The Laws of Identity

Kim Cameron
Identity and Access Architect
Microsoft Corporation

May 2005

Applies to:
Security
Web development
Web services

Summary: Understand the dynamics causing digital identity systems to succeed or fail in various contexts, expressed as the Laws of Identity. Together these laws define a unifying identity metasystem that can offer the Internet the identity layer it needs. (14 printed pages)

Contents

Problem Statement
Words That Allow Dialogue
The Laws of Identity
Conclusion
For More Information

The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet.

This paper is about how we can prevent the loss of trust and go forward to give Internet users a deep sense of safety, privacy, and certainty about whom they are relating to in cyberspace. Nothing could be more essential if Web-based services and applications are to continue to move beyond "cyber publication" and encompass all kinds of interaction and services. Our approach has been to develop a formal understanding of the dynamics causing digital identity systems to succeed or fail in various contexts, expressed as the Laws of Identity. Taken together, these laws define a unifying identity metasystem that can offer the Internet the identity layer it so obviously requires.

The ideas presented here were extensively refined through the Blogosphere in a wide-ranging conversation documented at www.identityblog.com that crossed many of the conventional fault lines of the computer industry, and in various private communications. In particular I would like to thank Arun Nanda, Andre Durand, Bill Barnes, Carl Ellison, Caspar Bowden, Craig Burton, Dan Blum, Dave Kearns, Dave Winer, Dick Hardt, Doc Searls, Drummond Reed, Ellen McDermott, Eric Norlin, Esther Dyson, Fen Labalme, Identity Woman Kaliya, JC Cannon,

James Kobielus, James Governor, Jamie Lewis, John Shewchuk, Luke Razzell, Marc Canter, Mark Wahl, Martin Taylor, Mike Jones, Phil Becker, Radovan Janocek, Ravi Pandya, Robert Scoble, Scott C. Lemon, Simon Davies, Stefan Brands, Stuart Kwan and William Heath.

Problem Statement

The Internet was built without a way to know who and what you are connecting to.

A Patchwork of Identity "One-Offs"

Since this essential capability is missing, everyone offering an Internet service has had to come up with a workaround. It is fair to say that today's Internet, absent a native identity layer, is based on a patchwork of ***identity one-offs***.

As use of the Web increases, so does users' exposure to these workarounds. Though no one is to blame, the result is pernicious. Hundreds of millions of people have been trained to accept anything any site wants to throw at them as being the "normal way" to conduct business online. They have been taught to type their names, secret passwords, and personal identifying information into almost any input form that appears on their screen.

There is no consistent and comprehensible framework allowing them to evaluate the authenticity of the sites they visit, and they don't have a reliable way of knowing when they are disclosing private information to illegitimate parties. At the same time they lack a framework for controlling or even remembering the many different aspects of their digital existence.

Criminalization of the Internet

People have begun to use the Internet to manage and exchange things of progressively greater real-world value. This has not gone unnoticed by a criminal fringe that understands the ad hoc and vulnerable nature of the identity patchwork—and how to subvert it. These criminal forces have increasingly professionalized and organized themselves internationally.

Individual consumers are tricked into releasing banking and other information through "phishing" schemes that take advantage of their inability to tell who they are dealing with. They are also induced to inadvertently install "spyware" which resides on their computers and harvests information in long term "pharming" attacks. Other schemes successfully target corporate, government, and educational databases with vast identity holdings, and succeed in stealing hundreds of thousands of identities in a single blow. Criminal organizations exist to acquire these identities and resell them to a new breed of innovators expert in using them to steal as much as possible in the shortest amount of time. The international character of these networks makes them increasingly difficult to penetrate and dismantle.

Phishing and pharming are now thought to be one of the fastest growing segments of the computer industry, with an annual compound growth rate (CAGR) of 1000%. (For example, the Anti-Phishing Working Group "Phishing Activity Trends Report" of February 2005 cites an annual monthly growth rate in phishing sites between July through February of 26% per month, which represents a compound annual growth rate of 1600%.) Without a significant change in how we do things, this trend will continue.

It is essential to look beyond the current situation, and understand that if the current dynamics continue unchecked, we are headed toward a deep crisis: the ad hoc nature of Internet identity cannot withstand the growing assault of professionalized attackers.

