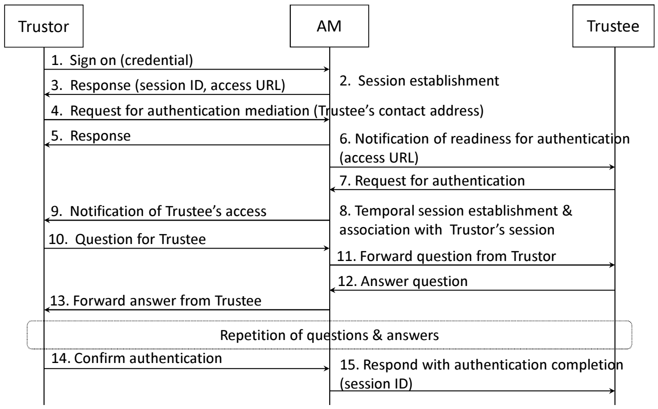

Trustor
AM
Trustee
1. Sign on (credential)
2. Session establishment
3. Response (session ID, access URL)
4. Request for authentication mediation (Trustee's contact address)
5. Response
6. Notification of readiness for authentication (access URL)
7. Request for authentication
8. Temporal session establishment & association with Trustor's session
9. Notification of Trustee's access
10. Question for Trustee
11. Forward question from Trustor
12. Answer question
13. Forward answer from Trustee
Repetition of questions & answers
14. Confirm authentication
15. Respond with authentication completion (session ID)

Figure 2. Interactions for user-managed authentication.

functionality for performing authentication and validating the procedure. In the contexts, the entity and how it validates are specified for SPs to evaluate the strength of the authentication.

B. User-managed Authentication Interactions

The following authentication interactions are considered as instances of UAs, shown in Figure 2.

1) First, the trustor signs on, presenting his or her credentials to the AM.
2) The AM establishes a session and assigns it with an identifier after validating the trustor's credential.
3) The AM returns a response including the session identifier and a URL that the trustor can access to request UA mediation.
4) The trustor sends a request for UA at the received URL attaching the trustee's contact address.
5) The AM responds in acknowledgement and tells the trustor to wait for the trustee to access the URL.
6) The AM informs the trustee that the trustor will authenticate the trustee at the access URL of the AM.
7) The trustee is given access to the specified URL for authentication.
8) When the AM receives the authentication request from the trustee, it assigns a temporary session to the trustee and associates the session with the trustor's session.
9) The AM informs the trustor of the trustee's authentication request and prompts the trustor to input his or her question for the trustee.
10) The trustor presents his or her question to the AM.
11) The AM shows the trustor's question to the trustee in the session of the trustee associated with the trustor's one.
12) The trustee sends the answer to the received question to the AM.
13) The AM forwards the received answer to the trustor. The trustor determines whether the answer is appropriate to trust in the trustee's identity.

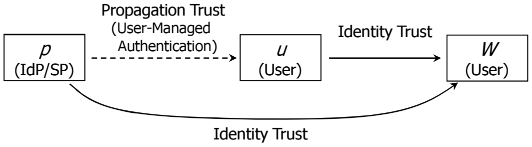


Figure 3. User-managed authentication trust.

14) The trustor obtains more confidence in the trustee's identity by repeating Steps 10–13. If the trustor has adequate assurance in the trustee's identity, the trustor notifies the AM of the authentication completion.
15) The AM updates the trustee's session so that it indicates that the trustee has a legitimate identity as claimed by the trustor.

During the above authentication interactions, the messages are transmitted in a secure communication channel. For each interaction, a specific authentication context is defined for characterizing its authentication method and strength.

C. User-managed Authentication Trust Derivation

In the authentication interactions described above, the AM is not involved with the sharing and validation of the credentials or questions. Instead, it mediates the exchange and confirmation of that information between the trustor and the trustee. Although the AM does not directly execute the procedure for authenticating the trustee, it can accept the trustee's identity as authenticated by the trustor in accordance with the AM's identity trust in the trustor, i.e., UA trust. These relationships are illustrated in Figure 3. The trust relationships among the entities shown in this figure are similar to the ones depicted in Figure 1. However, entity q in Figure 1 has an attesting capability whereas user u in Figure 3 does not have such a capability for propagating an assertion including authentication results to another party using a secure communication channel.

