IDENTITY AND RESILIENCE

Background

With the advent of the era of the Internet and globalization, empowered individuals and groups have emerged who use global interconnectedness and anonymity to engage in criminal activity and transnational terrorism. Security, privacy, and civil liberties are being severely challenged due to the limitations of existing policies, practices and systems. This problem will increase dramatically as we become even more dependent on the Internet and as we render more and more of our personal identifying information to arbitrary authorizing agents (e.g. governing agencies, merchants, social networking sites, etc.) for their perceived necessity, convenience and/or value. Compounding this problem is that our dependence on Internet services for critical infrastructure (e.g. national defense, homeland security, financial services, power, communications and transportation) will increase and without an adequate system to manage risk of authenticating counter-party claims, the probability of a breach compromising these critical services will most certainly become untenable within the next decade.

However, security and privacy interests do not have to present a dichotomous choice between identity and anonymity. Rather, the challenge is how to build systems for traceable anonymity (pseudonymity) that support both security and privacy needs. Pseudonymity can preserve privacy (through anonymity in the ordinary course of events and political autonomy) but also allow for security concerns to be addressed (match watch lists, verify authorization and provide accountability through exchange of digital hashes). This assumes legal, organizational and technical mechanisms are devised to protect identity escrow. The Markle Foundation Report on Privacy and Security in an Information Age concluded: "There is strong evidence that having reliable means of personal identification would greatly enhance many of the new security measures introduced since September 11, as well as those that were in place prior to the attacks."

Most of our economic well-being and many of our most pressing national initiatives are heavily reliant on information technology (IT). They range from reducing the cost of healthcare to national security concerns involving network resiliency and citizen identification. Today, each program develops its own security and identity approaches in isolation. The negative consequences of this tradition include increased IT costs, a balkanization of identity data, and, from the individual user's perspective, a confusing patchwork of authentication approaches and user experiences. In contrast, a holistic approach to identity is required. A common identity infrastructure that is open, distributed, privacy-preserving, secure, and convenient to use, would be an essential step in protecting individuals' rights and resources and enable society and the economy to safely achieve positive results for all. As we look to make huge savings throughout our government and business sector, innovative use of IT may well result in cost reductions from reuse of a standard framework, instead of the current ad hoc approach that has resulted in hundreds of incompatible identity "silos."

Just as DARPA's role in the creation of the Internet led to massive benefits for our country, leadership by the Federal government in identity infrastructure could not only address pressing concerns for security, resiliency, and cost reduction, but also create a foundation for new IT directions such as cloud computing and dynamic mobile networks. In fact DARPA didn't go far enough. Many have noted the absence of an Internet "identity layer" is what has created many of the problems just mentioned. After all, the Internet was designed for sharing information, not for securely identifying users and protecting personal data. However, the rapid proliferation of online theft and deception and the widespread misuse of personal information are threatening to erode public trust in the Internet and thus limit its growth and potential.

In addition to physical attack or natural disaster, the telecommunications networks and computer infrastructure required to support information-based economic and social life in modern economies is also subject to cyber attack. Cyber attacks can be malicious or accidental; can involve attacks by other nation states, organized groups, or individuals; and can be motivated by monetary gain, ill-will, or political interests. They can be directed at governments, firms, or individuals. They can involve the theft or destruction of information; the theft of services or financial assets; or the destruction of hardware or software infrastructure. They can result in financial loss, business or service interruption, or infrastructure destruction. They can be aimed at disrupting telecommunications services or infrastructure, or be intended to disrupt other services or industries dependent on functioning communication services.

Economic and national security require resilient communication networks—that is, networks that can withstand damage and continue to provide service in face of direct physical or cyber attack, natural disaster, or other disruptions. Network resilience requires strategies (1) to protect against or avoid failure; (2) to minimize, localize, or otherwise contain failures that do occur in order to avoid collateral or residual damage; and, (3) to repair, route around, or otherwise respond to failures in order to continue service. Achieving resilience requires investing in security, redundancy, and interoperability. Since over 90% of telecommunication infrastructure is in private sector hands, government policy mechanisms are needed to influence private firm behavior in areas where market externalities inhibit sufficient investment in resilience or inter-firm cooperation, particularly where the consequence of failure has national effect. Available policy mechanisms include direct regulation, technical standards, insurance requirements, immunity and liability policy, tax incentives, market mechanisms, government as a lead user, and others. The Federal government, including its law enforcement and intelligence agencies, requires a more secure identification system in order to screen access to the national borders, federal facilities, and certain vulnerable infrastructure.

Without the element of counter-party trust between those interested in executing transactions, it is hard to imagine the emergence of the Internet economy let alone Web presence. Identity management is the system of claims and attributes that can be asserted and verified by the actors in a transaction that solves this problem. Identity becomes the proxy for trust that enables the development of robust personal commerce on the Web.

The New Environment

What is emerging that demands change soon on identity solutions is the "cloud" environment; industry is already there (Google, Amazon, and many others) and DoD has already made the commitment to move its computing and communication to the cloud. The cloud and the Web are separate, but complementary platforms that are based upon the power of the Internet triad: the cloud will be the *computation, storage and communication utility* that provides commodity services upon which web service is generated, metered and billed. The Web consists of the "ends" interacting in an infinite number of dynamic relationships. We are now at the inflection point of the evolution of the Information Age, the point at which the commoditization of information technology will result in the emergence of the cloud of utility communication and computing services supporting the Web of collaboration and economic services on-demand. The cloud will enable the evolution of the web of safe and secure on-demand services for end users whose presence will be extended over the web merging their physical and virtual worlds.