A deepening public crisis of this sort would mean the Internet would begin to lose credibility and acceptance for economic transactions when it should be gaining that acceptance. But in addition to the danger of slipping backwards, we need to understand the costs of not going forward. The absence of an identity layer is one of the key factors limiting the further settlement of cyberspace.

Further, the absence of a unifying and rational identity fabric will prevent us from reaping the benefits of Web services.

Web services have been designed to let us build robust, flexible, distributed systems that can deliver important new capabilities, and evolve in response to their environment. Such living services need to be loosely coupled and organic, breaking from the paradigm of rigid premeditation and hard wiring. But as long as digital identity remains a patchwork of ad hoc one-offs that must still be hard-wired, all the negotiation and composability we have achieved in other aspects of Web services will enable nothing new. Knowing who is connecting with what is a must for the next generation of cyber services to break out of the starting gate.

It's Hard to Add an Identity Layer

There have been attempts to add more standardized digital identity services to the Internet. And there have been partial successes in specific domains—like the use of SSL to protect connections to public sites; or of Kerberos within enterprises. And recently, we have seen successful examples of federation in business-to-business identity sharing.

But these successes have done little to transform the identity patchwork into a rational fabric extending across the Internet.

Why is it so hard to create an identity layer for the Internet? Mainly because there is little agreement on what it should be and how it should be run. This lack of agreement arises because digital identity is related to context, and the Internet, while being a single technical framework, is experienced through a thousand kinds of content in at least as many different contexts—all of which flourish on top of that underlying framework. The players involved in any one of these contexts want to control digital identity as it impacts them, in many cases wanting to *prevent spillover* from their context to any other.

Enterprises, for example, see their relationships with customers and employees as key assets, and are fiercely protective of them. It is unreasonable to expect them to restrict their own choices or give up control over how they create and represent their relationships digitally. Nor has any single approach arisen which might serve as an obvious motivation to do so. The differing contexts of discreet enterprises lead to a requirement that they be free to adopt different kinds of solutions. Even ad hoc identity one-offs are better than an identity framework that would be out of their control.

Governments too have found they have needs that distinguish them from other kinds of organization. And specific industry clusters—"verticals" like the financial industry—have come to see they have unique difficulties and aspirations when it comes to maintaining digital relationships with their customers.

As important as these institutions are, the individual—as consumer—gets the final say about any proposed cyber identity system. Anything they don't like and won't—or can't—use will inevitably fail. Someone else will come along with an alternative.

Consumer fears about the safety of the Internet prevent many from using credit cards to make online purchases. Increasingly, malware and identity theft have made privacy issues of paramount concern to every Internet user. This has resulted in increased awareness and readiness to respond to larger privacy issues.

As the virtual world has evolved, privacy specialists have developed nuanced and well-reasoned analyses of identity from the point of view of the consumer and citizen. In response to their intervention, legal thinkers, government policy makers, and elected representatives have become increasingly aware of the many difficult privacy issues facing society as we settle cyberspace. This has already led to vendor sensitivity and government intervention, and more is to be expected.

In summary, as grave as the dangers of the current situation may be, the emergence of a *single simplistic digital identity solution* as a universal panacea is not realistic.

Even if a miracle occurred and the various players could work out some kind of broad cross-sector agreement about what constitutes perfection in one country, the probability of extending that universally across international borders would be zero.

An Identity Metasystem

In the case of digital identity, the diverse needs of many players demand that we weave a single identity fabric out of multiple constituent technologies. Although this might initially seem daunting, *similar things have been done many times before as computing has evolved.*

For instance, in the early days of personal computing, application builders had to be aware of what type of video display was in use, and of the specific characteristics of the storage devices that were installed. Over time, a layer of software emerged that was able to provide a set of services abstracted from the specificities of any given hardware. The technology of "device drivers" enabled interchangeable hardware to be plugged in as required. Hardware became "loosely coupled" to the computer, allowing it to evolve quickly since applications did not need to be rewritten to take advantage of new features.

