$N \pm \varepsilon$: Reflecting Local Risk Assessment in LoA

Hiroyuki Sato

Information Technology Center,
The University of Tokyo, Japan
schuko@satolab.itc.u-tokyo.ac.jp

Abstract. Risk analysis is one of major phases in information security. In a modern framework of qualitative risk analysis, it is common that each of information assets, threats and vulnerability is given a small number of grades on which risk assessment of the information is based.

In this paper, first, we propose that we use results of risk assessment in access control among servers. By reusing the results, we can collect the cost of risk assessment in access control. Secondly, we propose a hybrid of conventional risk assessment with detailed analysis in giving LoAs. Based on a conventional qualitative a-small-number-of-grade system, we adapt it in the way that we can get reward for a small investment by partially adopting detailed risk analysis. This adjustment is represented as epsilons.

We propose the system of epsilon, and show our case of OTP where this adjustment is effective in assessment of authentication mechanism. Our experience shows that we can implement the adjustment by making a local comparison with a reference model.

1 Introduction

It is not long before the significance of information security is considered to be important. Modern organizational security requires information security in the organization, together with computer security and communications security.

Information security is different to computer and communications security, because analysis from the view of computer science alone is not sufficient. Problems on information security include risks, management that do not come from computer science.

Risk analysis is one of major phases in information security. In major procedures such as ISMS, we are required to analyze risk on information assets in our organization. Technologies of risk analysis come from management engineering and theory of insurance, not necessarily from computer science.

In a modern framework of qualitative risk analysis, it is common that each of information assets, threats and vulnerability is given a small number of grades on which risk assessment of the information is based. For example, NIST 800-30 [15] assigns three levels (High-Medium-Low) to threat likelihood, impact, and risk-level. Moreover, some ISMS and GMITS compliant risk assessment assigns three or four levels to assets, threat, and vulnerability. A problem is that such methodologies of risk assessment do not satisfy both precision and economics.

R. Meersman, T. Dillon, P. Herrero (Eds.): OTM 2009, Part II, LNCS 5871, pp. 833–847, 2009.

Precise assessment based on detailed approach is very expensive. Moreover, it often causes confusion in the sense that the analysis reveals (unwanted) detailed workflow of an organization. On the other hand, top-down assessment is economic, but sometimes lacks precision.

A second problem is that the result of assessment is used only in the risk control section. In other words, use scenarios of the assessment are limited to risk treatment. This is also a reason of the cost-ineffectiveness of risk assessment. If the result is used in wider scenarios and brings benefit, we can say that the cost of risk analysis is collected as the benefit in the use of the result.

In a modern framework of information security, service providers require some evaluation of IDs in accessing their assets. In this framework, the servers that are given high grades are considered to have highly evaluated assets. They require strictly managed IDs to access the assets. Some standards such as NIST 800-63 [4] are published for the criteria of this kind of assessment. Some IdPs of SAML and OpenID can issue their LoA to prove their level of ID management.

In this paper, first, we propose that we use results of risk assessment in access control among servers. By reusing the results, we can collect the cost of risk assessment in access control. Secondly, we propose a hybrid of conventional qualitative risk assessment with detailed analysis in giving LoAs. Based on a conventional a-small-number-of-grade system, we adapt it in the way that we can get reward for small security investment by partially adopting detailed risk analysis. This adjustment is represented as ε.

We propose the system of ε, and show our case of OTP (one time password) where this adjustment is effective in assessment of authentication mechanism. Our experience shows that we can implement the adjustment by making a local comparison with a reference model.

This rest of this paper is organized as: Section 2 discusses a service framework based on grades. Section 3 associates grades with risk assessment. In Section 4, we propose adjusting grades for finer control of accesses and information assets. In Section 5, we survey related work. In section 6, we give summary of this paper.

2 Service Framework Based on Grades

In [14], we have proposed a framework in that SPs and IdPs have their own grades. Grades are exchanged by servers to control access. Highly evaluated IdPs/SPs are allowed to access highly evaluated information assets. Poorly managed IdPs/SPs are only allowed to access only trivial information.

2.1 Scenario of Grades

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

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.

In the rest of this paper, we sometimes use "LoA" for a grade of IdPs for the compatibility with previous results.

