Managing Identity and Authentication on the Internet
An Introduction

Identity on the Internet is fluid and uncertain. Online identities are provided by networks that are loosely coupled to each other and to the official identities provided by governments. Certainty or authenticity comes from personal acquaintance, contract or trust in a network administrator. These solutions are not scaleable and will not lead to the trusted public networks needed to take full advantage of digital technologies.

In response, governments and commercial providers are creating systems to manage and authenticate online identities. Governments in the U.S. and elsewhere may make robust digital identities a requirement for citizens to receive services and benefits online. Commercial services will use authentication of identities to authorize services and transactions as autonomous software agents, ubiquitous computer networks and wireless connectivity further extend the reach of the Internet into business and consumer activities.

Interaction between these government-issued identities and commercial services is unavoidable. While individuals will use a range of identities online (from near-anonymous to legally binding), high-value or high-risk transactions and services will require robust identities issued by or equivalent to those provided by governments.

The result is interconnected policy problems involving the interoperability and robustness of digital identities. Neither problem is technical. They ask how an identity issued in one autonomous system can authorize actions in another, and how much trust one system can place in an identity issued by another. As consumers and firms assume (or are assigned) online identities provided by both the public and private sectors, governments, companies and citizens will need to decide how autonomous and heterogeneous systems cooperate and interoperate in managing Internet identities.

To help move forward on identity and authentication issues, CSIS has created a Working Group of experts from industry, academia, and government. Lawrence Lessig and Craig Mundie co-chair the group which will consider the rules, standards or architectures required for robust, interoperable identities and identify where it is appropriate (or necessary) for government and commercial systems to interoperate and cooperate in authentication. The group will also look as the implications of identity systems for governance, privacy, cybersecurity and electronic commerce. The outcome of the group's deliberations over the eight months will be concrete recommendations for managing identity that work across companies and across national boundaries.

Managing Identity and Authentication on the Internet
Proposal and Summary
March, 2002

How does a machine know you are who you say you are and what you are allowed to do? A car 'knows' you are authorized to drive it when you insert a metal key. An automatic teller knows who you are and how much is in your account when you insert a magnetic card and enter a Personal Identification Number. The machine isn't actually confirming your identity; it is accepting a 'token' issued to you by someone else, who may have taken steps to confirm at the time of issuance that you are who you say you are.

Managing digital identities and information is a central issue for Internet governance and the digital economy. Identity management and authentication will only grow in importance as Internet and wireless applications and services become further integrated into business and consumer activities. Progress in resolving issues related to identity and authentication is essential to reach the full economic potential of the Internet and for its expanded use in providing new services. Identity and authentication also have deep implications for commerce, public safety, civil liberties, and privacy.

Americans identify concerns with the lack of security and privacy on the Internet as the chief obstacle to its greater use as a business tool. A "trusted" network goes beyond engineering concepts and requires a marriage of technology and procedures that allow users to feel confident that important data and messages are confidential, unmodified, and linked to an unambiguous identity. Building secure and trusted public networks requires developing the policies and legal and regulatory structures needed for trust, coordinating theses structures among nations, and determining how they relate to the architecture, technology and commercial viability of Internet services.

CSIS is undertaking a multifaceted examination of Internet governance issues, with projects on the political and economic implications of content regulation, the role of the private sector in cybersecurity, and on international regulation of online activity. Authentication of online actors' identities is an essential element of cybersecurity (along with infrastructure protection and confidentiality and integrity of data). This new project will look at the role of identity in cyber security and the growth of the Internet. CSIS will bring together experts from industry, academia, and government to identify feasible recommendations for managing identity on the Internet.

Background

The expansion and commercialization of the Internet, an open, geographically dispersed system, changed the nature of computer networks and created new problems for governance. Security, privacy, and trust were an assumed part of the smaller, government-run network populated by universities, government agencies and research networks. Infrastructure and rules were designed to maximize information sharing among networks and users. The nature of much of the activity on this early Internet- essentially the open exchange of information, subject to peer review among a community of researchers with no commercial transactions and few automated services

- also required a lesser degree of trust and security. Misrepresentation offered little benefit and held inherent risks and penalties. Privatization and commercialization changed this by adding millions of anonymous users and by introducing a broad range of commercial services to the Internet. The change to a quasi-anonymous commercial network created a new set of problems revolving around trust and security.

Early assumptions that a secure public network for communications and business would emerge naturally as a result of market forces were optimistic. The Internet is a collection of networks whose technical standards aim at compatibility among diverse systems. Data integrity, security and authentication were initially secondary issues. The Internet environment remains one of rapid growth and diverse, evolving technologies. The result is a network of unsecured systems that do not uniformly or predictably provide integrity and nonrepudiation, confidentiality, and authentication for transactions. The effect is to seriously impede the further development of the Internet as a new way to organize economic activities. A recent study estimated that $15 billion worth of business-to-consumer and business-to-business e-commerce transactions are unrealized because of concerns over trust.

