A Service Framework based on Grades of IdPs and SPs

SATO Hiroyuki
Information Technology Center,
The University of Tokyo, Japan.

Abstract— *In Web services, a framework for the separation of authentication (IdP) and services (SP) has been proposed and actually deployed. In this framework, quality of information provided by IdPs and SPs must be evaluated to assure the security of services. In this paper, we propose a security model in which IdPs and SPs obtain grades according to their assurance of services, and exchange information when the grade of counterparts matches their requirement. Our model gives grades to both IdPs and SPs, while in the conventional model, IdPs are the targets of grades. We also give criteria for evaluation of grades of IdPs and SPs. Grades of IdPs are given based on conventional CP/CPS and the NIST standard. Grades of SPs are given based on the risk assessment of information security used in ISMS etc., and on a general security criteria for system administrations/operations. Moreover, we propose security trust engineering as the generalization of security analysis based on grades. A matching mechanism of grades is discussed as an application of security trust engineering.*
Keywords: *LoA, security policy, IdP, SP*

1. Introduction

As a part of Web services, SAML[16] based authentication is proposed and deployed as a framework of Web service security. Also in conventional frameworks, PAM (Pluggable Authentication Method) is provided to many applications, which leads to building a server for authentication in an organization. As their results, it becomes common that services are separated from authentication. InCommon[18] is built as a Shibboleth[22] based federation system. OpenID[21] also provides IDs to service providers in concern.

This framework has brought a problem: the quality of information provided by other providers. Quality of information provided by IdPs and SPs must be evaluated to assure the security of services. Traditionally, SPs have had their own authentication process, which means that they are responsible for identities in their processes. However, as the two are separated, an SP must evaluate the quality of the ID information that is provided by another party. This "quality" is generally termed as LoA, "Level of Assurance."

The evaluation often causes conflict. For example, in 2007, in the process that NIH provides some service to InCommon, NIH evaluated the quality of IdPs of InCommon according to the US federal standard[2]. This was a major motivation of InCommon that InCommon introduced LoA to raise the level of IdPs under InCommon[9].

LoA is generally given to an ID system. In a common scenario, SPs are mainly concerned with the quality of information on authentication. However, as it becomes common that servers exchange information of their own, and as grades are given to information exchanged by servers, it becomes indispensable that the quality of information exchanged by SPs is also evaluated. In particular, considering the fact that a grade of information is given based on risk analysis in an organization, this must be discussed in compliance with security policies in an organization.

In this paper, we discuss LoA and grades of information. Specifically, they are applied to SPs and IdPs that are concerned with quality of information exchange between providers. Providers evaluate the grade of their counterpart, and according to the grade, they decide whether or not to release their information. It is an essential assumption that grades are given in an organization. The goals of this paper are to propose a solution to a conflict of SPs and IdPs caused by LoA, and to give criteria of evaluation of information assets in the implementation of a security policy, which leads to security trust engineering.

The rest of this paper is organized as: Section 2 discusses scenarios in which grades of information are essential. In Section 3, we study criteria for the assignment of grades. In Section 4, we propose security trust engineering. In Section 5, a grade matching mechanism is discussed as the first application of security trust engineering. Section 6 surveys related work. Section 7 summarizes this paper.

2. Scenario of Grades

2.1 Grades of IDs

Traditionally, grades are given to ID providers. We consider the scenario in that a human obtains information through a client program (browser) from a given server. To access the server, a human or a client program must be authenticated. A problem is that the server is concerned with the certainty of the authentication. In a modern framework, authentication is processed by a separate party. The server

is just using the authentication information. As independent ID providers such as OpenID appear, it becomes critically essential that a server evaluates the quality of the supplied IDs.

The problem to what extent an ID in use represents a specified human is attacked by identifying the quality of ID management, and the authentication method of the ID. The former can be rephrased as the quality of ID lifecycle management. The latter is the same as the strength of the authentication method.

Actually, this solution is organized in the four grade form in NIST SP800-63. It can be enhanced by recent discussions about the ID lifecycle management. Particularly in universities, where members can change regularly in a year, lifecycle management must be stressed on.

