L-038

Infrastructure model and protocol for the assurance of the authentication data exchange format

Ahmed Tallat
Tokyo Denki University

Hiroshi Yasuda
Tokyo Denki University

Kilho Shin
University of Hyogo

Abstract— conventionally, service providers have to manage their own authentication systems individually and independently without interoperation among them. Lack of the interoperability causes certain serious problems. In this paper, we clarify the requirements for the interoperability, and propose a model, where three independent players, that is, service provider, identity provider and authentication agent, cooperate and communicate with one another.

1. INTRODUCTION

The necessity of authentication becomes apparent in that threats are increased not only in numbers but also in complexity. Despite of current authentication frameworks, there are still multiple serious problems resulting from lack of interoperability; (a) unnecessary big investments made for authentication systems run by SPs independently and individually, (b) repetition of user registration and authentication, and (c) the risk of identity leakage as services increased. With the interoperability in authentication systems, service providers are relieved of the burden to authenticate users independently and individually, and users do not have register their identities per services so as to increase users convenience and security of identity. In this paper, we propose authentication infrastructure based on the requirements necessary to make interoperability possible in open environments, in which, unlike current authentication frameworks (e.g. SAML, OpenID, BioAPI, PKI etc) that confine their scopes on internet, biometrics, and public key respectively, authentication results can be shared among entities without restrictions.

2. Challenges with current authentication frameworks

Analyzing of the current frameworks, we concluded that the problems in section1 caused by the challenges of frameworks lack of authentication interoperability. Now the main reason of insufficiency interoperability is that we do not have authentication infrastructure supporting multiple authentication, whose authenticated data by standardized of authentication data exchanging format are recognized in open environment like PKI that is used in variety of media, the Internet, diverse operating systems and smartcard etc. In order to meet the need of establishing interoperability in the open environment, we clarified following challenges with current authentication frameworks.

1. Lack of trust mechanism of sharing authentication results in open environment. Taking advantages of SSO (Single Sign On) platform, SAML [1] and OpenID [4] aim at achieving interoperability by standardizing authentication data called “assertion” among SPs. But entities creating interoperability establish contract based trust-relation to run the protocol, which is out of scope of the “assertion”.

2. Insufficient separation of players in independency. Conventionally, SPs independently run their business by registering, authenticating and providing service, which cause security, convenience and cost problems. Next, known as the solutions for these problems, PKI, SAML, OpenID, BioAPI etc are created, in which independency of players start emerging. For example, in PKI[3] SPs entrust registration to CA, in SAML assertions created by IdP is accepted SPs. In BioAPI[2] authentication results created in a card are standardized and recognized by other machines. Yet, independency of players for registration, authentication and provision of services are not clarified enough to meet the requirements of establishing authentication infrastructure in these frameworks.

Independency of players is beneficial from security and economic aspects; in that accessibility to users` identity information is limited by IdP only and SPs are entitled to decide whether users are qualified for claimed resources by entrusting registration and authentication to IdP and AA respectively. Thus SP is relieved of possessing authentication system and securing users` identity data.

3. Limited scope of deployment with specific authentication methods. For authentication, we need to use variety of media, the Internet, diverse operating systems and smartcard etc in the open environment. However, the approaches stated above that aimed at achieving interoperability among diverse SPs, are confined with functions that apply SSO, Biometrics and public key only.

3. OUR MODEL FOR AUTHENTICATION INFRASTRUCTURE

In response to the challenges of current frameworks (including the problems in introduction) and recognizing the deep need for authentication infrastructure providing interoperability in the open environment, in this paper, we clarify the requirements for the authentication infrastructure, and propose a model of it, where independent players representing identity provider (IdP), authentication agent (AA) and service provider (SP) taking care registration, authentication, and provision of service by exchanging standardized messages among them for interoperability.

3.1. Protocol

To solve the problems stated above, our protocol consists independent players of IdP, AA and SP communicating to each other in registration, authentication and authorization phase respectively. IdP maintains evidence of user registrations, whereas AA provides unified interface to authenticate registered users by means of token, which can be private key, password, smartcard, fingerprint

or combination of them etc. On the other hand, SP as being an owner of services has no control over both IdP and AA, and provides users with conditional access to its resources, by taking advantage of both registration and authentication processes performed by IdP and AA respectively.

