

Position Paper

Using Strong Authentication for Preventing Identity Theft

Robert Pinheiro Consulting LLC

Better identity authentication has been proposed as a potential solution not only to identity theft, but also as a way to prevent thieves who steal passwords and other sensitive information from being able to perpetrate “account takeover”; that is, using the information to break into other people’s online banking and other accounts.

There is, however, a key difference between authentication for access to existing accounts, and authentication for preventing identity theft. By “identity theft” we specifically mean the unauthorized establishment of a new credit account using someone else’s identity, where someone obtains goods or services but is expected to pay for them at a later date. This could include any number of things that involve impersonating another person, such as:

- opening new credit card accounts,
- obtaining loans,
- establishing new cell phone accounts,
- getting electric, water, or natural gas service in a new house,
- getting medical treatment in a hospital,
- getting insurance,
- etc.

Also included would be the use of someone else’s social security number and birth certificate to get a job. In that case, the “service” would be the new job, and the new job holder would be expected to pay tax on the earnings from that job later on, by filing a tax return.

The difference between authentication for access to existing accounts, and authentication for preventing identity theft, is that authentication for access to existing accounts assumes that credentials have already been issued for subsequent access to the account. These credentials may range from the weak, such as passwords and Personal Identity Numbers (PINs), to the strong, such as cryptographic hardware tokens. Authentication would rely on the use of these credentials for account access.

When a new credit account is being opened, however, the credit grantor may not have a prior relationship with the person whose identity is being used to open the account (who may or may not actually be the person attempting to open the account). In that case, the credit grantor cannot make use of previously-issued credentials to authenticate someone’s identity. Instead, the new account applicant may be required to produce any number of identity documents, including birth certificates, passports, driver’s licenses, utility bills, etc., to establish identity. However, if the new account application is being processed

online, or over the phone, producing such identity documents would not be feasible. In that case, the only alternative is to rely on “knowledge-based” authentication (KBA) to verify the identity claimed by the person opening the new account. KBA is based on answers to questions that presumably could only be answered by the actual person whose identity is being claimed, and not by an imposter. This requires that the credit grantor have access to a source of such questions, and their answers. However, KBA would fail if the identity thief has managed to gain access to the right information, and can answer the questions correctly. With the large number of breaches of personal information maintained in corporate and government databases that we hear so frequently about, not to mention the availability of paper documents and public records containing social security numbers and other personal information, it is quite possible that an identity thief could obtain this information. In addition, each time that KBA is used to verify the identity claimed by someone opening a new account, this “secret” information may become exposed to a greater extent.

We suggest that there are at least two other possible means by which authentication might occur, and identity theft prevented, when new credit accounts are opened online, as follows:

- a. Use a digital certificate presented by the person opening the new account. Such a certificate would contain identity information and be “signed” by a party that the credit grantor trusts, such as a trusted Certificate Authority. The credit grantor can authenticate the claimed identity of the account applicant using the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol for secure communication between the credit grantor’s web server, and the applicant’s web browser. This assumes that the certificate is in the physical possession of the person to whom it was originally issued, that it has been “unlocked” by a password or PIN known only to this person, and that the Certificate Authority has done an adequate job of initially verifying the identity of the certificate holder prior to issuing it.
- b. Rely on a trusted third party to vouch for the identity of the new account applicant. This approach assumes that there is some “Identity Provider” that the credit grantor trusts, and that issues credentials to people that it can use for subsequent identity authentication. It further assumes that this Identity Provider has adequately verified the identity of the person to whom it issues these credentials. During the account opening process, the credit grantor would identify and contact the Identity Provider, and would request the Identity Provider to authenticate the person attempting to open the new account, using previously-issued credentials associated with the identity being claimed. The results of the authentication process are then transmitted by the Identity Provider back to the credit grantor in the form of an electronic identity assertion. Based on these results, the credit grantor decides whether to accept or reject the claimed identity.

Note that both of these alternatives still require that a person initially must establish identity based on paper documents or knowledge-based authentication. The difference is

that this would only have to be done once, and not each time a person must verify his/her identity to open a new credit account.

Proposal

We believe that identity authentication for preventing identity theft could be based either on the use of a digital certificate in the possession of the person claiming a particular identity, or more likely, on reliance on a trusted third party Identity Provider. A major reason to discount the use of digital certificates for identity theft prevention is because these certificates are not commonly issued to ordinary consumers for identification or authentication purposes. If these “client-side” certificates become more widely distributed to individual consumers for the mutual authentication of websites and users, this option would become more feasible. Even in this case, however, the Certificate Authority would need to rigorously verify the identities of those persons to whom it issues certificates.