The same can be said about the evolution of networking. At one time applications had to be aware of the specific network devices in use. Eventually the unifying technologies of sockets and TCP/IP emerged, able to work with many specific underlying systems (Token Ring, Ethernet, X.25 and Frame Relay)—and even with systems, like wireless, that were not yet invented.

Digital identity requires a similar approach. We need a **unifying identity metasystem** that can protect applications from the internal complexities of specific implementations and allow digital identity to become loosely coupled. This metasystem is in effect a system of systems that exposes a unified interface much like a device driver or network socket does. That allows one-offs to evolve towards standardized technologies that work within a metasystem framework without requiring the whole world to agree a priori.

Understanding the Obstacles

To restate our initial problem, the role of an identity metasystem is to provide a reliable way to establish who is connecting with what—anywhere on the Internet.

We have observed that various types of systems have successfully provided identification in specific contexts. Yet despite their success they have failed to attract usage in other scenarios. What factors explain these successes and failures? Moreover, what would be the characteristics of a solution that would work at Internet scale? In answering these questions, there is much to be learned from the successes and failures of various approaches since the 1970s.

This investigation has led to a set of ideas called the Laws of Identity. We chose the word "laws" in the scientific sense of *hypotheses about the world—resulting from observation—which can be tested and are thus disprovable*. (We consciously avoided the words "proposition," meaning something proven through logic rather than experiment, and "axiom," meaning something self-evident.) The reader should bear in mind that we specifically did not want to denote legal or moral precepts, nor embark on a discussion of the "philosophy of identity." (All three areas are of compelling interest, but it is necessary to tightly focus the current discussion on matters that are directly testable and applicable to solving the imminent crisis of the identity infrastructure.)

These laws enumerate the set of objective dynamics defining a digital identity metasystem capable of being widely enough accepted that it can serve as a backplane for distributed computing on an Internet scale. As such, each law ends up giving rise to an architectural principle guiding the construction of such a system.

Our goals are pragmatic. When we postulate the Law of User Control and Consent, for example, it is because experience tells us: a system that does not put users in control will—immediately or over time—be rejected by enough of them that it cannot *become and remain* a unifying technology. How this law meshes with values is not the relevant issue.

Like the other laws, this one represents a contour limiting what an identity metasystem must look like—and must not look like—given the many social formations and cultures in which it must be able to operate. Understanding the laws can help eliminate a lot of doomed proposals before we waste too much time on them.

The laws are testable. They allow us to predict outcomes, and we have done so consistently since proposing them. They are also objective, i.e., they existed and operated before they were formulated. That is how the Law of Justifiable Parties, for example, can account for the successes and failures of the Microsoft Passport identity system.

The Laws of Identity, taken together, define the architecture of the Internet's missing identity layer.

Words That Allow Dialogue

Many people have thought about identity, digital identities, personas, and representations. In proposing the laws we do not expect to close this discussion. However, in keeping with the pragmatic goals of this exercise we define a vocabulary that will allow the laws themselves to be understood.

What is a Digital Identity?

We will begin by defining a digital identity as *a set of claims made by one digital subject about itself or another digital subject*. We ask the reader to let us define what we mean by a digital subject and a set of claims before examining this further.

What Is a Digital Subject?

The Oxford English Dictionary (OED) defines a *subject* as:

"A person or thing that is being discussed, described or dealt with."

So we define a digital subject as:

"A person or thing represented or existing in the digital realm which is being described or dealt with."

Much of the decision-making involved in distributed computing is the result of "dealing with" an initiator or requester. And it is worth pointing out that the digital world includes many subjects that need to be "dealt with" other than humans, including:

- Devices and computers (which allow us to penetrate the digital realm in the first place)
- Digital resources (which attract us to it)
- Policies and relationships between other digital subjects (e.g., between humans and devices or documents or services)

The OED goes on to define *subject*, in a philosophical sense, as the "central substance or core of a thing as opposed to its attributes." As we shall see, "attributes" are the things expressed in *claims*, and the subject is the central substance thereby described.

(We have selected the word *subject* in preference to alternatives such as "entity," which means "a thing with distinct and independent existence." The independent existence of a *thing* is a moot point here—it may well be an aspect of something else. What matters is that a relying party is dealing with the *thing* and that claims are being made about it.)

What Is a Claim?