2.2 Grades of Servers

It becomes common that servers exchange information without intervention of humans. When IdPs or SPs release information to other servers, two problems arise: the identification of the communicating party and the level of information. The two must be independently discussed. In general, the former is rephrased as the LoA of server certificates, and the latter is evaluated by the security management of the servers.

2.2.1 Identification of Servers

This problem is inspired by today's confusions on server certification. WTCA(Web Trust for CA) qualification is widely used as the trust of server certificates. However, inspecting the criteria for WTCA[3], we see that there is much space for interpretation. Therefore we see gaps between strictly operated CAs and loosely operated CAs. As its result, the trust to loose CAs has been collapsed. Highly trusted CAs, together with browser vendors, establish EV-certificates[5], and differentiate themselves to loose CAs. Moreover, in Japan, cell phone vendors also characterize high CAs by denying trusting loose CAs. Thus, we can observe a kind of stratification of trust here.

2.2.2 Quality of Information at a Server

We consider cases that a server (IdP or SP) releases its information to another server. For example, the information may be an attribute information of a given ID (in the case of IdP) or may be database entries stored in an SP. In implementing security policies in an organization, it is common that first, information is given its rank in confidentiality, integrity, availability by using a method of risk analysis. The next step is to store the information of a given rank in a server that is operated at an appropriate security level. Highly ranked information must be stored in a securely operated server. Less highly ranked information can be stored in a less secure server, considering the cost of operation. Therefore, we can approximate grades of servers with ranks of information in the servers.

We consider the following scenario: let a grade N be given to a server. This means that at the server, information up to rank N can be stored.

Then,

1) A server of grade M requests some information to a server of grade N.
2) The server of grade N checks the grade of the requesting party. If its grade is higher than that of N ($N < M$), then the server releases its information to the requesting party.

As one of the principles of the theory of information flow, highly ranked information must not be released to less ranked object. Here, we regard "information of rank N" as "information stored in a server of grade N," by which we can interpret grades of servers as ranks of information.

Assignment of a grade to a server is reduced to identifying the security level of administration of the server. Criteria in an organization must be used there. For example, if a security policy of an organization is operated under ISMS (ISO/IEC 27000 series), it can be used as the criteria of the organization.

In summary, we must consider grades of servers together with grades of IDs. There is an agreement as for the importance of evaluating a grade of a given ID. In near future when servers constantly exchange information in Web service framework, we must evaluate grades of servers for secure information exchange. We summarize the scenarios in Fig. 1.

2.3 Correspondence of IdP Grades and SP Grades

Note that grades of IdPs and those of SPs are evaluated in different views. Strictly, grade N of an IdP is not equivalent to that of an SP. In order to use grades in access control as explained above, some policy or agreement must support correspondence of two different grades. Therefore, a security policy. A security policy must control assignment of grades to IdPs or SPs. Then, in an organization under the security policy, grades become effective in controlling access of/by servers.

3. Criteria of Grades

3.1 Grades of IdPs

According to NIST SP800-63, there are four criteria in evaluating grades of IdPs:

1) Binding of a token to a specified person (Token).

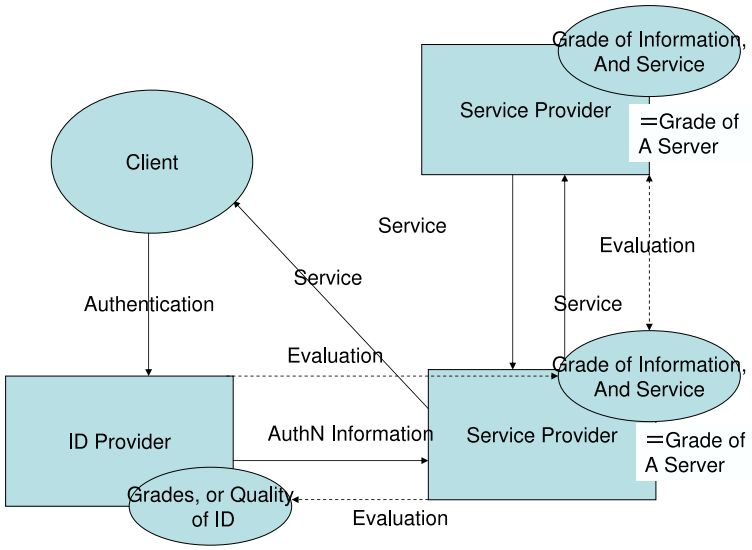

Fig. 1: IdP, SP, and Grades

2) ID proofing.
3) Authentication.
4) Assertion.