Although we do not provide details on how trusted Identity Providers could be employed to prevent identity theft, the basic concept is roughly as follows:

1. A person establishes his/her identity with some Identity Provider in a rigorous way. This might include presentation of various physical identity documents, and might also include correct answers to various questions as part of a knowledge-based authentication scheme.
2. Once a person’s identity has been verified, the Identity Provider issues “strong” identity credentials to that person for use in subsequent identity authentication. “Strong” credentials would be something better than passwords or other pieces of information that could be easily compromised. Examples include “hard” or “soft” cryptographic tokens, One-Time Password tokens, and biometrics such as fingerprints, etc.
3. A person claiming some particular identity when opening a new account presents identity information (name, birthdate, social security number, etc) to the credit grantor. The credit grantor determines, in some way, which trusted Identity Provider (if any) has verified that identity and has issued strong credentials for subsequent authentication.
4. The credit grantor contacts the appropriate Identity Provider, and requests that the claimed identity of the new account applicant be authenticated, using credentials associated with the claimed identity.
5. The new account applicant and Identity Provider interact directly, and the applicant is requested to authenticate using the identity credentials issued in conjunction with the claimed identity.

6. The result of the authentication process is transmitted to the credit grantor, using some secure electronic identity assertion message.
7. On the basis of this identity assertion message, the credit grantor decides whether to accept or reject the claimed identity.

Feasibility Issues

For this approach to be feasible, a number of issues must be resolved:

- Identity Providers need to exist and be willing to provide authentication-type services to relying parties such as credit grantors. Potential Identity Providers include banks and other financial institutions, credit bureaus, governmental agencies such as state motor vehicle bureaus and the US Postal Service, and private companies. Financial institutions already verify the identities of new account holders, and issue credentials for ongoing access to those accounts. Motor vehicle bureaus also verify identities and issue credentials, although these credentials (ie, driver's licenses) are not currently useful for online identity authentication. Private companies that issue user IDs and passwords to their customers for online access to their accounts perform these functions to some extent, but upfront identity authentication may be non-existent or weak.
- Identity Providers need to be reasonably protected from liability if they erroneously authenticate an identity, provided that they conform to established standards or accepted practices for identity verification and credential management, and have acted in good faith.
- Standards, or at least clearly-specified recommendations, need to be established for verifying a person's identity. These standards/recommendations may need to be consistent with the eventual requirements of the REAL ID Act's requirements for establishing identity for the purposes of obtaining a REAL ID driver's license or identification card.
- A business model that establishes the incentives for Identity Providers to offer identity authentication services needs to be formulated. Presumably Identity Providers want to be compensated for providing authentication services to credit grantors. The cost of granting credit is incrementally higher today because credit grantors use the services of credit bureaus (for a fee) to verify that applicants have a certain level of creditworthiness. If our society is serious about preventing identity theft, and if better authentication is a viable means of helping to prevent identity theft, the incremental cost of performing these identity checks needs to be acknowledged in the cost of providing credit. Might there even be some economies of scale if a credit check and an identity check could be combined in some way?

- Incentives or regulations must exist so that credit grantors actually use accepted authentication methods to verify a claimed identity before opening new credit accounts. One of the weaknesses of the fraud alerts that consumers can place on their credit files today is that there is no requirement that credit grantors act on those fraud alerts. Government needs to take an active role in making sure that better authentication methods, or other viable methods, are actually used.
- Two of the consequences of identity theft, from the victim's point of view, are that (a) victims may be dunned for payment of bills that they themselves didn't generate, and (b) the victim's credit rating may be ruined due to damaging information reported to credit bureaus by credit grantors who have not been paid, or have received late payments. Perhaps one of the incentives needed to ensure adoption of better ways to prevent identity theft, including better authentication, is to make the ability to pursue collection of unpaid accounts, or to adversely affect a credit rating due to damaging information, contingent upon actually adopting and using these methods.

Relation to Other Initiatives

One existing initiative that appears to have some relation to this proposal is Microsoft's CardSpace. Although CardSpace is not geared specifically to identity theft prevention, it does utilize Identity Providers for issuing "Managed Cards" to consumers for providing identity information, or "metadata" about a person's identity, to relying parties. Might Identity Providers that emerge as issuers of these Managed Cards for CardSpace applications also be viable Identity Providers for identity theft prevention, as outlined in this proposal? Might credit grantors who must authenticate claimed identities also play the role of relying parties in the CardSpace realm, accepting Managed Cards for identity authentication?

Comments welcome.

Bob Pinheiro

Robert Pinheiro Consulting LLC
bp@bobpinheiro.com