A claim is:

"An assertion of the truth of something, typically *one which is disputed or in doubt*."

Some examples of claims in the digital realm will likely help:

- A claim could just convey an identifier—for example, that the subject's student number is 490-525, or that the subject's Windows name is REDMOND\kcameron. This is the way many existing identity systems work.
- Another claim might assert that a subject knows a given key—and should be able to demonstrate this fact.
- A set of claims might convey personally identifying information—name, address, date of birth and citizenship, for example.
- A claim might simply propose that a subject is part of a certain group—for example, that she has an age less than 16.
- And a claim might state that a subject has a certain capability—for example, to place orders up to a certain limit, or modify a given file.

The concept of "being in doubt" grasps the subtleties of a distributed world like the Internet. Claims need to be subject to evaluation by the party depending on them. The more our networks are federated and open to participation by many different subjects, the more obvious this becomes.

The use of the word *claim* is therefore more appropriate in a distributed and federated environment than alternate words such as "assertion," which means "a confident and forceful statement of fact or belief." (OED) In evolving from a closed domain model to an open, federated model, the situation is transformed into one where the party making an assertion and the party evaluating it may have a complex and even ambivalent relationship. In this context, assertions need always be subject to doubt—not only doubt that they have been transmitted from the sender to the recipient intact, but also doubt that they are true, and doubt that they are even of relevance to the recipient.

Advantages of a Claims-Based Definition

The definition of digital identity employed here encompasses all the known digital identity systems and therefore allows us to begin to unify the *rational elements of our patchwork* conceptually. It allows us to define digital identity for a metasystem embracing *multiple implementations and ways of doing things*.

In proffering this definition, we recognize it does not jibe with some widely held beliefs—for example, that within a given context, identities have to be unique. Many early systems were built with this assumption, and it is a critically useful assumption in many contexts. The only error is in thinking it is mandatory for all contexts.

By way of example, consider the relationship between a company like Microsoft and an analyst service that we will call *Contoso Analytics*. Let's suppose Microsoft contracts with Contoso Analytics so *anyone from Microsoft* can read its reports on industry trends. Let's suppose also that Microsoft doesn't want Contoso Analytics to know exactly *who* at Microsoft has what interests or reads what reports.

In this scenario we actually *do not want to employ* unique individual identifiers as digital identities. Contoso Analytics still needs a way to ensure that only valid customers get to its reports. But in this example, digital identity would best be expressed by *a very limited claim*—the claim that the *digital subject currently accessing the site is a Microsoft employee*. Our claims-based approach succeeds in this regard. It permits one digital subject (Microsoft Corporation) to assert things about another digital subject without using any unique identifier.

This definition of digital identity calls upon us to separate cleanly the presentation of claims from the provability of the link to a real world object.

Our definition leaves the evaluation of the usefulness (or the truthfulness or the trustworthiness) of the claim to the relying party. The truth and possible linkage is not *in* the claim, but results from the evaluation. If the evaluating party decides it should accept the claim being made, then this decision just represents a further claim about the subject, this time made by the evaluating party (it may or may not be conveyed further).

Evaluation of a digital identity thus results in a simple transform of what it starts with—again producing in a set of claims made by one digital subject about another. Matters of trust, attribution, and usefulness can then be factored out and addressed at a higher layer in the system than the mechanism for expressing digital identity itself.

The Laws of Identity

We can now look at the seven essential laws that explain the successes and failures of digital identity systems.

1. User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent. (Blogosphere discussion starts here...)

No one is as pivotal to the success of the identity metasystem as the individual who uses it. The system must first of all appeal by means of convenience and simplicity. But to endure, it must earn the user's trust above all.

Earning this trust requires a holistic commitment. The system must be designed to put the user in control—of what digital identities are used, and what information is released.

The system must also protect the user against deception, verifying the identity of any parties who ask for information. Should the user decide to supply identity information, there must be no doubt that it goes to the right place. And the system needs mechanisms to make the user aware of the purposes for which any information is being collected.

The system must inform the user when he or she has selected an identity provider able to track Internet behavior.

Further, it must reinforce the sense that the user is in control regardless of context, rather than arbitrarily altering its contract with the user. This means being able to support user consent in enterprise as well as consumer environments. It is essential to retain the paradigm of consent even when refusal might break a company's conditions of employment. This serves both to inform the employee and indemnify the employer.

