Review Of The Cyberspace Policy And Trusted Identity Documents

Harry Katzan, Jr., Savannah State University, USA

ABSTRACT

This paper gives a brief but substantial review of two documents promulgated by the U.S. Office of the President: the Cyberspace Policy Review and the National Strategy for Trusted Identity in Cyberspace. An identity ecosystem, consisting of participants and infrastructure, is proposed and an operational framework is envisioned. The underlying concepts are substantial, and the overall implications should be of interest to the academic, business, and government communities.

Keywords: Cyberspace; Internet; trusted identity; policy, strategy

INTRODUCTION

Cyberspace policy and a national strategy for trusted identity are in the news, because the current digital infrastructure is inadequate to satisfy the operational needs of a modern society based on computers and the Internet. (White House 2010a and 2010b) An identity ecosystem is proposed to mitigate identity theft, fraud, and digital crime through an overall awareness of the root causes of information and communications security problems. (OECD 2008) The existing Internet is based on an open society, and a myriad of operational and security problems have evolved. It is generally felt that "leadership from the top" is needed to remedy the existing situation. Accordingly, the United States Office of the President has orchestrated a public/private 60-day clean-slate review of the existing U.S. policies and structures for cybersecurity. (White House 2010a) This paper gives a review of that initiative from a service science perspective. We will be taking a look at two documents, available from the White House at www.whitehouse.gov: *Cyberspace Policy Review* and the *National Strategy for Trusted Identity in Cyberspace*.

BACKGROUND

Several definitions are relevant to the ensuing review: identity, mission, strategy, governance, policy, service, and service system. *Identity* is means of denoting a subject in a particular namespace and is the cornerstone of security and privacy. A subject may have several identities and be associated with more than one namespace. A subject's identity may be self-determined or determined by others. The most trustworthy identities are determined by trusted authorities and established through an identity credential, such as a birth certificate, driver's license, passport, or military ID card. When one identity management system accepts the identity certification of another, a phenomenon known as "trust" is established, often facilitated by a third party.

Four organizational concepts are important, because they reflect the substance of this paper: mission, strategy, governance, and policy. (Katzan 2008) A *strategy* is "a long-term plan of action designed to achieve a particular goal," and *governance* is "the set of processes, customs, policies, laws, and institutions affecting the way an endeavor is directed, administered, or controlled. (Wiki 2008) The basic tenet of strategy is that a principal entity desires to accomplish an objective called a *mission*, required in order that an entity knows its direction, and the strategy determines how to get there. Thus, the mission is the subject's goal, and the strategy is the roadmap for achieving that goal. A strategy is a plan of action. A *policy* – the most problematic of the definitions – is commonly regarded as a set of guiding principles or procedures considered to be advantageous for influencing decisions or establishing courses of action.

Since we will be taking a service perspective, a brief mention of that approach is entertained. A *service* is generally regarded as work performed by one person or group that benefits another. Another definition is that it is a type of business that provides assistance and expertise rather than a tangible product. Still another definition is that it is after-purchase support offered by a product manufacturer or retailer. We are going to refer to it as a provider/client interaction in which both parities participate and both parties obtain some benefit from the relationship. The provider and the client exchange information and adopt differing roles in the process. A *service system* is a collection of resources, economic entities, and other services capable of engaging in and supporting one or more service events. Services, i.e., service processes, may interact or they may be included in a service value chain. This is a recursive definition of a service system that would support the following modalities of service operation: *tell me, show me, help me, and do it for me*. Service systems are inherently multidisciplinary, since a service provider may not have the knowledge, skill, time, resources, and inclination to perform all of the steps in a service process and require the services of an external service provider. (Katzan 2009) The service perspective is particularly appropriate to the study of interacting components in a trusted identity system.