Let $trust^{(ua)}_{pq}(x)$ designate UA trust of trustor p in trustee q regarding authentication context x. By using this, Definition 3 is formally given as follows:

$$trust^{(ua)}_{pu}(x) \equiv authn(u, w, x) \Rightarrow accept(p, x). \qquad (5)$$

In this axiom, $trust^{(ua)}_{pu}(x)$ means that if u authenticates w in authentication context x, p accepts x.

The UA trust of p in user u naturally depends on the identity trust in u since it is from u that p receives the authentication context. Here, another propagation trust for UA from p to u, $trust^{(i,ua)}_{pu}(x)$, is defined as follows:

$$trust^{(i,ua)}_{pu}(x) \equiv trust^{(i)}_{pu}(y) \wedge trust^{(ua)}_{pu}(x). \qquad (6)$$

With this axiom, the rule of the authentication trust derivation for UA is as follows.

Rule 2 (User-managed Authentication Trust Derivation).

$$trust^{(i)}_{pw}(x) \Leftarrow trust^{(i,ua)}_{pu}(x) \wedge trust^{(i)}_{uw}(x). \qquad (7)$$

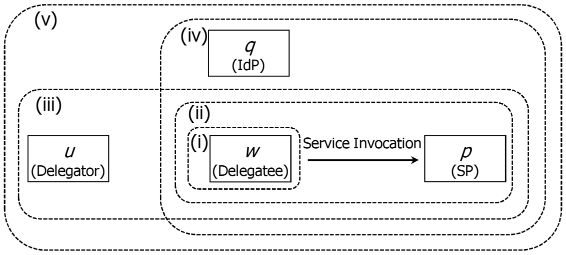


Figure 4. Combinational cases for delegatee authentication.

V. Authentication Trust Evaluation for Delegatees

This section examines the authentication trust in a delegation situation in which a delegator delegates to a delegatee the delegator's privilege to access his or her personal information. Let us assume that there are an IdP, an SP, and two users (delegator and delegatee). The IdP has an attesting capability and the SP grants or denies the delegatee's access in accordance with his or her authentication trust.

A. Authentication Trust in Delegatees

The following cases for collaboratively authenticating a delegatee are possible. They are shown in Figure 4, where the areas surrounded by the dotted lines indicate the scope of the entities involved with a delegatee's authentication. Consider the authentication trust of an SP in a delegatee for each case.

(i) **Anonymous access.** SP p does not identify delegatee w's identity because p does not have any information about w.

(ii) **Authentication by SP.** SP p successfully authenticates w directly by itself. In this case, the authentication trust in w corresponds to $trust^{(i)}_{pw}(x)$ if its authentication context x is given, as defined in (1).

(iii) **UA supported by SP.** SP p obtains UA trust in w by means of delegator u's corresponding direct authentication of w. Its authentication trust $trust^{(i)}_{pw}(x)$ is obtained using (7).

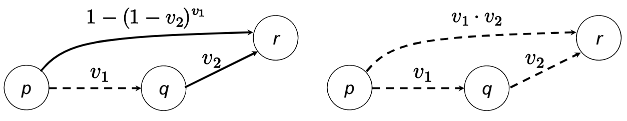
(iv) **Authentication federation between IdP and SP.** IdP q directly authenticates w and provides p with its corresponding authentication assertion related to authentication context x for w. Its authentication trust is given by (4).

(v) **UA supported by IdP plus authentication federation between IdP and SP.** First, IdP q obtains UA trust in w by means of delegator u's corresponding direct authentication of w. Its authentication trust is represented by $trust^{(i)}_{qw}(x)$ using (7),

$$trust^{(i)}_{qw}(x) \Leftarrow trust^{(i,ua)}_{qu}(x) \wedge trust^{(i)}_{uw}(x). \quad (8)$$

Then, by applying (7) and (8) to (4), the authentication trust $trust^{(i)}_{pw}(x)$ is obtained as follows:

$$trust^{(i)}_{pw}(x) \Leftarrow trust^{(i,a)}_{pq}(x) \wedge trust^{(i)}_{qw}(x). \quad (9)$$



(a) Propagation trust aggregation. (b) Direct trust aggregation.