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 security management of the servers.

Identification of Servers. This problem is caused 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 of 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 evaluate high CAs by denying trusting loose CAs. Thus, we can observe a kind of stratification of trust there.

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 graded 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 a 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 ($N \leq M$), 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 a less ranked object. Here, we regard "information of a rank N" as "information stored in a server of grade N," by which we can interpret grades of servers as ranks of information.

Thus, assignment of a grade to a server is reduced to identifying a 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 our scenario in Fig. 1.

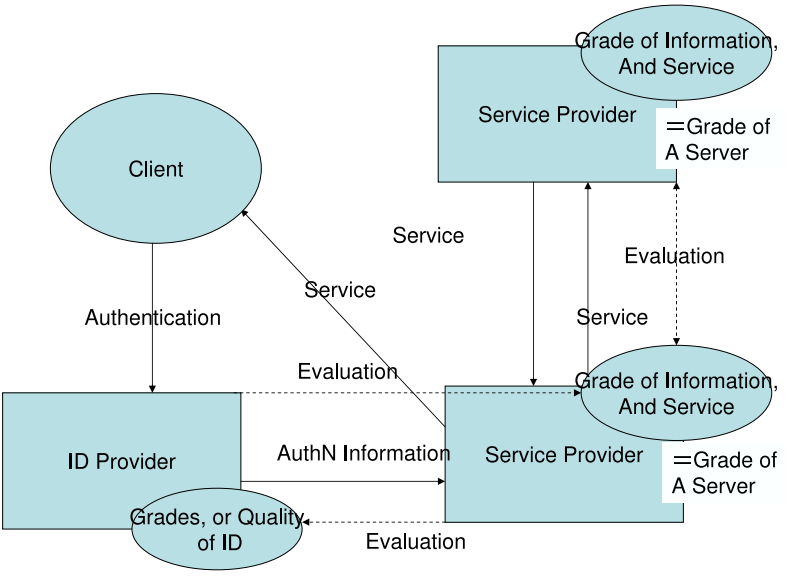

Fig. 1. IdP, SP, and Grades

3 Grades and Risk Assessment

3.1 Criteria of Grades

As for grades of IdPs, the criteria is almost the same as the NIST 800-63. The only difference is that we consider ID lifecycle (IdP-A-2) instead of initial identification in NIST 800-63.

IdP-A *Criteria on ID lifecycle management*:
1. Token.
2. ID lifecycle.

IdP-B *Criteria on Quality of Authentication*:
1. Authentication.
2. Assertion.

Note that the strength of authentication does not only depend on entropy of tokens, but also on management of ID lifecycle. These two independent criteria give flexibility in considering adjustment in Sec. 4.

As for SPs, we have two classes of evaluation: one is on the authentication of servers, and the other is the quality of information in the server.

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)

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

The criteria SP-B is closely related to the risk assessment process. Specifically, SP-B-1 must be set to the value of information assets in the risk assessment.

3.2 Security Policy in Assigning Grades

A security policy in an organization is concerned with the assignment of grades to servers.

Specifically, grades of IdPs and those of SPs are evaluated in different views. Strictly, a 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 different kinds of 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.

A grade of an IdP can be given in the conventional way. NIST 800-63 is helpful in assigning a grade to an IdP. On the other hand, a grade of an SP is given

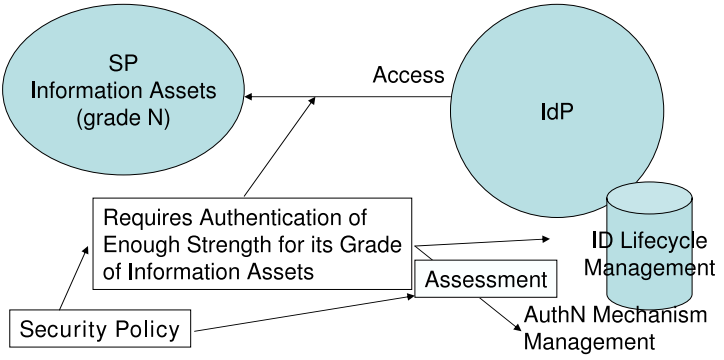

Fig. 2. Factors that affect Assignment of Grades

by an assessment of information assets in the SP. An SP requires some grade to IdPs to alleviate threat and vulnerability in access control. This is the very process of an organizational risk analysis.

