



Identity Matters: Taking a Fresh Look at Authentication

Andrea Klein, IdenTrust - 19 Feb 2008

Secure authentication is vital in the world of e-banking, but with malware and trojans designed to obtain your information, corporates need to create an end-to-end identification and authentication infrastructure.

This year is already proving to be a busy one for IT fraud detectives around the globe. The record-setting trading fraud case at France's Bank Societe Generale, which resulted in more than €4.9bn (US\$7bn) in losses, grabbed headlines in January. Just as threatening to individuals and businesses worldwide, however, is the proliferation of increasingly sophisticated man-in-the-middle and man-in-the-browser schemes that target financial transactions. Last month, we learned of a new intrusion program, the Silentbanker trojan. The malware, which has targeted more than 400 banks, is striking in its ability to circumvent two-factor authentication and inject itself into the middle of banking transactions, duping bank customers into sending funds to the fraudsters in what looks like completely valid transactions.

The steady cadence of high-profile reports of security threats and breaches - which have led to unauthorised access to sensitive information and, ultimately, theft - is driving corporations to take a more careful look at the risks inherent in Internet commerce and, more importantly, to rethink the role of identity authentication in their broader security and compliance infrastructure.

It is unnervingly easy for determined fraudsters to change company documentation, names of directors, and even official business addresses without the legitimate company's knowledge. Criminals can then use the documentation to create new accounts and use existing accounts for fraudulent activities without triggering alarm in the legitimate company. In this environment, companies are looking for ways to limit their liability, improve accountability, and standardise their approach to identity authentication across the enterprise and across the financial institutions with which they conduct business.

Feeling Vulnerable?

Corporations and their financial institutions have implemented numerous security measures over the years to address identity issues, but have generally pursued a piecemeal versus an enterprise approach, relying on a series of discrete point solutions that do not provide end-to-end visibility and address only parts of the total threat. For example, two-factor authentication, a frequently deployed identity authentication method that couples a password with another type of identification, has proved to be unsuccessful at thwarting man-in-the-middle attacks when used alone¹. When the link between the user and his/her internet service provider is phished or hacked into, the hacker can insert fraudulent sites into the workflow, collect password and personal information and then use that information to access accounts or commit other identity fraud crimes. Similarly, when fraudsters insert malware in the user's browser through a Trojan horse, confidential information entered into financial services websites is captured and stolen. Through case after case, we've learned that multi-factor authentication did not stop the hackers who cleverly designed programs to circumvent this safeguard.

Authentication - Not Access - is Vital

An important reason why the piecemeal approach has come up short is that most point solutions focus on access versus authentication. Thus, as long as an individual has the appropriate pin/password or token combined with a user name or site key, he or she can gain access to a site or data. This approach has proven to be short-sighted as companies need to understand and vet the way in which credentials are granted before they can rely on them.

Solutions that simply authenticate the site to the user, and not who the user really is - while good first attempts - simply do not guarantee a trusted infrastructure, and only meet basic compliance with domestic and international identity authentication guidelines and regulations.

To provide security on the highest level possible, organisations must perform multi-factor authentication enterprise-wide across all levels, using a comprehensive solution that achieves the following:

1. Integrates various point identity solutions for comprehensive protection.
2. Cross-authenticates the user with the site.

3. Secures the user through a digital certificate, which has been issued only after having been fully vetted.

It is also critical to enable validation of certificates against a real-time updated list that indicates whether or not the certificate has expired or been revoked.

Financial Institution as a Trusted Party

In an end-to-end infrastructure that leverages digital certificates as the vehicle for identity authentication; financial institutions have a unique role and opportunity. They can leverage their position as a trusted third-party in the traditional off-line world and offer new services as a third-party issuer of digital certificates in the online world, simplifying the delivery for customers and eliminating the need to expand the number of parties trusted with personal and confidential information.

Banks are in a unique position to offer these certificates as customers already trust them with their personal and financial information. As such, they can issue the certificates using customer information that they, in many cases, already have on file. Additionally, financial institutions around the world are regulated to perform Know Your Customer (KYC) authentication before opening any type of account, so there is consistency in the way that the authentication is performed. This approach allows corporations to limit how many third-parties have access to their personal information, as financial institutions can rely upon each other and how the authentication was performed. Additionally, since financial institutions are regulated to control the personal information that they collect, corporations can rely upon them as a trusted third party.

Global Considerations

In today's global economy, a comprehensive identity authentication approach must provide protection for corporations as they operate domestically and across international borders. It requires policies and a consistent operational and technology framework that users can rely upon wherever they conduct business. A legal framework that is acceptable domestically and internationally is just as important. Otherwise, a corporation or its financial institution could face the prospect of adjudicating possible disputes in jurisdictions around the world if a security breach arises or a digitally-signed document is not accepted as non-repudiable - an expensive and cumbersome prospect.

Equally important, international interoperability enables the digital identities issued by one financial services organisation to be relied upon - in a standardised way - by financial institutions around the world. This eliminates the need for the corporation to manage multiple identity authentication methods.

The benefits of a comprehensive identity infrastructure built around financial institution-issued digital certificates encompass more than protection from criminals. It also enables organisations to conduct e-business globally, uncover new revenue opportunities and achieve new operational efficiencies, while creating a comprehensive audit trail with full accountability for those transactions.

Such an infrastructure, for example, enables corporations to rely on the authenticity of digital signatures for purchase orders, invoices, compliance, and other documents, and to finally automate the last part of the supply chain. Additionally, using a financial institution issued certificate provides encryption that safeguards the content, ensures document integrity and eliminates pharming (man-in-the-middle or DNS poisoning). Digitally signing these documents replaces 'wet' signatures, provides user-level signatures and enables straight-through processing.

Corporations can also leverage the liability protection offered by financial institutions, providing the confidence to expand business in new directions. Multinational corporations that must manage relationships with financial institutions around the world can open and close accounts, and change signatories electronically and across institutional relationships. Conversely, financial institutions have full confidence that their digital signatures are secure and have not been compromised.

Identity authentication is the new front line in the battle for secure e-commerce. The assurance that both parties in a transaction are secure is essential to thwarting online fraud, which threatens to stop the growth of e-commerce in its tracks. Equally important, companies can ensure that their own transactions between divisions are authenticated and auditable to protect themselves against internal fraud.

Corporates - increasingly aware of the risk - are looking for ways to limit their liability and standardise their approach to identity authentication throughout the enterprise and across the financial institutions with which they conduct business. To achieve this goal, they require an end-to-end identity authentication infrastructure that provides comprehensive production, globally accepted policies, legally binding contracts, and consistency of operations.

¹*Man-in-the-middle attacks occur when a hacker intercepts confidential messaging between a bank and a customer without either party knowing that the link between them has been compromised. The hacker then uses the acquired information - usually a user ID and password - to gain access to the customer account.*