CYBERSPACE POLICY PRELIMINARIES

Within this paper, *cyberspace* is defined as the interdependent network of information technology components that underpin most of our digital communications. (White House 2010b, p. 1) Many persons are affected by cyberspace, since it is a platform for business, education, government, and daily affairs. There is an overwhelming concern for the security of cyberspace, since its use has exceeded the original architecture. Cyberspace is additionally a convenient means for government, business, and education to exercise their responsibility to their constituents and serves as backbone for social networking. Many persons feel that software errors and negligent human behavior are responsible for Internet security problems, and are as much a security problem as the technical infrastructure. (OECD 2008)

Regardless of the root causes of concerns over security in cyberspace, it would appear that the following tenets apply, since a secure cyberspace is necessary for continued support for the U.S. economy, civil infrastructure, public safety, and national security: (White House 2010a)

- The Nation is at a crossroads
- The status quo is no longer acceptable
- A national dialogue on cybersecurity is needed
- The U.S. cannot succeed with cybersecurity in isolation
- The U.S. cannot outsource its responsibility
- A public and private dialogue is required for the establishing of a secure cyber infrastructure

It follows that cybersecurity should address mission-critical principles for computer network defense, law enforcement investigations, military and intelligence activities, and the intersection of information assurance, counterintelligence, counterterrorism, telecommunications policies, and general critical infrastructure protection. (White House 2010a, p.2)

CYBERSECURITY POLICY PRINCIPLES

In order to make cybersecurity a national priority affecting the U.S. goals of economic growth, civil liberties, privacy protection, national security, and social advancement, a set of guiding principles would necessarily apply. Here is the set of principles as espoused by the subject document:

Principle #1: Leading from the Top

The intension of this principle is that leadership should emanate from the White House, since no other entity has responsibility to coordinate Federal government cybersecurity-related activities. A cybersecurity policy official is proposed with operational authority to assure effective implementation of the strategy.

Principle #2: Building Capacity for a Digital Nation

The Internet and computers have transformed most aspects of daily life, and in order for security to persist, risk awareness should be addressed through a "public awareness" program, an enhanced educations system, and a capable workforce to the relevant subjects.

Principle #3: Sharing Responsibility for Cybersecurity

This principle insures that developments in cybersecurity will result from a partnership between the private sector and the government, as well as with the international community.

Principle #4: Creating Effective Information Sharing and Incident Response

A comprehensive framework for coordinated response from relevant parties to cybersecurity events is necessary for continued success and enhancement of a cyber ecosystem. Information sharing is required for this endeavor with the overall accountability being anchored in the office of the cybersecurity policy official.

Principle #5: Encouraging Innovation

Technical innovation in telecommunications infrastructure products and service is anticipated and encouraged. A single vision is needed to guide decision-making by the private sector, academia, and government. An R&D framework to link research to development, that is lead by the cybersecurity official, is proposed.

The Cyberspace Policy Review document concludes with near-term and mid-term action plans for the implementation of cybersecurity.

Analysis. The document entitled "Cyberspace Policy Review**"** is an exceedingly well-written and comprehensive review of Internet security provisions sponsored by the Federal Government with public/private cooperation. However, the content of the policy review reads more as a mission statement than a set of policy principles. The report succeeds, because it resists the temptation to venture into strategy and cybersecurity technology. The policy review presents a service system where the Federal Government is the service provider, and the stakeholders are the service clients. In fact, the proposed identity management system demonstrates two concepts in service science: collectivism and duality. (Katzan 2010) Collectively, the ontological elements of the identity management system provide a service to a subscriber, and the subscriber demonstrates service duality to the identity system, as a client without which the identity system could not exist.

NATIONAL STRATEGY FOR TRUSTED IDENTITY PRELIMINARIES

A key aspect of mitigating online crime and identity theft is to increase the level of trust between parties in cyberspace transactions. In this context, usage of the term "trust" is intended to imply that the subject and relying party are actually who they say they are. The strategy seeks to delineate methods to raise the level of trust associated with the digital identities of individuals, organizations, services, and digital components through a trusted cyber ecosystem so as to enhance the following: (White House 2010b)

- Security
- Efficiency
- Ease of use
- Confidence
- Increased privacy
- Greater choice
- Innovation

The overall objectives of the endeavor are to increase the protection of personal privacy through the following goals: (White House 2010b *op cit.*, p. 2)