Figure 5. Trust aggregation with Beth-Borcherding-Klein metric.

In this way, possible cases for authentication trust in a delegatee are driven using the proposed trust model for an SP to control the delegatee's access.

B. Authentication Trust Calculation

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

$$v^{(i)}_{pq}(x) \overset{\text{def}}{=} \Pr(authn(p,q,x)). \quad (10)$$

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 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 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 (2) and (5), the following values of authentication trust for attestation and mediation are defined:

$$v^{(a)}_{pq}(x) \overset{\text{def}}{=} \Pr(accept(p,x)|assert(q,x) \wedge authn(p,q,y)), \quad (11)$$

$$v^{(ua)}_{pq}(x) \overset{\text{def}}{=} \Pr(accept(p,x)|accept(q,x) \wedge authn(p,q,y)). \quad (12)$$

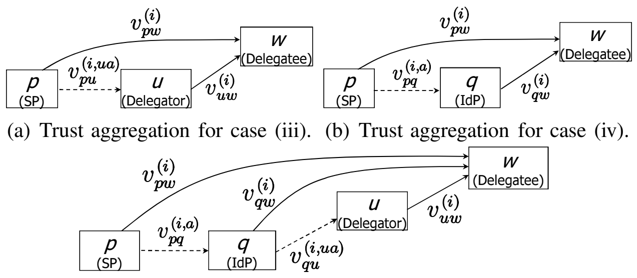
Let $v^{(i,a)}_{pq}(x)$ and $v^{(i,ua)}_{pq}(x)$ be the authentication trust values for $trust^{(i,a)}_{pq}(x)$ and $trust^{(i,ua)}_{pq}(x)$, respectively, in (3) and (6). The following equations are then obtained:

$$v^{(i,a)}_{pq}(x) = v^{(a)}_{pq}(x) \cdot v^{(i)}_{pq}(x), \quad (13)$$

$$v^{(i,ua)}_{pq}(x) = v^{(ua)}_{pq}(x) \cdot v^{(i)}_{pq}(x). \quad (14)$$

On the basis of the above definitions of authentication trust values, the Beth-Borcherding-Klein (BBK) metric [6] is applied to calculate the values of direct and propagation trust, shown in Figure 5. In an aggregated trust value, the BBK metric reflects the direct trust value more than the propagation value when the two values aggregated are sequentially located in the trust chain.

Next, each trust value for the five cases explained in Section V-A is calculated. The trust value for w's anonymous access, shown in case (i), is 0, since p does not have any information about w. The trust value for case (ii) is



(a) Trust aggregation for case (iii). (b) Trust aggregation for case (iv).

(c) Trust aggregation for case (v).

Figure 6. Authentication trust aggregation for delegatees.

equal to $v_{pw}^{(i)}(x)$, as defined in (10). The trust aggregations for cases (iii), (iv), and (v) are shown in Figures 6(a), 6(b), and 6(c), respectively. If we let a utility function $F(v_1, v_2)$ calculate $1 - (1 - v_2)^{v_1}$ for propagation trust aggregation in Figure 5(a), $v_{pw}^{(i)}(x)$ for cases (iii) and (iv) are obtained as $F(v_{pu}^{(i,ua)}(x), v_{uw}^{(i)}(x))$ and $F(v_{pq}^{(i,a)}(x), v_{qw}^{(i)}(x))$, respectively. Similarly, $v_{pw}^{(i)}(x)$ for case (v) is derived as $F(v_{pq}^{(i,a)}(x) \cdot v_{qu}^{(i,ua)}(x), v_{uw}^{(i)}(x))$ using the above results.