How can we secure the public Internet and make the promise of the Cloud a reality? Four steps are required to achieve a more secure Internet. First, we must provide a more robust notion of identity. Identity involves three broad concepts: labels, names, and trust. You can trust the data, even without trusting how it was delivered. Names allow us to attach semantics to these labels. Trust mechanisms mediate between these two sides of identity. They are market-driven, plentiful, and offer choice to the individual user. The second step is to secure the data and not the channel. The third step is to send the data through multiple pathways to ensure resilient data delivery. This can pose significant architectural challenges. The final step is to address denial-of-service cyber attacks.

Two of the largest challenges are open standards and identity. Our standards currently are not sufficiently open for the cloud to evolve. When the Internet and the Web first emerged, there were powerful centripetal forces that drove people together – through the benefits of linking networks and of developing single browsers that could move across the entire Web. Those forces are not as strong today as we build the cloud. In fact, numerous companies have attempted to build their own proprietary, walled-off gardens in the cloud. The same is true for identity, and it will not be tenable to have a single company or even a small group of companies controlling identity in the cloud. Unfortunately, no one has developed a viable business model yet for open-standards-based identity. This is one of the reasons that government, as an early adopter, should help push standards in the right direction and ensure that these companies do not make parts of the cloud proprietary.

Identity is everything. Security may not matter if you cannot solve the identity problem. This means that concepts of risk management should replace concepts of trust in our thinking.

The Rise Of A "Meta" Identity Framework

The Internet makes access, copying and asserting ownership of information and claims (e.g. claims of identity, authority, affiliation or capabilities) much easier and less expensive for the fraudulent claimant. It fortunately also presents us with the opportunity to solve this problem through the appropriate application of existing technology to leverage the Internet to implement a distributed identity management meta-system abstraction layer. This is made possible by the Internet's capability to reach any and all authenticating agents in order to effectively address the issue of counter-party trust through collaborative, distributed authentication, solving the problem in a systematic and comprehensive manner. Without adequate identity management we cannot effectively address homeland security, financial security, health care record management.

The technology exists today to address this problem, what is needed is visionary leadership to make possible the implementation of the policies and services required to enable it to succeed in solving the real-world problems that we will face in this century including homeland security, health care and identity theft (ecommerce) in a systematic and compressive manner. The technology to implement an Identity Management system is based on the *"Laws of Identity"*, codified and put forward by Kim Cameron. They serve as the basis for most of the work underway around the world on identity and together they define the architecture of this missing layer of the Internet that is both objective and testable. The basic idea is to implement this system based on the concept of "User Centric Identity" which abstracts identity from authentication and authorization and puts the user in control of the release of their personally identifying information. It is important to point out that the key to making this technology work is that this identity abstraction can only be effectively implemented based on a distributed system of authentication services, each with only the minimum set of personal information necessary to execute their particular service. In previous attempts to solve this challenge, both a centralized identity system (i.e., *Passport*) and a static token (i.e., *Real ID*) were proved to be too vulnerable to breach and catastrophic failure, as well as too static and not as scalable or robust.

Over the last five years, architects and developers concerned with identity management and security issues have worked together to develop a standards-based identity framework that embodies the principles outlined above. This new framework is inclusive and can integrate multiple protocols, authentication methods, and access control regimes. However, to be accepted for use on the public Internet, it was widely recognized that no single vendor should dominate or control the framework. For example, the inability of Microsoft's *Passport* to gain the trust of users and achieve widespread industry acceptance made it apparent that the new identity framework for the Internet had to be vendor-independent. This has been achieved by an unprecedented level of collaboration, including Microsoft and other software industry leaders. In order to be accepted by users, the new framework had to simplify their interactions with a wide variety of different systems on private and public networks. Today users are presented with a confusing array of authentication experiences. The requirement for a single, consistent user experience was the genesis of a new user metaphor called "Information Card" (I-Card).

The technologies to implement this identity management abstraction now exist and are implemented in software open standards. The previously mentioned I-Card system (http://en.wikipedia.org/wiki/I-Card) is one example and is supported by many of the largest technology companies. In June 2008 Microsoft and the Higgins group forged the I-Card alliance, the Information Card Foundation (ICF). The foundation works to promote interoperability of all aspects of I-Cards as well as to evangelize adoption. Leading developers and implementers of I-Card technology including Microsoft, Google, PayPal, Equifax, Novell, Oracle, Intel, Deutsche Telekom and many others launched the ICF.

A Consideration

One characteristic of open, vendor-neutral frameworks is that they are inherently commodities (or a "commons") for which, by design, little commercial advantage can be extracted and few profits can be captured. Everyone wants this infrastructure to exist, as it is a key enabler of more efficient and secure commerce, healthcare, and e-government. Paying for it is another matter. In fact, government agencies, healthcare providers, and technology providers often have structural incentives not to embrace disruptive, open technologies as they destroy certain proprietary advantages and lock-ins. Nevertheless, a holistic approach to identity is not only feasible, but it has been largely developed through a coalition of major industry actors. What is needed now is the vision and will to develop the policies that will drive deployment of a common identity infrastructure and enable commerce, healthcare, and government to enjoy its considerable benefits.

As the largest consumer of technology and information in the world the United States government is best positioned to facilitate the implementation of an effective Identity Management System. It would be a worthwhile first step for the executive branch to make solving the identity challenge a priority and engage public and private sector leaders in conversations leading to the development and adoption of a non-proprietary "meta" identity framework to enhance privacy, security, confidentiality, and economic growth.

This paper represents the collaborative work of Mr. Paul Trevithick of The Information Card Foundation; Mr. William Coleman, CEO of Cassatt; Dr. John Clippinger of the Harvard University Berkman Center for Internet and Society; and Mr. Kim Taipale, founder and executive director of the Center for Advanced Studies in Science and Technology Policy.