Goal 1: Develop a comprehensive Identity Ecosystem Framework

Goal 2: Build and implement an interoperable identity infrastructure aligned with the Identity Ecosystem Framework

Goal 3: Enhance confidence and willingness to participate in the Identity Ecosystem

Goal 4: Ensure the long-term success of the Identity Ecosystem

Nine comprehensive actions are anticipated to align the strategy with operational reality: (White House *op cit.*, p. 2-3)

Action 1: Designate a Federal Agency to lead the public/private sector efforts associated with achieving the goals of the strategy

Action 2: Develop a shared, comprehensive public/private sector implementation plan

Action 3: Accelerate the expansion of Federal services, pilots, and policies that align with the identity ecosystem

Action 4: Work among the public/private sectors to implement enhanced privacy protections

Action 5: Coordinate the development and refinement of risk models and interoperability standards

Action 6: Address the liability concerns of service providers and individuals

Action 7: Perform outreach and awareness across all stakeholders

Action 8: Continue collaborating in international efforts

Action 9: Identity other means to drive adoption of the identity ecosystem across the Nation

It is anticipated that the Executive Office of the President (EOP) will be the lead agency in the above actions.

The *identity ecosystem*, comprised of transaction participants and an operational trust infrastructure, is the paradigm for the national strategy. The guiding principle for trusted identity is that there will be standardized and reliable identical credentials, methods of insuring those credentials, and relying parties that accept the trusted identities. It is up to the designers of the identity ecosystem to determine how the presented ideas will interoperate.

IDENTITY ECOSYSTEM FRAMEWORK (IEF)

The IEF is conceptualized as being comprised of three layers:

- The *execution layer* that conducts transactions according to rules of the identity ecosystem
- The *management layer* that applies and enforces the rules
- The *governance layer* establishes the rules and operations

A basic set of ontological elements relevant to the IEF are summarized in Table 1.

The *executive layer* is the place where participants and service components come together to instantiate a trusted transaction. The subject will possess an *identity credential* and the relying party will possess a *trustmark*. Both participants can request verification from a *certified provider*, which can supply identity attribute data, as required. Subjects and relying parties register with the identity provider beforehand. A sponsor may be required for proper registration.

Table 1. Basic Set Of Ontological Elements Comprising The Identity Ecoystem Framework

Element	Definition
Accreditation Authority	Assesses and validates that identity providers, attribute providers, relying parties, and identity media adhere to an agreed upon Trust Framework.
Attribute Provider	Responsible for all the processes associated with establishing and maintaining a subject's identity attributes; they provide assertions of the attributes to the individuals, other providers, and relying parties.
Credential	An information object created by a credential provider that provides evidence of the subject's authority, roles, rights, privileges, and other attributes. The credential is normally bound to an acceptable identity medium.
Digital Identity	The electronic representation of an entity (e.g., a device, software, service, organization, or individual) in cyberspace that is comprised of an information artifact or correlated information sets.
Governance Authority	Oversees and maintains the Identity Ecosystem Framework and defines the rules by which a product or service provider in the Identity Ecosystem attains trustmarks.
Identity Ecosystem	It is an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities.
Identity (1)	A unique physical being that identifies somebody or something. Identities can apply to persons or non-persons (NPE).
Identity (2)	A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information (for example, an address, or some unique identifier such as an employee or account number) to make the name unique.
Identity Provider (IDP)	Responsible for processes associated with enrolling a subject and establishing and maintaining the digital identity associated with an individual or NPE. These processes include identity vetting and proofing, as well as revocation, suspension, and recovery of the digital identity. The IDP is responsible for issuing a credential, the information object or device used during a transaction to provide evidence of the subject's identity; it may also provide linkage to authority, roles, rights, privileges, and other attributes.
Identity Proofing	The process of providing sufficient information (e.g., identity history, credentials, documents) to a service provider for the purpose of proving that a person or object is the same person or object it claims to be.
Relying Party (1)	A relying party is a provider of online services to a subject. Within the ecosystem, a relying party is responsible for interacting with credential, identity, and attribute providers as needed to verify parties with whom they exchange information.
Relying Party (2)	An entity that relies upon the Subscriber's credentials or Verifier's assertion of an identity, typically to process a transaction or grant access to information or a system.
Trustmark	A badge, seal, image, or logo that indicates a product, device, or service provider has met the requirements of the identity ecosystem, as determined by an accreditation authority. To maintain trustmark integrity, the trustmark itself must be resistant to tampering and forgery; participants should be able to both visually and electronically validate its authenticity. The trustmark provides a visual symbol to serve as an aid for individuals and organization to make informed choices about the providers and identity media they use.

