THERE'S MORE TO ONLINE TRUST THAN SECURITY AND PRIVACY

by

Timothy R.D. Grayson

Trust underlies all business. Typically it is underpinned by credibility, which is in turn the product of a number of factors including reputation and experience. In the online environment particularly, credibility and trust are substantially dependent upon security and privacy. Thus many organizations focus on the quality of their security solutions and privacy procedures. These factors do not by themselves, however, address the fullness of systemic trust that is required to expand online business activity. They are necessary but not sufficient. Independent attestation and mediation, which create a hospitable environment for liability management and transaction non-repudiation, enhance security and privacy thereby extending e-business value. An appropriately positioned third party can provide the missing pieces.

Focus on Security and Privacy

At this stage in the evolution of the online commercial environment, market demands have placed the "trust" focus on security and privacy. They are similar but distinct functions, and must be dealt with by different measures.

Security is about protecting. For centuries physical assets, such as castles, homes, and paper documents, have been protected by barricades, walls, locks, and codes. In a digital world, these perimeters are electronic – PIN/pass, firewalls, encryption – better suiting the protection of digital matter. The concern over safely locking down information assets to the maximum allowable degree is paradoxically constrained by how much it inhibits use of the assets. Perfect security presents perfect inaccessibility, which, given that information's value is in its being used, may in fact reduce the value of the asset. For instance, the networked Web Services-based world of interactivity and direct sharing of data demands that the same digital assets as are being protected must also be widely exposed. Thus, ability to protect information by location-based security measures (i.e., walls, practically and figuratively) is and is continuing to be rapidly and substantially diminished in the digital domain.

The solution for security of digital assets, such as it is, begins with the human factor. Security is always founded on the intents and actions of humans. A lock doesn't work if left open. Similarly, digital assets are impossible to protect without digital-based security systems.

Security will always be a core trust focus for two reasons. First, continual development responds to the persistence and increasing sophistication of the bad guys. Second, privacy and technological development, among other related issues add new constraints on how digital assets are protected. Today's business world is moving toward increasing machine-to-machine transfer and manipulation of valuable information. Security professionals are pressured to find alternate protections in an increasingly open system. Without trying to limit or understate the importance of the cryptography and architectural requirements of proper online security, core security requirements today can be reduced to two areas of concern: *authentication* and *authorization*, collectively falling under the heading of identity management.

Authentication is primary to the practice of good security. It is the first form of determining who or what is allowed clearance. In the real world, we know of security clearances granted for access to sensitive locations and information. A clearance is typically based on a background search of the individual to a sufficient extent to offset the risk and liability in granting the access. The same happens in the digital world prior to granting access. One complication is that outside the enterprise environment, it is difficult to conduct a rigorous initial authentication. Moreover, authentications can be made to varying degrees of strength or proof. For general, non-sensitive Website access, a good faith online registration may be adequate. The next level of scrutiny may be satisfied by a credit card check. To authenticate for a valuable transaction or for access to highly sensitive information may require "strong" credentials only to be granted after an in-person proofing. Authentication is crucial because once authenticated, that identity is presumed to be known. Mistaken authentication can have extraordinary consequences, be it financial losses resulting from identity fraud or negative business effects deriving from security breaches. Moreover, the error is readily exploitable and can be rapidly replicated and perpetuated.

After authentication, online security focuses on authorization. In the simplest terms, authorization is the processing of identity credentials and granting access. It's precisely akin to an immigration control border check that examines the documents (e.g., passport and visa) of a visitor to be assured that the visitor is who (s)he is claiming to be for admission into the country. Online authorizations, however, tend to change more dynamically and impersonally. Access may be granted and then denied to the same identity (e.g., when employment ends), or when the amount and value of an information transaction shifts. While the actual authorization is a mechanical process, the rules by which authorization is granted comprise a complicated policy and administration process. Again, system effectiveness rests in the hands of people.

Security itself is a necessary condition for privacy. It is essential, however, to mark a distinction between the two. In the case of information, security is about the practical protection of data while privacy is about policies and actions to maintain opacity of the resultant information. Privacy is the second major facet of online trust, consistent with the focus on the protection and reclamation of personal privacy in the digital world. It is a hotly contested and widely debated issue in the context of the Internet because of the volume of personal data that is readily available and the velocity at which data can be connected to create information and knowledge about individuals. When information banks were hard copy files and in disparate storage locations, access to data was difficult to both obtain and correlate. Now, information is by necessity much more readily accessible electronically from a wide variety of sources. Obtaining digital data may be difficult – more difficult than, say, getting into a corporate filing room – but once the perimeter is breached more data about more people is more accessible.

