Research on Network Identity Management Systems Model

CHEN Bing[1,2,a]*, ZOU Xiang[1], TAN Chengxiang[2]

[1]The 3rd research institute of ministry of public security (key laboratory of information network security, Ministry of Public Security), Shanghai, China

[2]Dept. of computer engineering of Tongji University, Shanghai, China

[a*]bing_chen2000@163.com

Keywords: Network identity; Identity management; Systems model; Massive data

Abstract. With the rapid development of network, network identity management is becoming more and more important. Network identity in cyberspace associated in reality has been one significant and urgent task as online life becomes real. So this paper gives a new network identity management systems model based on the present model, including a two-party identity management model, a three-party identity management model, and a user-centric five-party identity management model. The new model made by new five parties can realize the network identity management under huge amounts of data and for all kinds of network identities, such as personal, organization, software, service, etc., and the new network identity management model helps to identity management in cyberspace.

Introduction

As online life becomes more and more engrossing in our realism, network identity management will be more and more important and focused on. Now, information technology has been making an explosive evolution, and there will be large security threats hidden in Internet. And it has been faced with great challenge on security and efficient management for network identity management in the process of people's network activities. So it is necessary to research network identity management systems model to achieve efficient security management of all kinds of entity identities in networks, especially about individual's online activities.

Challenges on network identity management system mainly focus on how to realize the system not only more efficient and safer but also protection personal privacy of citizens, for personal, organization, software, service, etc. Thus, the paper discusses a new network identity management systems model based on the present model, including a two-party identity management model, a three-party identity management model, and a user-centric five-party identity management model[1-5].

General Identity Management Systems Model

General identity management model includes application-centric model and user-centric model.

The application-centric identity management system means that identity services and policies are designed to satisfy requirements for identity providers and relying parties and optimized for the requirements of applications. There is an identity provider and a relying party in the application-centric identity management system. When an identity service is provided for the user, the identity exchange usually takes place between these two entities. The identity and access management technologies have focused mainly on the authentication of end users for federated access to applications and services. Therefore, the security requirement is limited to the perimeter of its application domains.

The user-centric identity management is mainly focused on end users and optimized for the requirement of those end users. It means that the main objective of an identity management system is to provide convenient and comprehensive identity services for users. The main feature is to give the

user full control over his identity. When a user's identity information is disseminated, it must pass through the user explicitly to give the user a chance to enforce some personal policy if necessary. In the user-centric identity management system, a client program has to be installed in the user's computing environment.

A Two-party Identity Management Model

A two-party identity management model is the basic query-response process common to most structured information exchange shown in Figure 1. The most basic form of message exchange involves two parties using an agreed-upon protocol and information model.

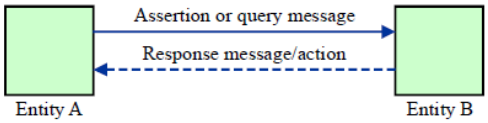

Figure 1. A two-party identity management model.

The parties that participate in this process may be any kind of entity. An entity can be a physical person, an organization, an active or passive thing, a device, a software application, a service, etc., or a group of these individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc. They can be any physical or virtual object, such as network equipment, software, terminal devices, sensors, actively tagged physical objects (e.g., using RFIDs or optical codes), passively tagged objects. Network devices, for instance, may be treated as entities subject to special identity management capabilities on behalf of end users, providers, and governmental authorities. In the context of digital rights management, the entity may be intellectual property or copyright protected material, such as multimedia or IPTV content. A special type of entity is the group. The group's identity is the intersection of the identities (common attributes) of the group members.

A Three-party Identity Management Model

A three-party identity management model means: where the relying party who originally receives the claim is not the identity service provider, and as illustrated in Figure 2.

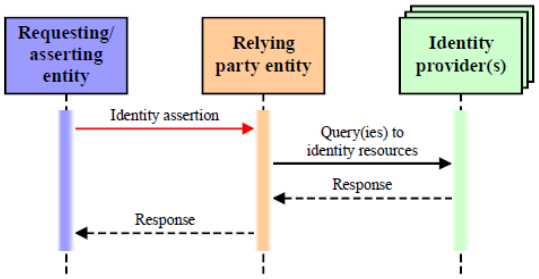

Figure 2. A three-party identity management model.

The function of being an identity service provider is separate and distinct from the relying party; the relying party evaluates the responses from the identity service provider(s) and decides whether there is a sufficient level of entity authentication assurance. The primary function of an identity service provider is to manage the creation, update, verification, suspension, and deletion of identity information.

A User-centric Five-party Identity Management Model

A user-centric five-party identity management model is another identity management model that provides the requesting party with more control of the identity relationships, as depicted in Figure 3.