Fig. 2 summarizes this discussion. We see that security policies, assessment of information assets, and access control are closely related to assignment of grades.

Another problem in assigning grades is its granularity. If we define too many levels, the process of assessment and assignment must reflect detailed analysis in the risk assessment to give a reason to fine difference between levels. On the other hand, if we define too few levels, an upgrade process of grades requires too much investment. Moreover, servers of the same grade may be operated under totally different importance.

We propose that we set the granularity of levels to the same as ranks in the risk assessment. Conventionally in qualitative approach of ISMS and GMITS, we assess risk of likelihood and impact on information assets, threat, and vulnerability in a small number of levels. The decision of the number of levels in the assessment reflects the management policy of a given organization. Therefore, we adopt this policy in the granularity. Although the classification is often based on detailed risk analysis, its details is abstracted in the qualitative assessment.

Actually, our grade assignment proceeds as:

1. First, the risk assessment is done on information assets, and a rank is given to the assets.
2. Second, an SP that has information assets of rank N is given a grade N.
3. As for IdPs, LoA is examined as the risk assessment of IdPs.
4. The rank of information assets and LoA are compared. Then the grade N is given to an IdP if an SP of a grade N accepts the IdP.

Actually, negotiations between SPs and IdPs are commonly observed. We can say that our process is a formalization of the negotiations in terms of risk assessment.

4 Adjusting Grades

4.1 Idea of Adjustment

Although it is reasonable to restrict the number of grades to a small number, there are cases that we need finer control of access control.

One of their reasons is incentive of security investment. If we consider the cost of upgrading a grade, the smaller is the better.

Example 1. Let us consider the upgrade of authentication system. NIST 800-63 assigns four levels to several authentication systems as below:

Authentication Mechanism	Level
Certificate	4
Public Key with encrypted private keys	3
One Time Password with a HW token	3
Password with entropy ≥ 14 bits	2
Password	1

If we consider the scenario in that we upgrade the authentication system from 2 to 3, we must totally change the authentication system. For example, we must newly adopt one time password system, and discard the old ID/password system. In this way, the upgrade of authentication often causes drastic change and huge investment.

If some kind of improvement of authentication is reflected as a minor upgrade of grades, we can consider it as an incentive of security investment. Actually, if we have a reference implementation of a server of a given grade N, by making a local comparison with the reference, we can easily conclude that the grade of this server is higher or lower than N.

4.2 $\pm\varepsilon$ for Representing Adjustment

To solve this problem, we propose adding ε to grades. Conventionally, grades are given as integers by a base method. We introduce a calculus on integers and ε as below:

Property 1. Let N be an integer grade given by a base method. We add ε to integers. We also consider the forms of $N \pm n \cdot \varepsilon (n > 0)$ as grades.

Property 2. We require

1. $N < N + n \cdot \varepsilon < N + 1$.
2. $N - 1 < N - \varepsilon < N$.

for each N and n.

Property 3. As for operations + and −, we require

1. $(N + (n-1)\cdot\varepsilon) + \varepsilon = N + n\cdot\varepsilon$.
2. $(N + n\cdot\varepsilon) - \varepsilon = N - \varepsilon$.
3. $(N - \varepsilon) + \varepsilon = N - \varepsilon$.

The next step is to associate criteria of IdPs with ε and $-\varepsilon$. In this association, we allow each authentication mechanism to have its own criteria of $+\varepsilon$ and $-\varepsilon$. Thus, we can evaluate $+\varepsilon$ local to a specific mechanism.

Example 2. As for authentication mechanism, we can consider different criteria of ε for ID/password authentication from that for OTP authentication. For example, the former may include the enhancement of ID lifecycle management as a source of $+\varepsilon$. The latter can include relaxing the password generation mechanism as a source of $-\varepsilon$. We concretely discuss them later in this section.