VI. Discussion

The proposed model enables authentication of a trustee who is not known to an AM by a trustor's identification of the trustee. This is effective because the scheme does not require registration of the trustee, which is needed for authentication in conventional security systems and often causes users to forgo proceeding with use of the service.

An IdP in the proposed framework can propagate authentication contexts using UA to SPs. In this approach, there is some vulnerability to a malicious trustor's attestation of a false or invalid authentication context. In this case, an SP receiving the context about an illegitimate trustee may grant his or her access inappropriately. Therefore, the framework needs to have a method for evaluating the trustworthiness of users and assessing the risk associated with their access as well as a formal and semantic representation of authentication contexts for UA, which will be future work.

UA can especially be strengthened if an AM can gain a trustee's accurate authentication context using its functionality that is validated by the trustor, as explained in the context validation example. In this sense, the strength of UA varies in authentication methods and their combinations. However, the flexibility of UA arises from the responsibility for authentication lying not with an AM, but with a trustor. This is an open issue in terms of which entity ensures a trustee's identity and how its integrity is assured.

VII. Conclusion and Future Work

A trust metric for deriving authentication context in an open environment was described. Based on the model, an authentication federation framework was proposed for propagating authentication trust in a person. In the framework, a user trusting in the person and an entity mediating the user's authentication of the person share the corresponding authentication context in a user-centric way. The logically derived authentication trust enables flexible access control in a quantitative fashion. Future work includes further investigation on the representation of authentication contexts, the responsibility of authentication, and risk assessment using the proposed framework.

References

[1] OASIS, "Assertions and protocol for the OASIS security assertion markup language (SAML) v2.0," Mar. 2005.

[2] IBM, Microsoft, BEA, RSA, and VeriSign, "Web Services Federation Language," Jul. 2003.

[3] OpenID, "OpenID Authentication 2.0 - Final," Dec. 2007.

[4] H. Gomi, "An Authentication Trust Metric for Federated Identity Management Systems," in *Proceedings of the 6th International Workshop on Security and Trust Management (STM'10)*, Sep. 2010, pp. 113–128.

[5] A. Jøsang, R. Ismail, and C. Boyd, "A Survey of Trust and Reputation Systems for Online Service Provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, Mar. 2007.

[6] T. Beth, M. Borcherding, and B. Klein, "Valuation of Trust in Open Networks," in *Proceedings of the 3rd European Symposium on Research in Computer Security (ESORICS'94)*, 1994, pp. 3–18.

[7] M. Reiter and S. Stubblebine, "Authentication Metric Analysis and Design," *ACM Transactions on Information and System Securiry*, vol. 2, no. 2, pp. 138–158, 1999.

[8] J. Huang and D. Nicol, "A Calculus of Trust and Its Application to PKI and Identity Management," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet (IDtrust'09)*, Apr. 2009, pp. 23–37.

[9] A. Jøsang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust Requirements in Identity Management," in *Proceedings of the Australasian Workshop on Grid Computing and E-research*, 2005, pp. 99–108.

[10] I. Thomas, M. Menzel, and C. Meinel, "Using Quantified Trust Levels to Describe Authentication Requirements in Federated Identity Management," in *Proceedings of the ACM Workshop on Secure Web Services (SWS'08)*, Oct. 2008, pp. 71–80.

[11] J.-M. Seigneur, S. Farrell, C. D. Jensen, E. Gray, and Y. Chen, "End-to-End Trust Starts with Recognition," in *Proceedings of the 1st International Conference on Security in Pervasive Computing (SPC'03)*, 2003.

[12] G. Theodorakopoulos and J. Baras, "Trust Evaluation in Ad-Hoc Networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSe'04)*, 2004, pp. 1–10.

[13] OASIS, "Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0," Mar. 2005.

[14] A. Bhargav-Spantzel, J. Camenish, T. Gross, and D. Sommer, "User Centricity: A Taxonomy and Open Issues," *Journal of Computer Security*, vol. 15, no. 5, pp. 493–527, 2007.

[15] W. Burr, D. Dodson, and W. Polk, "Electronic Authentication Guideline," Apr. 2006, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.