The Law of User Control and Consent allows for the use of mechanisms whereby the metasystem remembers user decisions, and users may opt to have them applied automatically on subsequent occasions.

2. Minimal Disclosure for a Constrained Use

The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution. (Starts here...)

We should build systems that employ identifying information on the basis that a breach is always possible. Such a breach represents a risk. To mitigate risk, it is best to acquire information only on a "need to know" basis, and to retain it only on a "need to retain" basis. By following these practices, we can ensure the least possible damage in the event of a breach.

At the same time, the value of identifying information decreases as the amount decreases. A system built with the principles of information minimalism is therefore a less attractive target for identity theft, reducing risk even further.

By limiting use to an explicit scenario (in conjunction with the use policy described in the Law of Control), the effectiveness of the "need to know" principle in reducing risk is further magnified. There is no longer the possibility of collecting and keeping information "just in case" it might one day be required.

The concept of "least identifying information" should be taken as meaning not only the fewest number of claims, but the information least likely to identify a given individual across multiple contexts. For example, if a scenario requires proof of being a certain age, then it is better to acquire and store the age category rather than the birth date. Date of birth is more likely, in association with other claims, to uniquely identify a subject, and so represents "more identifying information" which should be avoided if it is not needed.

In the same way, unique identifiers that can be reused in other contexts (for example, drivers' license numbers, Social Security Numbers, and the like) represent "more identifying information" than unique special-purpose identifiers that do not cross context. In this sense, acquiring and storing a Social Security Number represents a much greater risk than assigning a randomly generated student or employee number.

Numerous identity catastrophes have occurred where this law has been broken.

We can also express the Law of Minimal Disclosure this way: aggregation of identifying information also aggregates risk. To minimize risk, minimize aggregation.

3. Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. (Starts here...)

The identity system must make **its user** aware of the party or parties with whom she is interacting while sharing information.

The justification requirements apply both **to the subject who is disclosing** information and the **relying party who depends on it**. Our experience with Microsoft Passport is instructive in this regard. Internet users saw Passport as a convenient way to gain access to MSN sites, and those sites were happily using Passport—to the tune of over a billion interactions per day. However, it did not make sense to most non-MSN sites for Microsoft to be involved in their customer relationships. Nor were users clamoring for a single Microsoft identity service to be aware of all their Internet activities. As a result, Passport failed in its mission of being an identity system for the Internet.

We will see many more examples of this law going forward. Today some governments are thinking of operating digital identity services. It makes sense (and is clearly justifiable) for people to use government-issued identities when doing business with the government. But it will be a cultural matter as to whether, for example, citizens agree it is "necessary and justifiable" for government identities to be used in controlling access to a family wiki—or connecting a consumer to her hobby or vice.

The same issues will confront intermediaries building a trust fabric. The law is not intended to suggest limitations of what is possible, but rather to outline the dynamics of which we must be aware.

We know from the Law of Control and Consent that the system must be predictable and "translucent" in order to earn trust. But the user needs to understand *whom she is dealing with* for other reasons, as we will see in the Law of Human Integration. In the physical world we are able to judge a situation and decide what we want to disclose about ourselves. This has its analogy in digital justifiable parties.

Every party to disclosure must provide the disclosing party with a policy statement about information use. This policy should govern what happens to disclosed information. One can view this policy as defining "delegated rights" issued by the disclosing party.

Any use policy would allow all parties to cooperate with authorities in the case of criminal investigations. But this does not mean the state is party to the identity relationship. Of course, this should be made explicit in the policy under which information is shared.

4. Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles. (Starts here...)

Technical identity is always asserted with respect to some other identity or set of identities. To make an analogy with the physical world, we can say identity has direction, not just magnitude. One special "set of identities" is that of all other identities (the public). Other important sets exist (for example, the identities in an enterprise, an arbitrary domain, or a peer group).

Entities that are public can have identifiers that are invariant and well known. These public identifiers can be thought of as beacons—emitting identity to anyone who shows up. And beacons are "omni-directional" (they are willing to reveal their existence to the *set of all other identities*).

