Establishing Persistent Identity using the Handle System

Sam X. Sun
Corporation for National Research Initiatives
1895 Preston White Dr. Suite 100
Reston, VA 20191
ssun@cnri.reston.va.us

ABSTRACT

In this paper, we propose that identity reference used over distributed communication should be defined independent from any attributes and/or the public keys associated with the underlying subject. This allows the identity reference to be persistent over changes made to the attributes and/or the public keys. We further suggest to separate the trust establishment over distributed communication into three categories: the transport trustworthy, the administrative trustworthy, and the content credential, which we believe will simplify trust and trust management. These lead to our proposal to use handles registered under the Handle System [1] as persistent identity reference for Internet communication, and utilize the handle system security service to help trust management over the Internet.

Keywords

Handle and the Handle System; Persistent Identity; Trust and Trust Management; Public Key Infrastructure (PKI)

1. INTRODUCTION

Internet needs identity, which has been the subject for any Public Key Infrastructure (PKI). Due to the lack of secured name-attribute binding service over the Internet, traditional PKI implementations struggle in providing trustworthy binding between the public key and its underlying identity. They are forced in one way or another to take care of transport security along with content credential at the same time. The results are identity reference defined either in terms of cumbersome key-attribute bundle issued by legally non-liable third party (e.g. certificate authority), or using the public key itself that aren't easy to use and won't persist over time.

The Handle System [1], developed by CNRI (http://www.cnri.reston.va.us), provides a secured global name service for digital objects over the Internet. Using the Handle System, each digital object may be given a handle, i.e. a name that can be associated with a set of attributes describing the object, including its location, ownership, and permissions or rights that applies to the underlying object. The handle system protocol and its service framework provide a secured name-attribute binding service over distributed communication. Using the handle system protocol, clients may request handle server to authenticate its response using server's digital signature during handle resolution. Client may also authenticate itself as the owner of the handle (i.e., the handle administrator) to make changes to handle data. Further, the handle system data model allows credential reference to be defined for each handle value (i.e. the handle attribute) so that the credentials of the handle value may be further validated.

In this paper, we suggests that the Handle System may be used to establish persistent identity over the Internet. Using handles registered under the Handle System, security identities may be defined in a simple straightforward fashion, yet persistent over its attributes changes. Taking advantage of the secured name-attribute binding service from the Handle System, this new approach separates transport security from the content credential, and allows peer-to-peer trust to be established via mutual authorization agency directly, without reliance on non-liable third party (e.g. certificate authority). We believe that security identities defined in this way can be used in a more flexible fashion that maps closer to many real world transactions.

2. Identity in Distributed Communication

Any trusted communication requires that the parties involved be able to present their identity. According to Webster dictionary, identity is "collective aspect of the set of characteristics by which a thing is recognizable or known". As the definition of identity implies, a pure name or identifier by itself isn't enough to represent an identity. A name or identifier is useful as a reference to an identity, but it is the attribute of that name or identifier determines its trustworthy. In order for us to make the decision or to "trust" the name, other information about the name has to be available. On the other hand, we are used to identity defined in an abstract fashion, either via a name that we can remember of, or as a piece of document (e.g., a driver's license) that can be examined against. What is carried alone the name or the document is a collection of attributes including the role, the status, and the authorization information that uniquely identifies the subject.

Difference PKI defines their identity representations differently. The way identities are represented will not only have impact on how anyone establish such identity, but also governs the procedures and/or policies that will be used to manage such identity. Traditional Public Key Infrastructure, such as the one specified by IETF PKIX working group, defines the identity, or its reference, as the X.509 certificate [2]. An X.509 certificate is essentially an archive of the distinguished name, a public key used, and the set of attributes associated with the underlying subject. The archive is further signed by a third party, the Certificate Authority (CA) to "assure" its trustworthy. Besides many arguments on how much trust this binding can be expected [3], the identity established in this fashion will not persist because any of the attributes or the public key associated with the subject may change over time. This prevents prolonged identity establishment over subsequent communication, and the complicated binding procedure makes the identity hard to

establish or manage. An even bigger issue is how to "recycle" issued certificates that are no longer valid.

