Wireless LANs must be properly configured and tightly secured, whether in the office or at an employee's home. Sensible guidelines must be issued to all staff regarding the risks of using wireless hotspots and Internet cafes. The organization must ensure that all remote access is secured using VPNs and that no sensitive traffic, including email, is transmitted anywhere in the clear.

A process and policy should exist to ensure that all hard disks, CDs and other media are physically destroyed rather than recycled or simply thrown away. A recent survey of 100 hard disks purchased on eBay and at car boot sales showed around 40% had sensitive data easily recoverable and a further 40% had not even been formatted.

Implement strong authentication for all remote users and for all privileged users and accounts. There are many two-factor alternatives to the traditional password, including SecurID, Smart Cards, smart USB keys and even mobile phone SMS texts.

Institute thorough end-user training on secure communications, including what can be discussed over the telephone, what can be discussed outside the building and what can be written in an email. Try not to use e-mail notification or voicemails when away from the office - it sets up the replacement as a target. And most importantly, ensure everyone knows how to report an incident and to whom – most people do not.

> **"Strengthen your helpdesk password reset process"**

Strengthen your helpdesk password reset process. Permit password resets only with call-back and PIN authentication or some other form of cross-verification. Implement incident reporting and response procedures for all help desk staff, together with clear escalation procedures for everyone in the incident chain. Help desk staff should be encouraged to withhold support when a call does not feel right. In other words "just say no ….."

To adapt Tony Blair's mantra 'Education, education, education,' organizations must place priority on 'Training, training, training'. Train all employees - everyone has a role in protecting the organization and their own jobs. If someone tries to threaten them or confuse them, it should raise a red flag. Train new employees as they start. Give extra security training to security guards, help desk staff, receptionists and telephone operators, all of whom have a vital role to play in blocking identity theft. Make sure you keep the training up to date and relevant.

Finally, have a security assessment test performed and heed the recommendations. Test the company's ability to protect its environment, its ability to detect the attack and its ability to react and repel the attack. Have the first test performed when the company is expecting it, then do a blind test the second time around.

About the author

Peter Wood is Chief of Operations at First Base Technologies, an ethical hacking firm based in the UK. He founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas spanning network security reviews, firewall penetration testing and policy and procedures.

The case for federated identity

Roger K. Sullivan, VP, Oracle; Chair, Liberty Alliance Conformance Expert Group

Roger K. Sullivan

More than 80 years ago, a reporter asked the infamous thief Willy Sutton why he robbed banks. Sutton's reply was, "Because that's where the money is, stupid." Today, the money is in information and there's a lot of information out there - vulnerable in databases, exposed in transactions and circulating on the Web - helping to make identity theft the fastest growing crime in the world. Organizations across the globe are quickly learning that one of the best ways to prevent identity theft is through 'federation'.

A federated framework or model makes it extremely difficult to steal private information and directly mitigates against a wide range of attacks. To understand how federation works, it's important to first step back and look at how information is organized and stored. Today most organizations have disparate proprietary applications, data repositories and identities in use within applications (stovepipes). Every large enterprise knows that these stovepipes are difficult to integrate within a specific organization, let alone among outside trading partners.

Liberty Alliance's approach to free exchange

Enter the Liberty Alliance, an organization representing 150 leading banks, technology companies, wireless providers and government agencies from around the world. Liberty Alliance has designed standards, specifications and a framework that enable organizations to securely interoperate with their partners and customers by leveraging federated identity to establish "Circles of Trust" among different Web sites, intranets and other points of electronic platform contact. A Circle of Trust represents a business relationship formed by organizations to allow them to share identity information seamlessly and based on the privacy guidelines established by the end user.

In the federated identity model, a consumer or an enterprise designates who they want to communicate with (their own personal Circle of Trust) and to what degree. In this model, they input a password once. Their credentials—but not their private identity information—are then shared among the Circle of Trust members. This way, the consumer or enterprise can move from trusted site to trusted site without having to key in password or identity information over and over again.

> “Federation is the opposite of a centralized identity management model”

Circles of trust

A Circle of Trust is usually composed of a group of service providers who share linked identities and who have pertinent business agreements in place regarding how to do business and interact with identity providers. Once a user has been authenticated by a Circle of Trust identity provider, that individual can be easily recognized and take part in relationships with other service providers within the Circle of Trust. A trusts B. B trusts C so A trusts C, and so on.

For example, every airline has an affinity programme and wants to offer premier services – as well as ease of use to its customers so as to create a more ‘sticky’ customer relationship. With federation, a customer could gain access to multiple travel-related services (cars, hotels, insurance, etc…) via one airline site. Similarly, a travel agent could provide an opportunity to link to whatever provider (preferred choice) is offering the best deals – e.g. if the customer never wants to travel on XYZ Airline, she could decline to link with that airline. If she always rent cars from Avis or Dollar, then she only links to those sites. It’s up to the user to set up federated relationships in the way that’s most suitable.