A corporate Web site with a well-known URL and public key certificate is a good example of such a public entity. There is no advantage—in fact there is a great disadvantage—in changing a public URL. It is fine for every visitor to the site to examine the public key certificate. It is equally acceptable for everyone to know the site is there: its existence is public.

A second example of such a public entity is a publicly visible device like a video projector. The device sits in a conference room in an enterprise. Visitors to the conference room can see the projector and it offers digital services by advertising itself to those who come near it. In the thinking outlined here, it has an omni-directional identity.

On the other hand, a consumer visiting a corporate Web site is able to use the identity beacon of that site to decide whether she wants to establish a relationship with it. Her system can then set up a "unidirectional" identity relation with the site by selecting an identifier for use with that site and no other. A unidirectional identity relation with a different site would involve fabricating a completely unrelated identifier. Because of this, there is *no correlation handle emitted* that can be shared between sites to assemble profile activities and preferences into super-dossiers.

When a computer user enters a conference room equipped with the projector described above, its omni-directional identity beacon could be utilized to decide (as per the Law of Control) whether she wants to interact with it. If she does, a short-lived unidirectional identity relation could be established between the computer and the projector—providing a secure connection while divulging the least possible identifying information in accordance with the law of minimal disclosure.

Bluetooth and other wireless technologies have not so far conformed to the Law of Directed Identity. They use public beacons for private entities. This explains the consumer backlash innovators in these areas are currently wrestling with.

Public key certificates have the same problem when used to identify individuals in contexts where privacy is an issue. It may be more than coincidental that certificates have so far been widely used when in conformance with this law (i.e., in identifying public Web sites) and generally ignored when it comes to identifying private individuals.

Another example involves the proposed usage of RFID technology in passports and student tracking applications. RFID devices currently emit an omni-directional public beacon. This is not appropriate for use by private individuals.

Passport readers are public devices and therefore should employ an omni-directional beacon. But passports should only respond to trusted readers. They should not be emitting signals to any eavesdropper that identify their bearers and peg them as nationals of a given country. Examples have been given of unmanned devices that could be detonated by these beacons. In California we are already seeing the first legislative measures being taken to correct abuse of identity directionality. It shows a failure of vision among technologists that legislators understand these issues before we do.

5. Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers. (Starts here...)

It would be nice if there were one way to express identity. But the numerous contexts in which identity is required won't allow it.

One reason there will never be a single, centralized monolithic system (the opposite of a metasystem) is because the characteristics that would make any system ideal in one context will disqualify it in another.

It makes sense to employ a government issued digital identity when interacting with government services (a single overall identity neither implies nor prevents correlation of identifiers between individual government departments).

But in many cultures, employers and employees would not feel comfortable using government identifiers to log in at work. A government identifier might be used to convey taxation information; it might even be required when a person is first offered employment. But the context of employment is sufficiently autonomous that it warrants its own identity, free from daily observation via a government-run technology.

Customers and individuals browsing the Web meanwhile will in many cases want higher levels of privacy than is likely to be provided by any employer.

So when it comes to digital identity, it is not only a matter of having identity providers run by *different parties* (including individuals themselves), but of having identity systems that offer *different (and potentially contradictory) features.*

A universal system must embrace differentiation, while recognizing that each of us is simultaneously—and in different contexts—a citizen, an employee, a customer, and a virtual persona.

This demonstrates, from yet another angle, that different identity systems must exist in a ***metasystem***. It implies we need a simple encapsulating protocol (a way of agreeing on and transporting things). We also need a way to surface information through a unified user experience that allows individuals and organizations to select appropriate identity providers and features as they go about their daily activities.

The universal identity metasystem must not be another monolith. It must be polycentric (federation implies this) and also polymorphic (existing in different forms). This will allow the *identity ecology* to emerge, evolve, and self-organize.

Systems like RSS and HTML are powerful because they carry any content. We need to see that identity itself will have several—perhaps many—contexts, and yet can be expressed in a metasystem.

6. Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks. (Starts here...)

We have done a pretty good job of securing the channel between Web servers and browsers through the use of cryptography—a channel that might extend for thousands of miles. But we have failed to adequately protect the two or three foot channel between the browser's display and the brain of the human who uses it. This immeasurably shorter channel is the one under attack from phishers and pharmers.