Means of addressing privacy concerns consist of regulatory requirements for security technology and procedure along with privacy-controlling process, storage means, and data use. These come in forms as diverse as where and how data is stored, managed, and updated through to what that data can be used for. Privacy matters are being addressed by a multitude of citizens' protection groups and advocates, including government-sanctioned privacy commissioners. But the "owner" of that information is the final arbiter of its use; in Canada the owner of personal information is the person identified by and attached to that information. Because of this focus on privacy, constraints on data use have become ever more stringent and short-term. Blanket permissions to allow data use for an indeterminate time and purpose are no longer adequate. These developing circumstances are forcing businesses and governments to implement more sophisticated processes and procedures to ensure the privacy of all parties.

Obviously there is good cause for a significant emphasis on technical security and privacy measures. There will undoubtedly be an ongoing battle between the several sides of this issue, including businesses and governments seeking to use information, citizens seeking to protect their information and maintain its opacity, governments regulating and monitoring the situation, and the bad guys seeking it for other, nefarious purposes. But, it may be safe to presume that the limits of commercial and non-commercial online activity may presently have been reached in respect of security and privacy constraints. Which is to say that since a core requirement necessary for the Internet to develop further as a meaningful channel of activity is trust, and since the degree of trust that can be created by simple security and privacy measures (as a foundation) have generally been reached, additional facets of trust are required to further develop the commercial Internet.

The Next Focus in the Online Trust Framework

Assume for a moment that the technology and policy/procedure for identity authorization and authentication are resolved to an evolving, but satisfactory, level for the e-business that they can enable. The development of online business remains unfulfilled because the necessary extent of trust and fulfillment of a trust framework is lacking. The level of transactional sophistication will remain relatively trivial because the application of trust to the online model is inadequate for more elaborate and meaningful activity. Regardless of a transaction's value or "importance," a single-iteration transaction, such as the access to a classified directory or the online purchase of a product, is quite trivial. It is a matter of authorizing an authenticated identity for the right to conduct a transaction. The primary liability and trust exists in the authentication and authorization. On the other hand, multi-iterative, multi-identity, and multi-jurisdictional transactions have greater complexity and demand support that was previously unnecessary.

The two foci of the online trust framework that are sure to be next on the e-business agenda are, corresponding to processes and features in the physical world, *attestation* and *mediation*.

Attestation is, online and off, stating the truth as a witness. Attesting is done, for example, when a guarantor signs a passport application; when an auditor signs off on a record. The role of the guarantor is to witness an activity and – independently – verify it. The function keeps all parties honest prior to and even through a transaction dispute. To varying degrees, the act of independent attestation increases the trust *in the system*. It provides added comfort with and certainty in the transaction process and record, so the required degree of trust directly between the interested parties can be lowered.

The online environment presents complications that make attestation even more relevant, not the least of which is that often the parties with interest in a transaction do not meet or even see each other. They are therefore conducting business with a much higher implied trust requirement. Because electronic documents are not presently countersigned by both parties – let alone witnessed – and, in common electronic transport systems there is no definitive arbiter of sending/delivery of communication, there is higher potential for misinterpretation and dispute. For these and other reasons, there is an increased requirement to authenticate the parties' digital credentials that identify them, and to keep time-stamped records of transaction activity. The trust level increases particularly when this function is marked explicitly with a visually identifiable trust mark.

Mediation is the natural next step beyond attestation. It is a trusted third party orchestrating the flow of multi-party, multi-iterative electronic transactions so that an accurate chronicle is maintained. Mediation also implies the activity of the guarantor ultimately bearing witness in the resolution of disputes. The mediator would be aided significantly, and the legal system relieved of substantial burden, if the third party came with or was granted legislative support to exercise its role expeditiously – particularly in the context of dispute resolution.

Collectively attestation and mediation, which rely on the identity security factors noted above (authentication and authorization), provide increased transaction integrity. The very nature of attestation and mediation within a legal context demand they be provided by an independent party. This trusted third party and the functions of attestation and mediation, which require the technological capability to securely archive transactional artifacts in time, are essential for at least two key reasons. First, there is no alternative strong means to introduce and manage a transaction life-cycle, including the prevention of misrepresentation and fraud. Second, without them there exists no means to resolve disputes based on legally-acceptable evidence presented by an independent witness.

To develop out the online commercial space further then, in addition to security and privacy – provided by robust systems and strong identity credentials – a third party that can attest to the identities and the content of the communication between those entities must get in the middle of the transaction. Making this even more challenging, the function has to be executed consistently, persistently, and transparently to the users.

Summary

Currently, "trust" in the online commercial transaction environment in focused on security and privacy. However, as e-business evolves, that focus will be redirected to systemic trust issues, including independent attestation to and arbitration of the integrity of digital identities and transactions.

Timothy Grayson works for Canada Post Corporation, in Ottawa. He is the author of Every Canadian's Guide to Common Contracts *published by HarperCollins. He can be contacted at timothy.grayson@canadapost.ca*