(Source: White House 2010b, Katzan 2010d)

Clearly, the subject and relying party are outside of the basic cyber infrastructure, whereas the identity provider and supporting elements are subsumed in the identity ecosystem framework. The ecosystem provides a service to the relying party, and the relying party provides a service to the subject.

The *management layer* is the component that handles credentials, attributes, and registration. A subject and a relying party must register with at least one identity provider. Identity validation is performed by the identity provider according to rules established at the governance layer for use in the management layer. The notion of an attribute provider is conceptualized but appears to be an operational item requiring further study.

The *governance layer* will provide facilities for assessing and certifying identity ecosystem service providers through a Governance Authority, conceptualized to control the rules for identity and trusted certification to identity providers and service providers (i.e., relying parties). Before any participant, with the exception of individuals, can join the identity ecosystem framework, it must be certified by an accreditation authority to insure that the service provider is trustworthy.

As a conceptual entity, the identity ecosystem will have the following characteristics: (White House op cit., p. 17)

- Individuals and organizations choose the providers they use and the way they conduct transactions securely.
- Participants can trust one another and have confidence that their transactions are secure.
- Individuals can conduct transactions online with multiple organizations without sacrificing privacy.
- Identity solutions are simple for individuals to use and efficient for providers.
- Identity solutions are scalable and evolve over time.

and provide the following benefits for individuals:

- Security
- Efficiency
- Ease-of-use
- Confidence
- Privacy
- Choice

Analysis. The proposed National Strategy for Trusted Identity in Cyberspace appears to be a well-conceived vision for future operations in a global society based on the Internet. Many persons feel that the Internet security problems are simply the result of buggy code and careless users. However, the identity problem still remains. Without a trusted authority, how do you know that the participant on the other end of the line is who he says he is?

SUMMARY

The reports addressed by this paper are long and complex document, consisting of 65 and 36 pages, respectively. A comprehensive summary would be long and tedious. One approach could be that the contents be summarized by the 8 Fair Information Practice Principles (FIPPs): (White House 2010b op cit., p. 36):

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

The principles are rooted in the United States Department of Health, Education, and Welfare's report entitled *Records, Computers, and the Rights of Citizens*. "The universal application of FIPPs provides the basis for confidence and trust in online transactions."

AUTHOR INFORMATION

Dr. Harry Katzan is the author of books and papers on computer science, decision science, and service science and is the founding editor of the *Journal of Service Science.* His current research interests are in service design and the National Strategy for Trusted Identity in Cyberspace (NSTIC).

REFERENCES

1. Katzan, H. 2008. *Foundations of Service Science: A Pragmatic Approach*, New York: iUniverse, Inc.
2. Katzan, H. 2009. Principles of Service Systems: An Ontological Approach. *Journal of Service Science*, 2(2): 35-52.
3. Katzan, H. 2010a. *Privacy, Identity, and Cloud Computing*, New York: iUniverse, Inc..
4. Katzan, H. 2010d. Ontology of Trusted Identity in Cyberspace, (in publication).
5. OECD 2008. Scoping Paper on Online Identity Theft: Ministerial Background Report, June 17-18, 2008, (DSTI/CP(2007)3/FINAL, Organization for Economic Co-Operation and Development.
6. White House 2010a. Cyberspace Policy Review: Assuring, a Trusted and Resilient Information and Communications Infrastructure, Office of the President, 2010, (www.whitehouse,gov).
7. White House 2010b. National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy, Office of the President, June 25, 2010, (www.whitehouse,gov).

NOTES