The main part of this authentication infrastructure is AA providing interface with the capability of multiple authenticating functions so as to serve a variety of diverse SPs` interests. To meet the challenges of current frameworks mentioned in Section 2, an independent enterprise runs the AA and bares a huge financial investment for it to relieve the duplication investments made by SPs to independently run authentication systems. Visualization of AA can be ATM in convenient store. Thus it is preferable that AA should be publicly distributed independent entity, and it performs authentication procedures on behalf of variety of SPs.

- **Registration phase**;

In this phase, users pick up IdP they trust to register themselves, and the IdP verifies claimed identity based on official documents (passport, IDcard etc) by means of its policy. As result of registration, Token and Reference data are created for subsequent authentications (typically private & public key, fingerprint & templates etc).

- Authentication phase

By interface provided by AA, users create identity proof from the Token activated by IdP, and AA either sends the identity proof to the IdP for verification, or authenticates the users by reference sent by the IdP. As a result, Endorsement is created containing necessary information for SPs to evaluate IdP and AA in terms of security levels. Furthermore, AA sings the endorsement and sends it to authenticated users with certificate used by SPs for evaluation of trust level.

- Authorization phase

Receiving Endorsement and certificate from AA, users try to access SPs access control services, and SPs, in order to provides users with their resources, verify (a)whether security level of endorsement meet the need of SPs requirements, (b) Integrity, confidentiality and validity of both Endorsement and Certificate (c) whether IdP and AA are trustworthy.

3.2. Requirements for interoperability

Receiving authenticated data created by AA, SP requires not only sufficient information from it but also trustworthiness of its issuer. Thus to meet the challenges of current frameworks caused by insufficiency of interoperability in open environment, authentication infrastructure proposed in this paper should meet the following requirements.

- **Security level of Endorsement must meet the need of SPs.**

Our model consists of registration, authentication and authorization phases, in which IdP, AA and SP exchange messages independently. Such an independency of players makes it necessary for SPs to be provided sufficient information for evaluation of security levels of IdP and AA, by means of risk assessments determined by potential damages caused by an attack—be it intentional or accidental. To meet the requirement, we clarified both threats and counter-measures in order to determine both registration and authentication requirements, and as a whole they constitute security levels [5] by retrieving information necessary for SPs to evaluate the security level of endorsement.

- **Common format of Authenticated data**

Before the evaluation of endorsement, first it should of course be recognizable by diverse SPs, regardless of the devices and authentication protocol implemented for authenticating users; Endorsement should be expressed in a "standardized" language among diverse SPs.

- **Trust level of the entities issuing Endorsement**

Common format description of endorsement alone cannot make the assurance of authentication data exchange possible in the open environment, where an independent entity should also be able to accept authentication data from an unknown entity. Since both registration and authentication are made by IdP and AA respectively, which are not necessarily known to SPs, thus SPs should have reasons to believe that IdPs and AAs are trustworthy. To meet the requirement, our model deploy auditing scheme taking advantage of a third trusted party (TTP), which not only guarantees the binding between AA and public key corresponding to AA`s private key, but also audits the trust level of AA/IdP in terms of the duty to be performed, obligation to be fulfilled and liability to be promised.

1st and 3rd requirements solve the challenge 1. 2nd requirement is the inevitable consequence of the interoperability among independent entities.

To solve the challenge 2 we propose a model, where IdP, AA and SP are defined as independent players taking care registration, authentication and authorization of user by standardized messages exchanged among them. To solve the challenge 3 we introduced authentication infrastructure to able Endorsement to be shared in SPs without restriction. The detailed explanation is stated in section 3.

4. CONCLUSION AND FUTURE WORK

We indicated problems resulting from lack of interoperability among a variety of SPs and proposed authentication infrastructure model aiming at achieving interoperability in open environment, which is also beneficial security, convenience and economic perspective. Next we will put the model into practice by simulation experiment to verify feasibility, acceptability and scalability of the protocol.

[1] OASIS, Security Assertion Markup Language (SAML) V2.0, 2007

[2] The BioAPI Consortium, BioAPI Speci_cation Version 1.1, 2001.

[3] "Internet X.509 Public Key Infrastructure:Certificate.Management Protocols", RFC 2510.

[4] OpenID Authentication2.0 Final.

[5] NIST, Electronic Authentication Guideline, April.2006.