As for $+\varepsilon$, because of the restriction of $N + n\cdot\varepsilon < N + 1$ for any n, simple risk analysis suffices, because it does not affect N, the calculation of the base method. On the other hand, as for $N-\varepsilon$, we must be careful because the relaxation of IdP system could hurt the strength of the original system. Some detailed analysis local to the IdP and the requirement for $N - 1$ is indispensable.

4.3 Criteria for $+\varepsilon$

Let us consider the criteria of IdPs. The criteria are composed of ID lifecycle management (IdP-A) and strength of authentication (IdP-B). There are two directions to enhance grades:

Enhancement of ID lifecycle management: There have been proposed several methods of ID lifecycle management. All of them focus on the internal control of IDs. IDs under an appropriate internal control must be maintained under the control of master (trusted) employee database in an organization. The privileges associated with IDs must reflect the master database. Thus, the management of ID lifecycle originating from the master database matters. Policies on ID lifecycle management are written in an organizational security policy. Furthermore, the workflow of ID lifecycle management must be implemented by using a method that enables the audit process. Satisfying those conditions, ID lifecycle management is worth rewarding with $+\varepsilon$. Actually, there are already several tools of ID management in the market.

Enhancement of strength: Even if a method of authentication is fixed, there are several methods that enhance the strength.

For example, let us fix the case of ID/password authentication. Password management often causes trouble in ID management. They are often circumvented, lost, etc. causing vulnerability of authentication.

To enhance the entropy of passwords, there have been proposed some password policies. We list PWDPOLICY implemented on the OpenLDAP in Fig. 3. Note that there are at least two classes regarding strength of

Attributes	Category
pwdAttribute	–
pwdHistory	s
pwdCheckQuality	s
pwdMustChange	s
pwdMinLength	s
pwdLockout	s
pwdLockoutDuration	s
pwdMaxFailure	s
pwdReset	s
pwdMinAge	d
pwdMaxAge	d
pwdExpireWarning	–
pwdExpireWarning	–
pwdGraceAuthnLimit	–
pwdFailureCountInternal	–
pwdMustChange	–
pwdAllowUserChange	–
pwdSafeModify	–

s – category of password search space. d – category of password duration.

Fig. 3. Password Policy defined as PWDPOLICY in OpenLDAP

passwords: one is the criteria that expands of search space of possible passwords(denoted by 's' in the Fig.). The other is the criteria that restricts the duration of passwords(denoted by 'd' in the Fig.). Both are regarded as protection against a brute force attack.

Although the management of password quality is a hard task, we see that a password policy affects the quality of passwords even without detailed analysis, and that this kind of effort is worth rewarding with $+\varepsilon$.

4.4 Criteria for $-\varepsilon$

Different to $+\varepsilon$, $-\varepsilon$ needs a detailed analysis to guarantee that relaxation of IdP management does not hurt the original grades.

However, the cost of detailed risk assessment is too high to apply to every authentication system. Instead, we propose assigning a grade to an authentication mechanism by

- specifying a reference model for each grade, and
- comparing the mechanism with the reference model.

As its background, a set of reference models for each LoA must be determined. Moreover, a set of criteria for comparison must also be determined. Reference models must be determined by detailed risk assessment, by which we can also determine the criteria of comparison.

If an authentication mechanism is compared with a reference authentication model of grade N, and the comparison concludes that the weakness of the target mechanism is within allowance, then the mechanism is given a grade $N-\varepsilon$. Note that the overall comparison among every conceivable mechanism requires complex criteria. For example, in the emergence of biometrics, its comparison with conventional authentication mechanism is a complicated one (e.g. [12]). However, once the reference models are fixed, one can make a local comparison. For example, if a novel mechanism is classified as a variant of public key authentication, the comparison can be done locally in terms of characterization of secret key management, etc.

As a set of reference models, NIST 800-63 is considered to be useful. By adopting external standards, we can save cost of building reference models. Thus, we can concentrate on building the criteria of comparison, and on proving that the criteria is consistent with the external standard.

Let us review this ε system in terms of grade comparison. $N < N+n\cdot\varepsilon < N+1$ in Property 2 indicates that the local improvements (ε) of a given authentication system does not upgrade the original grade: $N + n \cdot \varepsilon < N + 1$. Moreover, $-\varepsilon$ must always be compared with the original grade N, and the result is always $-\varepsilon$ from N: $(N + n \cdot \varepsilon) - \varepsilon = N - \varepsilon$, and $(N - \varepsilon) + \varepsilon = N - \varepsilon$ (Property 3).