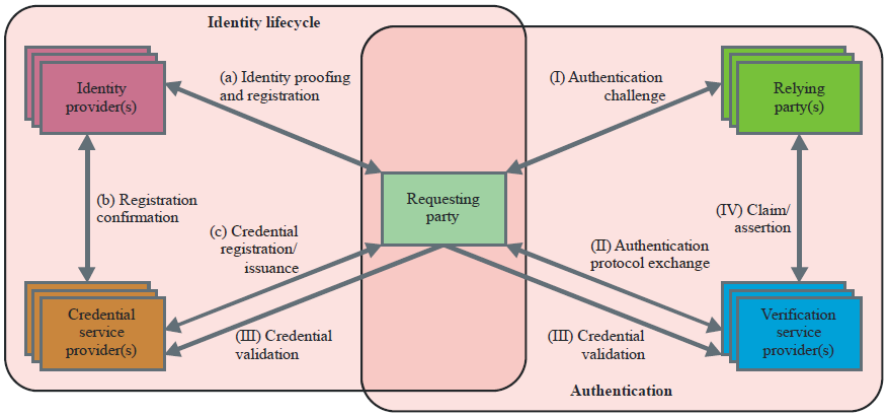

Figure 3. A user-centric five-party identity management model.

The model shows an structure where specialized roles and capabilities for identity management are provided by different service providers. All queries/responses are directed through the requesting party. For the purposes of these kinds of model, the entities are described as follows:

1) Identity provider: An entity that maintains and manages, and may create, trusted identity information of other entities and offers identity-based services. This entity responsible for assigning and issuing attributes – also described as enrolment – is responsible for the lifecycle management of the identity which includes proofing, registration and maintenance of the identity, including revocation.

2) Credential service provider: The entity providing capabilities related to the issuance of credentials and tokens.

3) Verification service provider: The entity providing capabilities of assessing identity information and classifying its validity.

4) Relying party: An entity that relies on an identity representation or claim by a requesting/asserting an entity within some request context.

A New Five-party Identity Management Model

A new five-party identity management model is another identity management model that provides users, identity relying party, identity providing party, identity basic database, and supervising party with more control of the identity relationships, as shown in Figure 4.

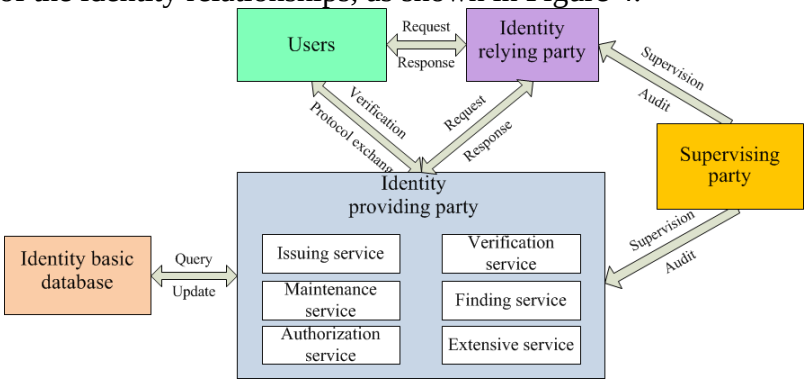

Figure 4. A new five-party identity management model.

The model include the all kinds of privilege, such as users, supervising party, and so on. It can deals with all kinds of circumstance under huge amounts of data and for all kinds of network identities, such as personal, organization, software, service, etc. in cyberspace. The entities are described as follows:

1) Users means entities of needing to be verification, and the entity of a transaction may be an individual or a non-person entity (NPE). An individual is a person engaged in an online transaction Individuals are the first priority of the Strategy. An NPE may also require authentication. NPEs can be organizations, hardware, networks, software, or services and are treated much like individuals. NPEs may engage in or support a transaction

2) An identity relying party (IRP) makes transaction decisions based upon its receipt, validation, and acceptance of a entity's authenticated credentials and attributes, a relying party selects and trusts the identity and attribute providers of their choice, based on risk and functional requirements. Relying parties are not required to integrate with all permutations of credential types and identity media. Rather, they can trust an identity provider's assertion of a valid subject credential, as appropriate. Relying parties can choose the strength of the authentication and attributes required to access their services.

3) An identity provider (IDP) is responsible for establishing, maintaining, and securing the network identity associated with that entity. These processes include revoking, suspending, and restoring the entity's network identity if necessary.

4) Identity basic database provides the basic identity information for IDP, including the nation population database, legal person database, and ICP database, etc. basic information database.

5) A supervising party is the national authoritative management organization, in charge of designating network identity management strategic plan, issuing directive opinion and policy laws and regulations of network identity management, supervising IRP and IDP, and auditing them.

Conclusion

The paper presents research on several network identity management systems models, and gives a new network identity management systems model based on the present conventional model, including a two-party identity management model, a three-party identity management model, and a user-centric five-party identity management model. The new five-party model made by new five parties can realize the network identity management under huge amounts of data and for all kinds of network identities, such as personal, organization, software, service, etc., and the new network identity management model helps to identity management in cyberspace in the future.

Acknowledgment

The research work was sponsored by the National High Technology Research and Development Program of China 2012AA01A404 and the Key Program Project of Ministry of Public Security 201301ZDYJ023.

References

[1] ITU-T X.1250, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY: Cyberspace security – Identity management, Baseline capabilities for enhanced global identity management and interoperability, 2009.

[2] ITU-T X.1253, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY: Cyberspace security – Identity management, Security guidelines for identity management systems, 2011.

[3] Ensia European Network and Information Security Agency. A Roadmap for a pan-European eIDM Framework by 2010, 2006.

[4] Ensia European Network and Information Security Agency. Report on the state of pan-European eIDM initiatives, 2009.

[5]US White House. National Strategy for Trusted Identities in Cyberspace, 2011.