Each axis has four ranks in evaluation. The least scored grade in the four axes is the overall grade.

There are some other criteria. In PKI, RFC 3647[6] is defined as a framework of CP/CPS. Actually, this can also be interpreted in the framework of the NIST standard. We rephrase these criteria in two viewpoints: the quality of ID lifecycle management and the quality of authentication. We define our criteria as:

IdP-A *Criteria on ID lifecycle management*:

1) Token.
2) ID lifecycle.

IdP-B *Criteria on Quality of Authentication*:

1) Authentication.
2) Assertion.

Each criterion of IdP-A and IdP-B is brought from the NIST standard. Here, we discuss ID lifecycle management as the enhanced ID proofing. ID proofing criteria of the NIST standard mostly focus on initial identification. However, modern ID management requires that the whole process from ID creation to destruction must be appropriately controlled. In other words, this type of ID lifecycle management must be *organizational*. Furthermore, it is characterized that its origin must be the ID master record of an organization. In particular, a modification of attributes of a member must be appropriately reflected as the corresponding modification of the ID master record. It must (semi-)automatically activate the modification on subsequent phases of ID management. In this meaning, we assume that IDs must be controlled in an organization. Therefore, a grade can be given by evaluating the policy and the practice statement of IDs in an organization. Some IdPs do not assume a specific organizational domain. Most commercial IdPs do not, and OpenID do not too. Coverage of such IdPs is a future work.

3.2 Grades of SPs

According to the scenarios of server grades, we list two categories of criteria:

SP-A *Criteria on Server Authentication*:

1) Quality of ID proofing (LoA of FQDN proofing)
2) Quality of token (protection of an SSL private key)

Problems to be solved are related to the LoA of FQDN of the communicating servers. They are parallel to LoA of human IDs. According to the NIST standard, ID proofing and token management are significantly important. ID proofing of FQDN is implemented in the inspection of SSL server certificates. There are several criteria of server certification. The EV-SSL standard and WTCA standard are available here. Today, these standards are visualized in colors (green for EV-SSL, white for WTCA or its compatibles, red for others) of address bars of major browsers.

The quality of token management is independent of the LoA of FQDN proofing, although it has often been confusingly discussed. Therefore, we make it a separate item here.

Moreover, we need criteria of the quality of information in a server, together with the quality of how strictly a server is controlled. The two criteria are coupled, resulting the criteria SP-B below:

SP-B *Criteria on Quality of Information in a Server*:

1) Quality of information stored in the server.
2) Quality of management of the server:
   a) Management of access control
   b) Control of physical security.
   c) Management of privileges in operation

As for control of operation of a server, there have been proposed and tested a number of criteria, some of which are summarized as ISO 27000 series. Referring to the conventional criteria and RFC 3647, we propose SP-B-2-a,b,c.

A grade of SP-A-1 is given by evaluating CP/CPS of the issuing CAs. As for SP-A-2 and SP-B, a grade is given by evaluating security policies implemented in an organization.

4. Security Trust Engineering

Today, grades are not given in real numbers, but in three or four discrete values. This is because the cost of evaluation is high, and we do not need fine control of security.

Although this certainly optimizes the evaluation cost, it brings extra cost to upgrade LoA. If a security enhancement is brought by reasonable cost, it is reasonable to reflect the security upgrade as LoA upgrade. This much resembles to the complex pricing of insurance. To avoid complicated LoAs, it is reasonable that we restrict levels of LoAs to three or four. However, this results in unreasonable cost to upgrade to the next level.

To partially solve this dilemma, we propose adding $\pm\varepsilon$ to LoA.

Example 1: For example, let us assume that OTPW (one time password) is given grade 3 in an organization. Consider a case where an IdP authenticates its ID with OTPW-like mechanism, but its LoA is somewhat lesser than OTPW. Conventionally, grade 2 is given in this case.

