HAVE Identities Before You MANAGE Them

Authenticity and Accountability in Identity-Critical Environments

Reliable Identities, Inc.
Identity is the foundation of security™

Have identities before you manage them

As networks and digital assets become more critical to an enterprise, users of those networks and assets come from more diverse places.

Security and manageability have become more elusive as available technology has become more powerful.

Telecommuters have made personal devices a part of corporate networks, bringing anyone with access to that device inside the company.

Inauthenticity, starting with the sharing of credentials, infests all networks. And inauthenticity anywhere in the network makes the entire network less trustworthy and therefore less useful.

Identity is the support beam of information architecture

Identity and Access Management (IAM) – the application of identity records in an information infrastructure – is a well -developed discipline. As described in the literature of Identity and Access Management, its various parts can be grouped into two categories:

- Provisioning of identities
- Application of provisioned identities to information infrastructures

IAM is often deployed by companies for reasons that have more to do with efficiency and economy than security. Allowing new employees to be productive right away by provisioning information resources can quickly justify the investment in deployment of IAM software and services.

Beyond the efficiencies related to personnel changes, reliable management of identities introduces new levels of security and manageability with potential cost reduction.

Old identity assumptions

In the current IAM framework, provisioning is identified as the beginning of the identity management process. Provisioning is, in short, the filling in of user data into the identity management system, so that it can act as a proxy for the user in applications. The traditional assumptions of provisioning are:

- Available identities are sufficiently reliable for all purposes
- An identity is a manifestation of a relationship
- Rules and their enforcement prevent sharing of identity credentials
- Identity management starts with provisioning

Let's examine those assumptions.

Assumption: Available identities are sufficiently reliable for all purposes

This might be a safe assumption, in the case of the single office of a very small, well-established firm consisting only of long-term employees working in one location.

As we consider larger organizations, where contractors, consultants, and outside personnel connect from multiple locations, the notion of reliable identities begins to elude us. This happens long before we start to consider federated identities and circles of trust, which exacerbate the problem of unreliable identities.

Assumption: An identity is a manifestation of a relationship

Relationships change. People get transferred, promoted, assigned from newly acquired subsidiaries, go from full-time to part-time and vice versa. As long as a staff function is dedicated to

keeping identity records up to date, relationship-based credentials can be made workable, if not efficient.

> ***The propensity of people to subvert the security of an information system is proportional to the value to be gained by doing so.***

As long as nothing important is going on in your network, you needn't worry about the reliability of the identity credentials relied upon nor the identities they represent. If you feel your network needs to grow in importance, then you should look at the quality of the identities underneath its access credentials.

Assumption: Rules and their enforcement prevent sharing of identity credentials

If a newly assigned project team member needs access to a file to meet a deadline, we can expect the sharing of credentials to occur in order for the deadline to be met. Usernames and passwords are routinely shared in such situations, despite policies with stern penalties for doing so. It's how work gets done.

Speed of credential issuance is one of the motivating factors in the adoption of Identity and Access Management. Yet even when the issuance of typical relationship-based credentials is quick and efficient, usernames and passwords still get shared, typically when users and their managers don't see eye-to-eye on what permissions are needed to perform a task.

Now, suppose the access credential were the employee's bank ATM card. What would happen if a new team member asked to borrow his colleague's card and PIN? Of course he would never make such a preposterous request. The uncomfortable truth is that a credential protecting only your company's assets is treated more casually than one that protects the user's own assets.

Therefore, a credential that has a degree of universality is inherently superior to a credential that only represents a single relationship, as between employer and employee.

Assumption: Identity management starts with provisioning

Provisioning a directory is roughly synonymous with populating it. Filling it in. Pouring names and usernames into it. Picture the contents of a truck full of identity information being dumped into a bin and you have a metaphor for the process of provisioning.

A current theme in information security journalism concerns the erosion of the network perimeter. With increasing numbers of mobile users, rogue wireless access points, telecommuters, and USB connections to assorted "outdoor" spaces, the whole notion of a perimeter isolating the company network from the Internet is withering fast. In many ways, it's all Internet.

The headlines are full of accounts of breaches where millions of credit card numbers and other personally identifiable information found their way into the wrong hands, causing disastrous levels of brand damage and cost to the owners of the files.

A sound approach to identity and access management starts not with the traditional provisioning "dump" of user information into the system, but rather with an assessment of the degree of *identity quality* needed for each group of digital assets and for each group of users needing to access that group of assets. The next step is enrollment, or the establishment of identities with the requisite level of reliability.

If it's broke, fix it.

New assumptions

How then do we develop a better approach to building an identity infrastructure? Let's start with some new assumptions:

- A viable identity infrastructure starts with *identity quality needs assessment*, not provisioning
- Reliable identity management starts with *reliable identities*
- Reliable identities are the product of sound enrollment practices
- Credential sharing and other problems are mitigated when the user owns their own universal credential

To get to our reliable identity management system from here, we must first ask:

Where did our identities come from? What was the enrollment process? Who is liable for consequences of enrollment problems – the enrollment officer? The enrollee? Both?

> ***"If it's broke, fix it."***

If we don't ask the questions we are left with the answer that *the organization that uses the identities* is responsible for problems with them.