Federation is the opposite of a centralized identity management model, which creates a centralized store of information and, as such, a single point of failure. In the federated model, each service provider recognizes the individual or organization in whatever way they choose. That identification is then accepted at other points within the Circle of Trust.

Bucking the trend

Currently many enterprises use an identity framework that involves a government-issued common identifier like a social security number. These identifiers are static and portable, and therefore can easily be used at multiple Web sites if they are stolen. The Liberty model approaches the concept of identifying individuals differently by deploying an opaque identifier which improves security and builds in protection against fraud/identity theft. Within the federated model, the Identity Provider establishes a unique opaque identifier for a Principal so that the Principal can make a connection. Consequently, different Service Providers are unable to easily collude to inappropriately share information about a Principal.

Federation resembles the credit card model where the merchant authenticates that the credentials (cards) are valid, but they don’t authenticate the individual nor verify that the individual is credit worthy. Specifically, credit information, social security numbers and other data are not required from store to store to make a credit card transaction.

As long as they call in the card, the merchant is covered and the liability shifts to the credit card issuer. If they don’t authenticate, then the merchant is responsible for the bad debt per the terms of the merchant card agreement. The federation model balances liability for actions among the trading partners and with new identity management technologies in place, provides opportunities for new business initiatives.

Flexibility

The beauty of the Liberty standards and specifications is they enable organizations to engage with partners of all sizes. The flexible applicability of Liberty Alliance technology broadens trading relationships beyond large peer-to-peer business entities to include medium and smaller entities that were once unable to assume the financial burden of large scale “triple A” products, but are nonetheless vital members of the business community.

> “Federation resembles the credit card model”

In addition, the standards are written to be applied across a heterogeneous platform environment - from servers and mainframes to PCs, handheld devices and mobile phones. The aim is to provide business and individuals with the means to conduct transactions whenever and wherever they see fit, using whatever system configuration is most appropriate to their needs.

Liberty has also made the conscious choice to focus on the business side of implementing identity management and identity-based Web services standards. This includes addressing the business imperatives, rules and policies, as well as best practice and liability challenges associated with operating in a federated model.

The organization has a Public Policy Expert Group which provides advice and guidance on enabling privacy functionality with its specifications. Liberty members represent global companies in most major verticals—meaning the technology, policy and business guidelines around privacy that are driven from this group have been developed collaboratively and take into account varying privacy laws across the globe.

How federation works

Federation offers businesses, governments, employees and consumers a secure and convenient way to control identity information. A federated network identity uses a simplified sign-on for users by allowing them to “link” elements of their identity between accounts without centrally storing all of their personal information. This increases security and delivers better identity control. With a federated network identity approach, users authenticate once in a trusted environment while still retaining complete control over their personal information.

Liberty's open identity specifications have been developed based upon the principle that consumers should 1) have choice in what personal information they share and 2) be able to give permission before data is passed on to others.

The goal of an identity thief is to get at identity information, and then use that information for illegal purposes. The more identities a thief can breach, the more profitable the scam. Liberty’s specifications and framework make it extremely difficult to retrieve private information and mitigate against a range of attack types in ten specific ways:

1. Superior security and privacy inherent in transactions among the Principal the Identity Provider, and the Service Provider: Enterprises which adopt the Liberty Alliance specifications for identity federation are adopting standards which have a high level of security and privacy protection built in. As a result, identity interactions which operate under the specifications are also adopting standards which reduce the risk of fraud or security breaches through sniffing, hacking, replay and other common online attack modes. In addition, federation limits the number of Identity Providers vulnerable to breach. One way is that Identity Providers can use (relatively) heavyweight verification methods (multifactor authentication or biometric devices) in order to issue signed assertions – these methods or devices are not available to insiders or hackers that may be able to steal PII (Personally Identifiable Information) from databases. Any Identity Provider will need to provide proof that its security practices are sufficient to the satisfaction of any company accepting its identity assertions. Additionally, fewer Identity Provider may be needed, hence fewer sites with PII .

> **“Critics of the federation model would argue that the ‘linking’ of accounts increases this level of insecurity”**

2. Moving sensitive data from place to place can be eliminated as a security practice: In order to stymie hackers and protect data, many organizations routinely move data and store it in different places. Rather than protecting information this opens up the number of targets and the very act of moving is risky. Federation simply reduces the number of places to those selected by the user and the specifications provide a mechanism to reduce/eliminate theft through security enhancements (encryption, dig-sig, etc.).

3. No single point-of-failure: Since identity and attribute information remains distributed in the identity federation model, there is no common repository - no catastrophic point of failure - in the event of a breach of an entity’s databases. The federated model is the result of a direct agreement between individual companies and does not apply to a transitive relationship. A log-on for a single site is not necessarily useful at other sites, as it would be in the case of a centralized data repository for authentication data. For example, if company A has federated single sign-on (SSO) with company B, and company B has federated SSO with company C, that does not mean that company A has federated SSO with company C. Further, only if the breached site has been accepted as an Identity Provider for federation, is there any risk of this data being useful to gather data from other distributed sites federated to it through the SSO.