However, if some risk analysis concludes that the OTPW-like method has almost the same LoA as OTPW, and the risk can be accepted under reasonable cost, then the method can be graded as $3-\varepsilon$. Actually, the high security of OTPW is guaranteed by the fact that a hardware token is given to a principal, and the passphrase supplied by the token is used only once by the principal.

It is easy to write a program that supply a passphrase in limited duration. If we use strong authentication to get the passphrase, the only difference to OTPW is the duration of passphrase. If a finer risk analysis can evaluate this downgrade to ε, and we determine to accept this ε, a software OTPW can be used in the same way as OTPW.

Example 2: Let us consider authentication by using ID and password. Usually, grade 2 is given. It is well known that it is hard to keep the quality of passwords. Some additional password policies are defined and implemented as PWDPOLICY on OpenLDAP, PWPOLICY on Sun Java Directory Servers, and an IETF expired draft[17]. It is reasonable to upgrade the LoA of LDAP authentication of password authentication to $2+\varepsilon$, if the LDAP server adopts an appropriate password policy to control the quality of passwords.

Example 3: Let us assume that the issuer of the certificate is given a grade N. As in the same discussion of IdP authentication, a closer evaluation of LoA in SP-A-1 by inspecting CP/CPS of specific certificates can result in upgrade to $N+\varepsilon$.

Actually, major certificate vendors deliver seals to certificates. They claim that a sealed Web page is certified by the corresponding vendor, and the quality of the certificate is guaranteed by CP/CPS of the vendors. A vendor's seal expects users to assess the corresponding certificate as higher than other vendors' certificates. However, this assessment must be done in the level of the same colors of address bars of a browser. In this meaning, seals can be considered as ε's in our framework.

These cases do not change the framework of grades. Instead, we perform risk analysis on specific topics. The result is a grade in the original framework with adjustment ε. The cost of risk analysis is limited to a specific topic, which results in reasonable cost in security analysis.

Engineering of LoA or, engineering of trust is concerned with the representation of security level and the cost of its implementation. If some information must be kept with high assurance, the cost to operate a server that stores the information can be high. It is a reasonable decision that it refuses the access by less securely operated servers which may be operated with less cost. Furthermore, if a server is operated with $N-\varepsilon$, a lower level than expected, but if another server considers that the difference ε is acceptable, then the server can accept $N-\varepsilon$ as N with its own decision. Note that in considering ε, *risk analysis* plays a more important role in security trust engineering.

Moreover, we must note that grades are given by an organization. In an organization, a security policy is given. Grades are given according to the security policy. In this meaning, security trust engineering depends on *organizations*.

Furthermore, we are concerned with the utilization of LoA in real security service. It is a fact that LoA is evaluated and maintained with high cost. If we can utilize the LoA information in real security service, especially, if LoA can

be used in access control required by a security policy of a given organization, then, we can collect the cost of LoA in the implementation of organizational security policies.

In the next section, we discuss a mechanism of matching grades among servers.

5. Grade Mathcing Mechanism

A conventional method for an SP to trust an IdP is that the SP first evaluates LoA of the IdP off-line, and if it satisfies the criteria of SP, it accepts access by the IdP. Although the cost of evaluation is not low, considering that the number of IdPs are much smaller than that of SPs, this method is acceptable.

A problem arises in solving the same problem between servers. Evaluation cost by an SP of an SP or evaluation cost by an IdP of an SP is in concern. Because the number of SPs is very large, scalability is a problem there. We analyze a grade matching mechanism as an application of trust engineering.

Considering our fundamental assumption that the criteria of grades are given based on a security policy in an organization, the grade must be given by an (upper) organization. Therefore, it is natural that there is an authority that gives a grade to a server. A grade given to a specific server is obtained by inquiring of some authority on grades. This authority has database of grades given to IdPs and SPs in a given organization. We call this authority as a "grade server."

First, we fix our grade matching policy as "a server X accepts access by a server Y if the grade of Y is higher than that of X." Second, we assume that we have a grade server in an organization, and that grade servers communicate with designated brokers. Grade servers replies only YES/NO to inquiries.