This problem will only grow more complex as ubiquitous computing and expanded Internet activity become normal elements of business and private life, and as nations take different approaches to regulating internet activities. The drivers of this new digital environment for consumers and firms will be embedded network, wireless connectivity and autonomous software agents. Processing power and memory will be abundant resources in the near future. Computer and Internet access will, in a few years, be like the electrical grid: cheap, readily accessible, and integral to daily life. Wireless connections to this computing grid will make Internet-enabled devices sophisticated, interconnected and ubiquitous.

With the right framework of rules, new software applications will take advantage of these ubiquitous computing resources and automate many routine activities (allowing machine to talk to machine without human interaction). These applications could allow for computer control of devices and appliances or authorization of commercial transactions through the Internet, using mobile, wireless devices (like laptops and PDAs) and through anonymous public access points that will allow use of the Internet much the way that public phones allow access to the telephone networks. Autonomous software agents could automate a new range of routine activities, to control inventory, negotiate contracts and prices between suppliers and customers for purchases, and arrange for shipping and delivery without human intervention.

Trust (in this case, authentication of identity) has become a function of exchanges between persons and machines or exchanges between machines (without human involvement). Interactions are rapid and automatic, executed according to a series of pre-programmed rules whose composition and nature may not be accessible to the user. We have examples of this available now - gas pumps and fast food outlets automatically accept passkeys for payment and bill specified accounts, implicitly accepting that the person holding the key is authorized to make the transaction.

The need for automatic authentication of identity and authorization will increase as wireless applications proliferate and as people become increasingly sophisticated in using network

enabled services. Standards like 802.11 and Bluetooth already allow devices to link wirelessly to computer networks. New applications will take advantage of this wireless connectivity to let people use the Internet to remotely or automatically authorize actions. Using the Internet for authorization instead of special purpose devices simplifies applications and lets a greater number of appliances and applications authorize more activities at greater speed and range. Wireless connectivity and cellular networks will offer new applications and services that are cheaper and more convenient and will let individuals remotely authorize new sets of transactions - such as remote management of houses and other property, mobile authorizations for purchases, or delivery of specialized services and data. Price advantages and market forces will drive applications and networks in this direction.

Ubiquitous computing and wireless connectivity to the Internet will place an increasing burden on mechanisms for authenticating identity and the authorities associated with that identity. Currently, digital identity can involve a profusion of telephone numbers, PINs, accounts, Internet connections with multiple user-names and passwords; legal identities associated with government issued documents and. The result is multiple, incompatible sets of rules that govern issuance and the use of identities.

The rules will for the most part be developed privately, but they lack a common framework of principle, law, and practice to guide them. Existing legal structures for identity and authentication are, for digital applications, sufficiently amorphous (or insufficiently developed) and allow a wide range of variation. Digital signature laws do not always address how identity is assigned or managed. Public scrutiny and oversight and compatibility among systems (nationally and internationally) pose real challenges. Market forces alone will not generate a solution. Improved governance means replacing a series of unrelated, ad hoc efforts with a transparent and accountable system using cooperative efforts among private entities, legislative and regulatory processes or some combination of private and governmental approaches.

In one scenario, a single smart card with strong biometric identifiers could serve as a driver's license, passport, credit card and Internet access enabler. The University of Pennsylvania already issues its students a 'smart' ID that authorizes network and building access and which can be used in local stores and restaurants. Alternatively, a single, firmly linked legal identity could be established and shared by a number of devices - smart cards, cell-phones, PDAs, for authentication and authorization. Or individuals could use a matrix of identities, some robustly linked and binding and others offering more anonymity or a reduced authority that they could draw upon for differing kinds of transactions.

The implication of a lack of trust is that Internet use and the provision of services will be slowed and made more complicated, imposing real economic and social costs. The events of September 11 give the issue added importance for security. "Trusted" networks are an essential element of cyber security and critical infrastructure protection. The ability to reject traffic from "untrusted" sources (i.e., those without certificates or not otherwise properly authenticated) would improve cyber security and critical infrastructure protection. Information technologies, combined with biometrics, could be used to create a national or even international identity system for use both on the Internet and in daily activities. Increasing the level of trust is not technologically infeasible, but the technologies required to increase it can create serious political and policy

problems. A lack of compatible rules for how identities would be established and authenticated and how they would interact and enable would create confusion and increase the potential for balkanization of the Internet.

Managing Identity on the Internet

A completely anonymous world would be neither safe nor productive. Identity allows us to assign privileges and responsibilities, and liability in cases of dispute. At the same time, a world where identity was unbreakably linked to every action would be stifling. The Internet offers the possibility of both worlds. Individuals will want a range of identities, from anonymous or near-anonymous, weakly linked identities or pseudonyms, to robust, legally binding identities that mirror the options available to them offline.