Based on this adjustment, an SP can determine the LoA that the SP requires. First, let us assume that an SP requires ID/passwords of grade 2 in authentication.

- If an SP requires a slightly stronger authentication than ID/password authentication, it can raise the requirement to $2 + \varepsilon$, instead of 3. The IdP can raise the quality of ID lifecycle management to match the requirement instead of introducing the totally new system, saving total cost of security enhancement.
- If an SP decides discarding highly graded information assets, and therefore concludes that a slightly looser ID/passwords in the authentication is enough, it can lower the requirement to $2 - \varepsilon$. It is the *responsibility* of the SP that accepts the threat and the vulnerability of $-\varepsilon$.

In this way, the $\pm\varepsilon$ system brings reasonable rewards in IdP management, and flexibility in authentication management.

4.5 Example Scenarios of Adjustment

Usually, adjustment of grades is considered on IdPs. We list two example scenarios in that adjustment of grades is effective.

Note that we also consider grades of SPs. If an appropriate grade criteria system such as NIST 800-63 become common for SPs, a similar system is also possible.

A. Enforcing ID Lifecycle Management

It is an important knowhow that an appropriate ID lifecycle management enhances the quality of ID/password system.

For example, an organization can determine the criteria of $+\varepsilon$ in terms of ID lifecycle management as:

1. a security policy is established,
2. ID lifecycle is under management of a master employee database, and
3. the management is under appropriate control.

An organization can give $+\varepsilon$ if an IdP is operated well in terms of the three criteria.

B. Enforcing Password Policies

Let us consider authentication by using ID/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 [19]. It is reasonable to upgrade the LoA of LDAP password authentication to $2 + \varepsilon$, if the LDAP server adopts an appropriate password policy to control the quality of passwords.

For example, an organization can determine the criteria of $+\varepsilon$ in terms of password entropy as:

1. At least one of criteria regarding the password search space must be specified in the password policy.
2. At least one of criteria regarding the duration of passwords must be specified in the password policy.

An organization can give $+\varepsilon$ if an LDAP server as a backend of an IdP adopts the password policy with the above two criteria.

C. Building and Analyzing a SecureID-Like OTP System

In universities, there is a set of information assets of every grade of significance. Several levels of access control methods are necessary to manage the variety of information assets.

However, providing every kind of authentication mechanism is not realistic because of cost of deployment and the complexity of management. A natural solution is that the university offers an authentication mechanism of the highest level, and that authentication mechanisms of lower levels must be (1) left alone, if the level matches the required level of access control, and (2) replaced with the mechanism of the highest level, if an enhancement of level is required.

For example, the University of Tokyo has established CAs for smart cards and mobile phones [22]. However, it does not provide mechanisms for lower grades. Therefore, if one adopts ID/password authentication, and needs an enhancement of authentication levels, one must adopt smartcard authentication. For smartcard authentication, one must carry a smartcard and a specific card reader with him, one must be patient with the inconvenience.

Therefore, we have deployed an OTP (one time password)-like authentication mechanism with less inconvenience. The point of this mechanism is our "password server." The password server is implemented as a front end of an LDAP server. The authentication proceeds as:

1. A user accesses the password server by using certificate authentication. Typically, a mobile phone is used as its device.
2. The password server replies with a newly generated password to the user. The password is also set to the backend LDAP server with *short* expiration.
3. The user then accesses the target SP. The ID/passwords of the SP are provided by the backend LDAP server. The password given in 1. is used for the authentication.

Fig. 4 summarizes the architecture of our system. Note that the architecture does not depend on the memorability of passwords. Instead, the password is given by the password server each time of authentication. Therefore, we can consider this architecture as one of OTP , but not as an ID/password system.

What must be proved is that the LoA of this system is almost the same as that of a reference model of OTP.

For example, let us assume that OTP is given grade 3 in an organization. Consider a case where an IdP authenticates its ID with OTP-like mechanism, but its LoA is somewhat less than OTP. Conventionally, grade 2 is given in this case.