No wonder. What identities is the user dealing with as she navigates the Web? How understandably is identity information conveyed to her? Do our digital identity systems interface with users in ways that objective studies have shown to work? Identity information currently takes the form of certificates. Do studies show certificates are meaningful to users?

What exactly are we doing? Whatever it is, we've got to do it better: the identity system must extend to and integrate the human user.

Carl Ellison and his colleagues have coined the term 'ceremony' to describe interactions that span a mixed network of human and cybernetic system components—the full channel from Web server to human brain. A ceremony goes beyond cyber protocols to ensure the integrity of communication with the user.

This concept calls for profoundly changing the user's experience so it becomes predictable and unambiguous enough to allow for informed decisions.

Since the identity system has to work on all platforms, it must be safe on all platforms. The properties that lead to its safety can't be based on obscurity or the fact that the underlying platform or software is unknown or has a small adoption.

One example is United Airlines' Channel 9. It carries a live conversation between the cockpit of one's plane and air traffic control. The conversation on this channel is very important, technical, and focused. Participants don't "chat"—all parties know precisely what to expect from the tower and the airplane. As a result, even though there is a lot of radio noise and static, it is easy for the pilot and controller to pick out the exact content of the communication. When things go wrong, the broken predictability of the channel marks the urgency of the situation and draws upon every human faculty to understand and respond to the danger. *The limited semiotics of the channel mean there is very high reliability in communications.*

We require the same kind of bounded and highly predictable ceremony for the exchange of identity information. A ceremony is not a "whatever feels good" sort of thing. It is predetermined.

But isn't this limitation of possibilities at odds with our ideas about computing? Haven't many advances in computing come about through ambiguity and unintended consequences that would be ruled out in the austere light of ceremony?

These are valid questions. But we definitely don't want unintended consequences when figuring out who we are talking to or what personal identification information to reveal**.**

The question is how to achieve *very high levels of reliability* in the communication between the system and its human users. In large part, this can be measured objectively through user testing.

7. Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Let's project ourselves into a future where we have a number of contextual identity choices. For example:

- **Browsing**: a self-asserted identity for exploring the Web (giving away no real data)
- **Personal**: a self-asserted identity for sites with which I want an ongoing but private relationship (including my name and a long-term e-mail address)

- **Community**: a public identity for collaborating with others
- **Professional**: a public identity for collaborating issued by my employer
- **Credit card**: an identity issued by my financial institution
- **Citizen**: an identity issued by my government

We can expect that different individuals will have different combinations of these digital identities, as well as others.

To make this possible, we must "thingify" digital identities—make them into "things" the user can see on the desktop, add and delete, select and share. (We have chosen to "localize" the more venerable word "reify".) How usable would today's computers be had we not invented icons and lists that consistently represent folders and documents? We must do the same with digital identities.

What type of digital identity is acceptable in a given context? The properties of potential candidates will be specified by the Web service from which a user wants to obtain a service. Matching thingified digital identities can then be displayed to the user, who can select between them and use them to understand what information is being requested. This allows the user to control what is released.

Different relying parties will require different kinds of digital identities. And two things are clear:

- A single relying party will often want to accept more than one kind of identity, and
- A user will want to understand his or her options and select the best identity for the context

Putting all the laws together, we can see that the request, selection, and proffering of identity information must be done such that the channel between the parties is safe. The user experience must also prevent ambiguity in the user's consent, and understanding of the parties involved and their proposed uses. These options need to be consistent and clear. Consistency across contexts is required for this to be done in a way that communicates unambiguously with the human system components.

As users, we need to see our various identities as part of an **integrated** world that nonetheless respects our need for independent contexts.

Conclusion

Those of us who work on or with identity systems need to obey the **Laws of Identity**. Otherwise, we create a wake of reinforcing side effects that eventually undermine all resulting technology. The result is similar to what would happen if civil engineers were to flaunt the law of gravity. By following them we can build a unifying identity metasystem that is universally accepted and enduring.

For More Information

Microsoft's Vision for an Identity Metasystem whitepaper

Join the identity discussion at http://www.identityblog.com/