The Authenticity™ effect

Identity management implies that there are identities to be managed. Thus we define identity infrastructure:

Identities + Identity Management System

= IDENTITY INFRASTRUCTURE

Reliable identities are essential to a reliable identity infrastructure, and consequently to a reliable *information* infrastructure. Conversely, good management of unreliable identities is a waste of resources.

With identity architecture as the support beam of information architecture, reliable identity is the obvious meter by which an identity management architecture (IMA) is measured.

Good privacy protection is an integral part of a properly designed identity provider system. As you assume the role of relying party, you relieve yourself of that responsibility. By relying upon a user-owned identity provided by an external IdP (Identity Provider) your organization leaves the risks associated with detailed user records with the identity provider.

At the same time, your organization entitles itself to the same kind of user accountability that it enjoys in physical space. Think about it: what would it mean if every employee and every employee of every supplier and distributor, every consultant and contractor, were as accountable for his or her actions on your premises or cloud-based network as he or she is for actions around the physical office? How would security improve if there were no doubt about who touched which file when?

That is *The Authenticity Effect*.

IDQA™

Identity Quality Assurance (IDQA) is a methodology and accompanying API for verifying that an identity credential is appropriate, as measured in each of eight categories, for a given risk profile or protection of a specific set of digital assets.

Identities and identity management are two different things. Measure the credential quality and you can therefore know the *reliability* of the identities in your system.

The eight metrics of Identity Quality™

There are a number of objective and subjective evaluations that contribute to an identity credential's identity quality "score." These are grouped into eight metrics:

Metric 1: Quality of ownership

Does the user have "skin in the game" or are the organization's assets the only ones at risk? If the only reliable way to prevent credential sharing is with credentials that protect the *user's* financial, reputational, and identity assets, then to what extent does the credential protect those personal assets?

Metric 2: Quality of enrollment practices

What type of enrollment procedure was used? Did it involve PII (personally identifiable information – those questions about old addresses, relatives, etc.) corroboration? Was it-face-to-face-notarial or remote? How is the process supervised and audited? How many eyes are watching? Each risk profile and highest protected digital asset value will call for a particular enrollment procedure.

Metric 3: Quality of means of assertion

Does the credential support popular identity protocols such as OpenID, i-Name, Shibboleth, CardSpace, FIDO, SAML assertions, national identity assertion networks? A well-used identity is a more reliable identity, so the more places it can be used the better.

Metric 4: Quality of attesting authority

What source of authority attests to the validity of the assertion of identity? Is the attesting party a certification authority? How reliable are their attestation practices? How is identity status (active vs. revoked) reported: CRL/OCSP or another method?

Metric 5: Quality of other attestations

To what extent do self-sovereign methods support your claim of identity? Do colleagues, employers, and sources of other relationships corroborate the claim of identity? The more acquaintances who are willing to put their own identity quality scores at risk, and the higher *their* scores are, the higher *your* score will be.

Metric 6: Quality of protection of the PEN (private key)

What are the characteristics of the credential and its carrier? Is one key pair used for every-thing, or are different key pairs or simple serial numbers used for different applications? The carrier of the credential is equally important. Some risk-profile / asset-value situations call for two, three, or four factor hardware tokens or a one-time password, while a soft credential in the user's computer or even a record in a directory will suffice for others.

Metric 7: Quality of assumption of liability

If fraud is committed with the use of the credential, who carries the liability? Is that commitment bonded? What are the terms of the bond? What is the source of funds for fulfillment of the bond? Are there caveats or is the commitment absolute, regardless of the circumstances that made the credential available to the perpetrator? To protect assets and processes of the highest value, where a compromised identity would have the most serious consequences, there should be both civil and criminal liability involved in the issuance and ongoing use of the credential. Equally important is protection against fraudulent repudiation. Nonrepudiation is perhaps the most difficult goal for a trust system to achieve, but it is necessary for the system to be useful to relying parties where significant transactions are involved.

Metric 8: Track record of credential

How long has the credential been used without apparent problems? How many transactions and authentications has it been used for? Evidence of nonduplication can be added — assurance that a new credential has not been

created to avoid accountability for acts under a previous credential.

Levels of security

Different workgroups and applications have varying requirements for security, assurance of authenticity, and manageability. For example, a judge responding via secure PDA to a police detective's request for a warrant may require three-factor authentication, while a warehouse data entry function may be just fine with usernames and passwords assigned in the provisioning step.

Criteria for required level of security may include (among many others):

- Degree of financial risk
- Characteristics and degree of non-financial risk
- Requirement for non-repudiation
- Duration of assignment

Applying IDQA

Consider changing your enterprise's role in the identity infrastructure – leaving the role of IDP (Identity Provider) to an outsourcer, and becoming a PRP (Principal Relying Party). This will have the following effects:

- Since users own their credentials, they are responsible for their own password resets – making it *their* job, not yours, to maintain a working identity credential
- End the sharing of identity credentials
- End credential revocation problems at termination
- Have the benefit of clear liability assumption by the Identity Provider

Micro-segmentation and digital asset management

These are the right approach, but if there's not complete confidence in the identities of those touching those segments and assets, then those practices will not produce the security you need.

Conclusions

An IDQA™ assessment, combined with a change in your role from Identity Provider to Principal Relying Party, will make your identity infrastructure more workable. In turn, your enterprise's whole information infrastructure will become more manageable, more economical, and more secure.

To bring the benefits of a *reliable identities* infrastructure to your enterprise, please get in touch with Reliable Identities, Inc.