Identifiers and Authentication – Smart Credential Choices to Protect Digital Identity

In a digital age, the reality is that simple identifiers (e.g., e-mail addresses, login names, identification numbers) are used without any protection and should be considered public information even though they point to a specific individual. In addition to the increase in public exposure of such data, the provisions of ownership of personal identifiers have not been effectively addressed, and there is a lack of legal infrastructure today to ensure the privacy of such information. For example, when personal identity information is altered, misappropriated, or attached to another user, what are the rights or duties of the custodian organization on the behalf of the person who in effect "owns" the identifier? Should there be some form of authentication (involving a hard-to-duplicate element) for such a restricted operation?

Identifiers are in widespread use today including the following examples:

- License plates on cards
- Vehicle identification numbers (VINs) on cars
- Toll payment tags (e.g., E-ZPass)
- Transit fare payment cards (e.g., Metro cards in Washington, DC)
- Passport numbers
- Credit card numbers
- Medical insurance card numbers
- Driver's license numbers
- Bank account numbers
- Social media identifiers
- E-mail addresses
- Telephone numbers
- Usernames for online accounts

Each of these identifiers has varying levels of security features built-in (for example, resistance to cloning, ability to be used for tracking, ability to be used alone or with other authentication factors such as a personal identification number (PIN) or password). All of these identifiers have the capacity to be over-used and point to individuals in the same way that the Social Security Number (SSN) is used within the United States. The lack of legitimate owner control of changes to (and sometime use of) these identifiers and the information attached to them presents a threat to personal identity (whether for tracking activities, stealing funds, or providing a gateway to other elements of personal information).

The Social Security Number, initially created to identify people for taxation, has been used for many other purposes, such as linking people with their credit worthiness. There are fewer motives to steal an identifier used to file taxes than to steal an identifier that allows access to money. It is obvious that the authentication methods used to verify who owns an identifier must be very different depending on the criminal incentives to illegally obtain such numbers.

It will be difficult (but would not be impossible over time) to get back to the separate identification mechanisms that many other nations have adopted. For example, it is not uncommon for Europeans to have an identifier for a passport, another identifier for an identity card, another for a driving license, another for retirement and government benefits, another for taxation purposes, and another for health insurance. However, the use of separate identifiers has created a fear that this approach would lead to more confusion about an individual's identity, allowing some people to have different "identities" in all of these apparently separated systems. In the U.S., the notion of a national identity card also raises the fear that personal liberty would be at risk. These two concerns have resulted in all of these separate systems using the SSN as the de-facto identity super-identifier, in an attempt to verify that individuals are who they claim to be.

Using the SSN as the super-identifier has been proven to be fraught with problems and has highlighted the need to change the methods for identifying individuals.

An alternative method could be to recognize different types of identifiers for the various systems, but have a common identity vetting process and focus on authenticating the identifiers in a trusted agent model. In this model, identifiers would be assigned through a trusted agent based on a common identity verification model and each system would have the capability to authenticate its own identifier when later used by the individual. (The U.S. Federal Bridge is an example of this type of trusted agent model for identity vetting.) Use of a trusted agent model for identity vetting allows separate systems to share a common trust model for establishing the identity of an individual based on common identity vetting practices accepted by all these systems.

Nevertheless, an individual's identifiers should not be volatile and changed too often since this would force the identity vetting process to be repeated each time the identifier is changed. In the early 1990s, Germany changed the numbering system for medical insurance cards. Instead of identifiers generated by individual insurance companies that changed each time employers changed medical plans, Germany created a medical insurance number that is assigned to each person eligible for medical insurance. The number, allocated once for each citizen, would be used by all insurance companies and stay with the individual. This completely changed how an individual's medical information was exchanged, protected and stored.