Then, functions of a grade server are illustrated in Fig. 2. and summarized as:

Database

An organization has its grade server that stores grades of servers under the organization.

Communication

1) If a server X issues the inquiry "Is the grade of the requesting party Y in the same organization higher than that of me (X)?" to the grade server, it replies Y/N as its answer.
2) If a server X issues the inquiry "Is the grade of the requesting party Z in a different organization B higher than that of me (X)?" to the grade server, it processes the request by:
   a) it calculates the grade N of X.
   b) it issues the inquiry "Is the grade of Z in the organization B higher than N?" to an appropriate broker.
   c) it returns the answer from the broker.
3) If the grade server receives an inquiry "Is the grade of W in the organization A higher than M?" from a broker, it compares the grade of W with M, and returns the answer by Y/N.

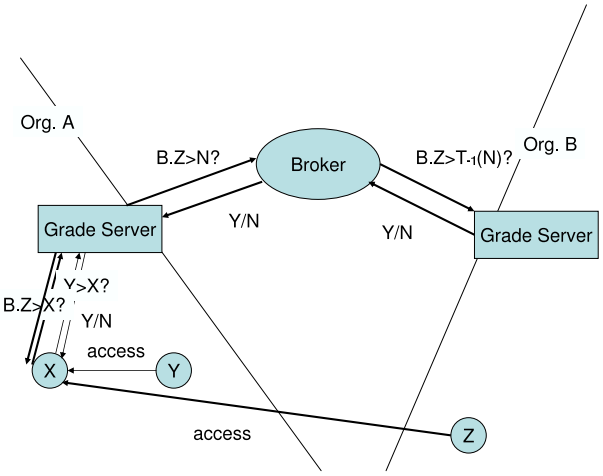

Fig. 2: Grade Server and Broker in Grade Matching

Interorganizational grade evaluation requires policy matching in an authority (PMA [23], for example), and a broker between organizations. The functions of the broker are similar to that of bridges in certificate path construction. The functions of the policy broker are summarized as follows.

Translation Table

It has a translation table T of grades among organizations.

Communication

1) If it receives the inquiry "Is the grade of Z in an organization B higher than N_{A} in the organization A?" from the grade server of A, it processes the request by:
   a) it calculates N_{B} = T(A→B, N_{A}), the corresponding grade of N_{A} in B.
   b) If N_{B} cannot be calcuated, it directly returns N (No) to A.
   c) It inquires "Is the grade of Z is higher than N_{B}?" to the grade server of B.

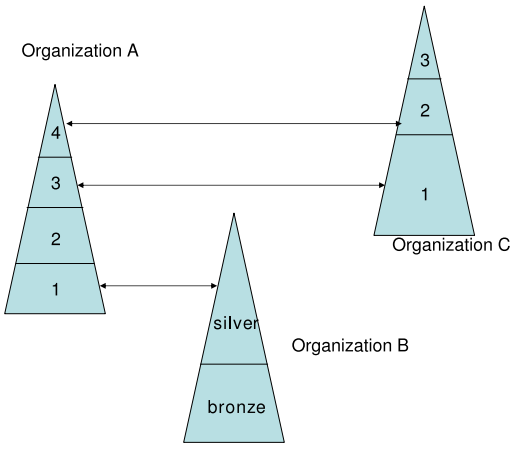

Fig. 3: An Example Grade Translation

d) It redirects the answer to the grade server of A.

The point of a broker is that it maintains the translation table of grades among participating organizations. Fig. 3 illustrates an example of grade translation. In the Figure, Organization A, B, C have four, two, three grades, respectively. Arrows correspond to translations of grades. Every grade in one organization does not have corresponding grade in its counterpart. It is a very political issue for two organizations to agree on correspondence of grades in the translation table.

6. Related Work

Although discussions of LoA[10] have been limited to ID and authentication, they are very fruitful in assuring security level in building federations. In particular, they are essential in the framework that ID information is provided to an SP by IdPs in multiple organizations via SSO.