However, if some risk analysis concludes that the OTP-like method has almost the same LoA as OTP, and the risk can be accepted under reasonable risk, then the method can be graded as $3 - \varepsilon$.

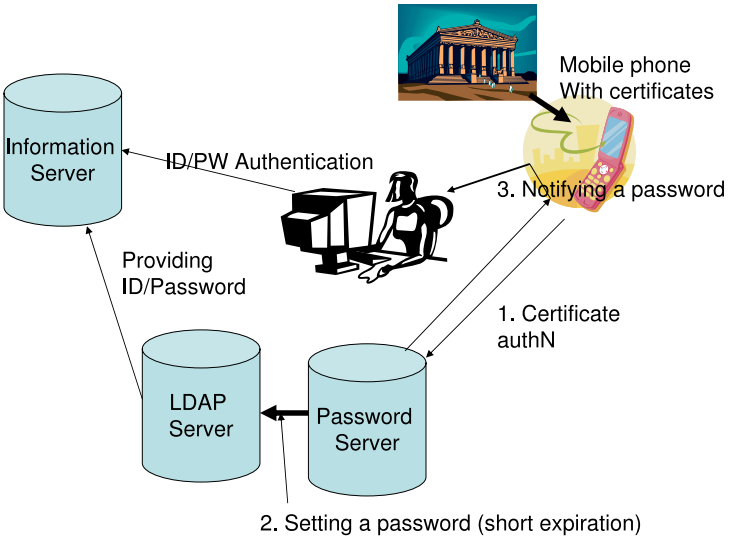

Fig. 4. Implementation of OTP-like system using Mobile Phones and LDAP server

Actually, the high rank security of SecureID of RSA (`http://www.rsa.com/node.aspx?id=1156`) is guaranteed by the fact that a hardware token is given to a principal, and a password supplied by the token expires very soon.

It is easy to write a program that supplies a passphrase in limited duration. If we use some strong authentication to get the passphrase, the only difference to SecureID (reference OTP) is the duration of passphrase and the algorithm of passphrase generation. If a finer risk analysis can evaluate this downgrade to ε, and we determine to accept this ε, a software OTP can be used as having almost the same strength as the reference OTP.

Let us analyze our OTP-like system in terms of OTP. First, let the criteria of comparison be given as:

- Security in token management and delivering passwords,
- Complexity of password generation, and
- Duration of passwords.

Note that this criteria is given by comparing with SecureID of RSA.

As for the security of token management and delivering passwords, we see that a hardware token is replaced with a mobile phone. Because the mobile phone is provided with the certificates of individuals in our system, we see that the security is of the highest level.

As for the complexity of password generation, because SecureID is operated under "security through obscurity," we cannot make comparison. This may be the source of $-\varepsilon$. However, if a password is randomly generated with a secure seed, we think that the "security through obscurity" is also satisfied.

As for the duration of passwords, we see that the duration of passwords of SecureID is 30-60 seconds. Considering the brute force attack, the possibility of false match rate must be equally low. Let n be the number of conceivable attacks in a given duration, and p be $1/(\text{key search space})$. Then, because the possibility of successful attacks under this condition is $1-(1-p)^n \sim np$, we have to compare $n_{SecureID} \cdot p_{SecureID}$ and $n_{ours} \cdot p_{ours}$. Therefore,

$$\frac{n_{ours} \cdot p_{ours}}{n_{SecureID} \cdot p_{SecureID}} = \frac{n_{ours}}{n_{SecureID}} \cdot \frac{p_{ours}}{p_{SecureID}}.$$

Because n represents the duration of passwords, if we assume the same key search space as SecureID, that is, $p_{ours}/p_{SecureID} = 1$, and the passphrase of SecureID expires in 60 seconds, then we approximate the above formula as

$$\frac{\text{Duration in seconds}_{ours}}{60,}$$

considering SecureID's duration.

If we set the expiration of passwords to two minutes, then the system is two times weaker than SecureID. To compensate this weakness, we can give a longer password with an extended set of characters, guaranteeing $p_{ours}/p_{SecureID} > 1$.

If the organization (university) decides to accept this weakness, and adopts the convenience, then the organization sets the grade of our OTP as $3 - \varepsilon$.