Traditional methods of identification, developed over decades of practice and evolving in the face of new technologies, are inadequate for Internet purposes. Visual or voice recognition and even some digital signature technology are vulnerable to capture and manipulation during transmission over the open, distributed networks that make up the Internet. Advances in digital signature technology promise some relief, as do biometric technologies, but existing digital identification techniques are not yet widely used.

This reflects several factors. Individuals prefer to "manage" their identity (or identities) through a variety of mechanisms. The degree to which they are identified and the amount of information imparted through that identity process will vary depending on their assessment of the benefits and the risks. As with cars or ATMs, identification depends on a third party placed between user and machine, whose 'assertion' or 'token' can be trusted. Risk appears in the structure of authenticating identity, in the effectiveness of third party authentication and, more importantly, in issues regarding how information generated by identity systems is safeguarded and used.

A failure to improve identity management would reduce the benefits of a global computer network for commerce and public activity. These benefits are so great that it was once thought that market forces would result in improvement, but we can no longer assume that the market alone will rapidly or smoothly resolve authentication problems. Better systems for identity authentication and authorization may not emerge if governance is not adjusted to allow their use or if demand for them remains low. A number of factors could depress demand for authentication below the point necessary for widespread adoption, in particular risk (especially risks associated with third parties) and pricing (in light of viable, albeit limited, alternatives for managing identity).

Despite progress in digital signatures and the provision of certificate services, many larger network users still rely on signed, written contracts as the basis for trust. Contracts, which spell out the responsibilities of each party, create a private basis for trust in business, but this solution is not scaleable, is overly expensive for many transactions and reduces the benefits of autonomous agents and public networks.

Authentication mechanisms are necessary for a thriving networked economy, but their development and implementation raise important concerns for individual privacy and system

security. The core issue is that the third party will not adequately protect identifier information from misuse, or that the third party service provider will itself misuse information - not authentication information per se, but information provided as part of the identification process or generated by the client's activities on the internet. To strengthen trust, multiple parties will have to act in a coordinated way. Third parties can overcome some of these concerns if there are strong procedures for their activities. This can be accomplished through regulation and oversight, either by government agencies or through some self-regulatory process. Both public and private solutions have strengths and weaknesses in managing authentication and identity. Improving identity and authentication on the Internet, and ultimately security, requires addressing these problems.

Governance, the ability to determine policies and set rules, has not been one of the Internet's strong points as it has developed. Governance issues, like the management of identity, have become an obstacle to growth, and a source of risk for public safety. Providing the architecture and rules for persistent, unambiguous authentication of identity is one of the challenges that must be addressed for further progress.

Working Group on Authentication and Identity

To encourage progress on identity and authentication issues and to help move forward the development of a more secure digital environment, CSIS proposes to create a Working Group that will bring together American and foreign experts from industry, academia, and government. The Working Group will meet to consider and discuss larger questions about trust, security and privacy, and then concrete recommendations for the treatment of identity. Potential issues for consideration include:

- What rules are needed for more robust mechanisms for identity on the Internet? What is the process for making these rules, and what principles or standards should guide them? How should they govern the actions of multiple authentication systems, allowing cross recognition and cooperation (between companies and between nations)?
- What are the requirements for international cooperation, and what are the potential vehicles (official or private sector) for achieving this?
- What are the economic, technological and regulatory implications for managing identity? Do different technological approaches to managing identity have differing requirements and implications?
- What effects do different architectures, organizational models or hierarchies have for the wide deployment of authentication technologies on the Internet? How would multiple identities be managed and authenticated?
- What is the nature of the partnership between government and the private sector within countries and between countries? Which activities and services are best left to the private sector and which are better supplied as a public service? How are private actions coordinated to achieve a public good?
- Are there new legal or regulatory authorities needed for improvements in authentication and trust? How will trust and authentication systems be enforced?
- What is the connection to larger privacy and civil liberties issues of reducing anonymity and expanding accountability?

The project effort would be supported and informed by expert groups composed of both working group members and outside exports to review specific issues. The involvement of experts from outside the U.S. will be a particular goal. Sessions could be open to public participation if there was interest among working group members to do so.

Goals and Deliverables

The goal of the Working Group is to develop common principles and recommendations that could be applied to developing identity and authentication, including recommendations for processes that would lead to clear set of rules for identity that would be compatible across companies and across borders. An interim report would identify issues and options for principles, rules and processes. A final report would propose principles for identity and authentication, make recommendations for government and the private sector, and suggest a common platform for international compatibility. These reports will be distributed extensively to the Washington policy community as well as multilateral bodies such as the European Union. Particular effort will be made to distribute the report to Congress. CSIS and the Working Group will also arrange a series of public briefings and related press events to publicize the findings of the report.