All these analyses suggest that it is essential to separate identity reference from its attributes to allow any persistence of the identity reference. Separating the identity reference from its attribute also avoid revocation issues that have to be dealt by X.509 certificates, and allows trust validation directly via its authorization agency. However, this does require a secured global name service, like the Handle System, that can guarantee the binding between the name and its attributes over distributed communication. The secured global name service will act as the certificate authority that assures that attributes of the identity reference are securely transported from one-end of the communication to the other. Using this approach, identity reference can be defined as a mnemonic name that is independent from any other attributes of the underlying subject, including its public keys. The abstraction of identity reference into a mnemonic name allows the identity reference to persist when any of the attributes or the public keys associated to the subject has to change. For example, the identity reference may remain valid even after the key used to establish the trust relationship get expired or replaced.

3. Trust and Trust Management in Distributed Communication

One important question on establishing any private communication over the distributed computing environment is how to define the trust between the parties involved. A closer look into any trusted communication channel suggests that trust establishment may be divided into three categories. These are:

- Transport Trustworthy, that is, the name/attribute and their binding is delivered without being tempered.
- Administrative Trustworthy, that is, any attribute is indeed issued from the attribute holder.
- Attribute Credential, that is, the attribute value is trustworthy. In other words, the subject didn't lie and is speaking the truth.

Traditional PKI defines its identity reference using public key certificate (e.g., X.509 certificate). Trust establishment is carried out by verifying the certificate against its Certificate Authority (CA). CA in PKIX is responsible not only for transport trustworthy in terms of name/attribute binding, but also for attribute credential. However, in practice, hardly any CA will stand behind or accept legal liability on attribute credential, making certificate apprehensive for trust establishment in critical applications. The combination of name, key, and attributes makes the certificate very un-persistent by nature. The PKIX approach by making the identity reference as a collection of potentially any attribute makes processing of the certificate very difficult to implement, and hard to manage. Many argues that the reliance on third party CA has made the process inconvenient in practice and costly to deploy. And issue the certificate revocation has never been adequately resolved. The fact is, binding every attribute together as the identity reference doesn't really simplify the trust management process, instead, it makes it more complicated in practice.

Our analysis shows that the way identity reference is defined has a direct impact on trust establishment and its subsequent management. We argue that separating the transport trustworthy from the content credential will potentially remove the reliance on Certificate Authority as used by existing PKIs and will eventually make the trust management more flexible and straightforward. A secured global name service, such as the Handle System, can take care of the transport trustworthy during trust establishment process, and will separate the identity reference from its attributes. This will not only make the identity reference persistent over its attribute change, but also allow more flexible use of the identity under different situations. For example, a user may sign a document bearing only those attributes that are related to the signed document. It also allows publishers to distribute digital contents with the envelope with specific consumer in mind.

4. Conclusion and Work in Progress

In this draft, we propose that identity reference used in any trusted communication should be defined independent from any attributes or the public keys associated with the underlying subject. This allows the identity reference to be persistent over changes made to the attributes of the underlying subject, including its public key. We further suggest to separate the trust establishment over distributed communication into three categories: the transport trustworthy, the administrative trustworthy, and the content credential. We argue that separating the transport trustworthy from the content credential will potentially remove the reliance on Certificate Authority as used by traditional PKI and will eventually make the trust management more flexible and straightforward. We believe that the Handle System, a secured global name service, is a perfect candidate to realize what we have proposed in this paper.

5. REFERENCES

1. The Handle System Overview http://www.handle.net/overview-current.html, August, 2000
2. Public-Key Infrastructure (X.509) http://www.ietf.org/html.charters/pkix-charter.html
3. C. Ellison, B. Schnerer, Ten Risks of PKI", computer Security Journal, v16, n-1, 2000 pp 1-7.