OMB guidance[12] and NIST standard[4] are milestones in the discussion. They are also the driving force to define LoA to large federations. Today, LoA is widely discussed in many organizations, grids, federations, and inter-federations. Such federations and inter-federations include US E-authentication[12], InCommon[2], [9], SWITCH[15], and FPKIPA[1].

Major protocols for SSO have completed implementation of mechanisms of exchange of LoAs ([11] for SAML, [13] for OpenID).

Grade matching among organization is similar to path construction in certificate validation [7]. It is understood that nontrivial path construction is a burden to a general client, and delegation to a server is a reasonable solution, e.g, CVS of Hitachi and SCVP protocol [8].

There can be many applications in utilizing grades. For example, [14] applies trust to information flow analysis.

Security policies are very hard to maintain. In Japan, several templates are proposed to reduce the cost of maintenance [19], [20].

7. Conclusion

In this paper, we have discussed scenarios in which IdPs and SPs are given grades. First, we have discussed use cases of grades, in which grades of SPs play an important role together with grades of IdPs. Second, we have proposed criteria for evaluating the grades. This naturally supports the idea of security trust engineering. Finally, we have discussed grade matching mechanism as an application of security trust engineering.

This paper is the first step to the security trust engineering. Note that we assume that IdPs and SPs are operated under a security policy of their belonging organization. Security policy is essential to evaluate the criteria, or to give a grade to the servers.

References

[1] Alterman, P., “Interfederation Initiatives for Identity Authentication,” Federal Demonstration Partnership, January meeting, 2008.
[2] Alterman, P., Keltner, J., Morgan, R., “InCommon Federation: Progress, Partnerships, Opportunities,” Internet2 2007 Fall Meeting, 2007.
[3] American Institute of Certified Public Accountants and Canadian Institute of Chartered Accountants, “Trust Services Principles, Criteria and Illustrations for Security, .Availability, Processing Integrity, Confidentiality, and Privacy,” 2006.
[4] Burr, W., Dodson, W., Polk, W., “Electronic Authentication Guidelines,” NIST SP800-63, 2006.
[5] CA/Browser Forum, “Guidelines for the Issuance and Management of Extended Validation Certificates,” 2007.
[6] Chokbani, S., Ford, W., Sabett, R., Merrill, C., Wu, S., “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,” RFC 3647, 2003.
[7] Cooper, M., Dzambasow, Y., Joseph, Sl, Nicholas, R., “Internet X.509 Public Key Infrastructure: Certification Path Building,” RFC 4158, 2005.
[8] Freeman, T., Housley, R., Malpani, A.: Cooper, D., Polk, W., “Server-Based Certificate Validation Protocol,” RFC 5055, 2007.
[9] InCommon Federation, Identity Assurance Profiles Bronze and Silver, 2008 (http://www.incommonfederation.org/docs/assurance/InC_Bronze-Silver_IAP_1.0_Final.pdf).
[10] Nedanic, A., Zhang, N., Yao, L., Morrow, T., “Levels of Authentication Assurance: an Investigaction,” Proc. 3rd Int’l Symposium on Information Assurance and Security, 155–158, 2007.
[11] OASIS, Level of Assurance Authentication Context Profiles for SAML 2.0, 2009.
[12] Office of Management and Budget (U.S.), E-Authentication Guidance for Federal Agencies, M-04-04, 2003.
[13] OpenID, OpenID Provider Authentication Policy Extension 1.0, 2008.
[14] Srivana, M., Balfe, S., Paterson, K., Rohatgi, P., “Trust Management for Secure Information Flows,” Proc. 15th Computer and Communications Security, 175-187, 2008.
[15] SWITCH, Assurance Levles Definition of SWITCH pilot phase, 2006 (https://wiki.aai.switch.ch/bin/view/AAIHomeOrgs/AssuranceLevels).

[16] http://docs.oasis-open.org/security/saml/v2.0/
[17] http://tools.ietf.org/draft/draft-behera-ldap-password-policy/
[18] http://www.incommonfederation.org/
[19] http://www.nii.ac.jp/csi/sp/
[20] http://www.nisc.go.jp/active/general/kijun01.html
[21] http://www.openid.org/
[22] http://www.shibboleth.internet2.edu/
[23] http://www.tagpma.org/