Many identifiers are used for different types of accounts or documents – for example, passports, driver's licenses, bank accounts, telephone numbers, credit cards, and car, home and medical insurance numbers. In addition to these, a myriad of usernames and e-mail addresses are used to access online accounts and resources. The identifiers all point to different databases, have specific purposes, and have a specific type of information attached to them. Too often, even with these identifiers, it is the SSN that is used as the ultimate element identifying an individual.

The SSN is the only truly unique identification number in the U.S. that is attached to an individual and that is assigned to virtually the entire population. The problem is that this number is not (and cannot be) protected and as such it should never be used as an authenticator. In addition, recent research has shown that the SSN can be predicted based on an individual's date and place of birth.[1] The SSN is an identifier that has been used and abused without proper authentication. Whoever claims the number can be identified as the person to whom the database identifier points. All identifiers, including the SSN, should be considered as public information and should never be used without authenticators when a person claims ownership of the identifier.

Smart Chip Credentials – An Option

Organizations are looking for solutions to the problem of accurate identification of individuals. For example, credit bureaus have proposed protecting (or freezing) access to credit information using a number (possibly the SSN) as the identifier and a PIN as the authenticator. Using a PIN for authentication is an improvement over other methodologies (such as using the mother's maiden name, which can be found in any ancestral data base). However, a person would rarely need to access this information, so it is likely that the PIN will be forgotten or recorded somewhere. What kind of security will be used when, as happens, the PIN is forgotten and must be reset?

In this specific example, a technical solution exists that offers very strong authentication, is very resistant to cloning, provides a unique physical object used for authentication, and is very hard to imitate even when used with an insecure computer over an insecure network. This solution is a smart chip-based credential and card. If lost or stolen, the card can be revoked and a new one issued. Unlike passwords or knowledge-based information, an attacker must physically steal the smart card in order to try to use it. Even then, the card can only be in the possession of one person at a time (as no duplicate can be easily made), limiting the speed and scalability of attacks. Adding biometric verification to the possession of the card would provide another level of security.

Using smart cards to authorize access to critical credit information would be a way to secure our existing systems and limit the serious problem of identity theft. Instead of freezing credit information and requiring a PIN to unlock the information when access is needed by the user, merchants (or banks or credit

[1] New York Times, " Weakness in Social Security Numbers Is Found, July 6, 2009

bureaus) could provide a terminal (or a portable device) that would be used by the information owner with the smart card for authentication to the credit bureau (e.g., over a phone or network). The smart card would provide a one-time authorization allowing the information requestor to access the credit information.

Smart chip-based credentials are being used around the world for identity verification. The most common application is the mobile phone. By using a smart chip, billions of unique identifiers have been created that allow mobile phone owners a secure method for being identified when engaging in communications and transacting commerce. Within the payments industry, smart chip technology is deployed in nearly a billion payment cards and devices to ensure secure transactions for merchants, banks and consumers; the use of smart chip technology has shown a clear causal link to reducing fraud. In the United States, the issuance of millions of interoperable smart identity credentials to Federal and transportation workers has created the identity infrastructure to support credential holders and place them clearly in control of their unique identifiers. These credentials support multiple authentication factors (PIN, fingerprint template, digitally signed photo), as well as provide a way to digitally sign and encrypt security documents, other data, communications and transactions. Smart chip-based credentials equip people to use their identities safely, quickly and widely and trust that their personal information remains private.

Conclusion

As the use of unique identifiers increase, the risk of identity exploitation from the misuse of personal identity information increases and requires actions on the part of policy makers to protect individuals. Commercial entities need to create a trust model and information policies to ensure that individuals who own these unique identifiers are protected. (For example, any modification to personal information should trigger a communication to the individual to whom the information is pointing.) Smart chip-based credentials are proven and ubiquitous tools that protect personal identifiers and personal information. As policy makers look to solve the growing problem of identity theft and enable new services that require unique identifiers, smart chip technology should be used to protect personal identity information and allow individuals a greater level of control of the use of this information.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology.

Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.