To be noted is that we make a local comparison with a reference model of the given grade. The cost of local comparison is reasonable.

5 Related Work

Risk assessment is one of major phases of risk analysis. Conventionally, NIST 800-30 [15], ISMS (ISO 27000 series) and GMITS (ISO/IEC TR 13335) have been proposed as qualitative risk assessment methods.

Although discussions of LoA [9] 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 [11] 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 [11], InCommon [2, 8], SWITCH [17], and FPKIPA [1].

Furthermore, major protocols for SSO have completed implementation of mechanisms of exchange of LoAs ([10] for SAML, [13] for OpenID).

There can be many applications in utilizing grades. For example, [16] 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 [20, 21], but not yet successful.

The rationale of LoA is refined every time when new technologies emerge. In the emergence of biometrics, there have been made intensive comparisons with conventional methods [12]. [7] tries formalizing the ranking of authentication methods by using filtering and entropy.

There are some studies on strength of authentication to specific methods. [18] reports the experience on qualities of passwords.

6 Concluding Remarks

In this paper, we have proposed the access control based on grades given to SPs and IdPs. This framework subsumes conventional discussion on LoA. Grades are naturally associated with risk assessment in the organization.

Moreover, we have proposed adjusting grades for finer control of accesses and information assets. $N \pm \varepsilon$ is introduced, and $+\varepsilon$ is evaluated as a reward to keep the quality, and $-\varepsilon$ is given in the local comparison with a reference model.

An organization can collect the security investment by utilizing grades for access control. Moreover, $\pm\varepsilon$ can be used to represent small investment to enhance security. In other words, we can use grades as a reward to any security investment from small to large.

Controlling the quality of assigning ε is a problem. Rewarding small investment requires finer control and assessment of management/operation of servers. How to control the cost of assessing the finer points is our future work.

References

1. Alterman, P.: Interfederation Initiatives for Identity Authentication. In: Federal Demonstration Partnership, January meeting (2008)
2. Alterman, P., Keltner, J., Morgan, R.: InCommon Federation: Progress. Partnerships, Opportunities. In: 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. Helkala, K., Snekkenes, E.: Formalizing the ranking of authentication products. Information Management and Computer Security 17(1), 30–43 (2009)
8. InCommon Federation: Identity Assurance Profiles Bronze and Silver (2008), http://www.incommonfederation.org/docs/assurance/InC_Bronze-Silver_IAP_1.0_Final.pdf
9. Nedanic, A., Zhang, N., Yao, L., Morrow, T.: Levels of Authentication Assurance: an Investigation. In: Proc. 3rd Int'l Symposium on Information Assurance and Security, pp. 155–158 (2007)
10. OASIS: Level of Assurance Authentication Context Profiles for SAML 2.0 (2009)
11. Office of Management and Budget (U.S.): E-Authentication Guidance for Federal Agencies. M-04-04 (2003)
12. O'Gorman: Comparing passwords, Tokens, and Biometric for User Authentication. Proceedings of IEEE 91(12), 2019–2040 (2003)
13. OpenID: OpenID Provider Authentication Policy Extension 1.0 (2008)
14. Sato, H.: A Service Framework based on Grades of IdPs and SPs. In: Proc. Securiy and Management 2009, pp. 379–385 (2009)
15. Stoneburner, G., Goguen, A., Feringa, A.: Risk Management Guide for Information Technology Systems, NIST 800-30 (2002)
16. Srivana, M., Balfe, S., Paterson, K., Rohatgi, P.: Trust Management for Secure Information Flows. In: Proc. 15th Computer and Communications Security, pp. 175–187 (2008)
17. SWITCH: Assurance Levels Definition of SWITCH pilot phase (2006), https://wiki.aai.switch.ch/bin/view/AAIHomeOrgs/AssuranceLevels
18. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password Memorability and Security: Empirical Results. IEEE Security and Privacy, 25–31 (September/October 2004)
19. http://tools.ietf.org/draft/draft-behera-ldap-password-policy/
20. http://www.nii.ac.jp/csi/sp/
21. http://www.nisc.go.jp/active/general/kijun01.html
22. http://www.pki.itc.u-tokyo.ac.jp/