4. Permission-based access to attributes: In the Liberty Alliance protocols, access to personal information, or attributes, is permission-based. As a result, in addition to attribute data being distributed, that data may only be accessed with the Principal’s permission. This has two benefits when considering the issue of exposure. First, any given site or resource which the Principal accesses will only have the data required for that application, and not data which is extraneous to that application; this results in limited data exposure at any one site. Secondly, under the most stringent implementation, a Principal may require explicit consent in order to link a new account to the existing SSO, which affords the best opportunity to restrict access in the event of an active attack. The user is in direct control of what information is available to whom at any given time.

5. Single sign-on: One of the problems with protecting online identity is the sheer number of passwords and relationships a user typically has to manage. Passwords are made less secure when users base them on something familiar like a child’s name or a birthday - but this is a trade-off many users make in order to simply remember passwords. To make matters worse, the most commonly used password is still password.

Also using the same password for multiple sites represents an all too common, but totally understandable problem. Once a criminal learns that single password, it represents an open door, or the 'keys to the kingdom'. In addition, with the need to manage so many passwords, users naturally write them down or store them. This opens up the possibility for abuse.

Global single sign-on the ability to go to a single site, log on and from there securely access multiple accounts at disparate sites, is a key feature of the Liberty Alliance protocols. Global single sign-on allows the Principal to rely on a single, secure password, rather than use many different not-so-secure ones, improving security for the on-line user.

6. Reduced reliance on common identifiers like social security numbers: In current security situations, some of the worst compromises occur when a user maintains a common identifier across many domains with differing security levels. This scenario grows more and more likely with the phenomenon of "password and account inflation" – the growth of the number of domains that individuals must "authenticate" into. The three components of this scenario (the common identifier, many domains and gradient levels of security across those domains) combine to be dangerous precisely because the common identifier (credit card, SSN, or in some cases username and password) serves as a gateway into many domains that lack standardization of security.

Critics of the federation model would argue that the "linking" of accounts that occurs in federation increases this level of insecurity. But the linking of accounts in federation actually serves to a) remove the ability of the common identifier to act as a gateway, and b) moves toward standardizing the levels of security across domains. It actually strengthens security.

All SSO communications in the Liberty model use this agreed upon pseudonym. The opaque identifier is valid only within the Circle of Trust and even if it were breached, the partnering companies could create a new one with no negative impact to the Principal. It's useless outside of that single transaction and it's useless outside of the communication of that specific Identity Provider and Service Provider. The credentials are transient and limited to a specific domain. It will not enable identity fraud to occur elsewhere if stolen. Trying to use it elsewhere would be like trying to speak Mongolian to a group of Danes: they'd know you were speaking, but have no idea what you were saying or how to apply it to their conversation.

> **"Around 400 million Liberty-enabled identities and devices will be deployed by the end of 2005"**

7. A way to extend internal business models to external relationships The Liberty Alliance model enables an organization to provide controlled authentication access to only what is needed for the business transaction. This is an important advantage as organizations build technology that keeps the bad guys "out," but lets the good guys "in."

8. Reduced risk through a more balanced authentication management process: Liberty enables an organization to balance authentication management between partners more equitably. Let's say an outside company is managing the assets for an organization's retirement fund. The organization wants to give its employees access to the fund to check their balances and personal information. Providing a list of employees to the retirement fund management company isn't enough. What if an employee quits? What if there are changes to an employee's status? With only a list, the retirement fund company is assuming liability for what people do when they come to the site. This is a risky practice. If the retirement fund company requires some sort of authentication from the individual's current employer before the individual comes to the site, authentication is improved and risk is more fairly shared.

9. Track and close breaches quickly and cleanly: The Liberty Alliance standards specify that the SSO assertion must clearly indicate the Identity Provider (a fact likely logged by the Service Provider). If a Principal claims that activity conducted with a Service Provider was the result of identity theft/fraud originating elsewhere, then the Service Provider can easily determine if the entry point for this disputed activity in their domain was through a federated SSO with a particular Identity Provider or through an authentication performed locally at the Service Provider.

10. Coordinated response to incidents of fraud: The necessity for a business framework with agreements between Identity Providers and Services Providers establishes a basis of trust and cooperation. It is upon this framework that participants can implement procedures for rapid investigation and resolution of identity theft.

Federation in action

Federation represents the most secure and common sense model for doing business on the Internet. It offers organizations a way to 1) shore up their defences, and 2) more easily interact with customers, trading partners, employees and other constituencies.

Several commercial and vendor company members of the Liberty Alliance are aggressively implementing Circles of Trust. These organizations - including AOL, General Motors, Fidelity and Nokia - are able to achieve significant processing efficiencies while mitigating risk. In fact, approximately 400 million Liberty-enabled identities and devices will be deployed by the end of 2005. Today, an organization that has more control over its processes and security is a more attractive business partner. It's that simple.

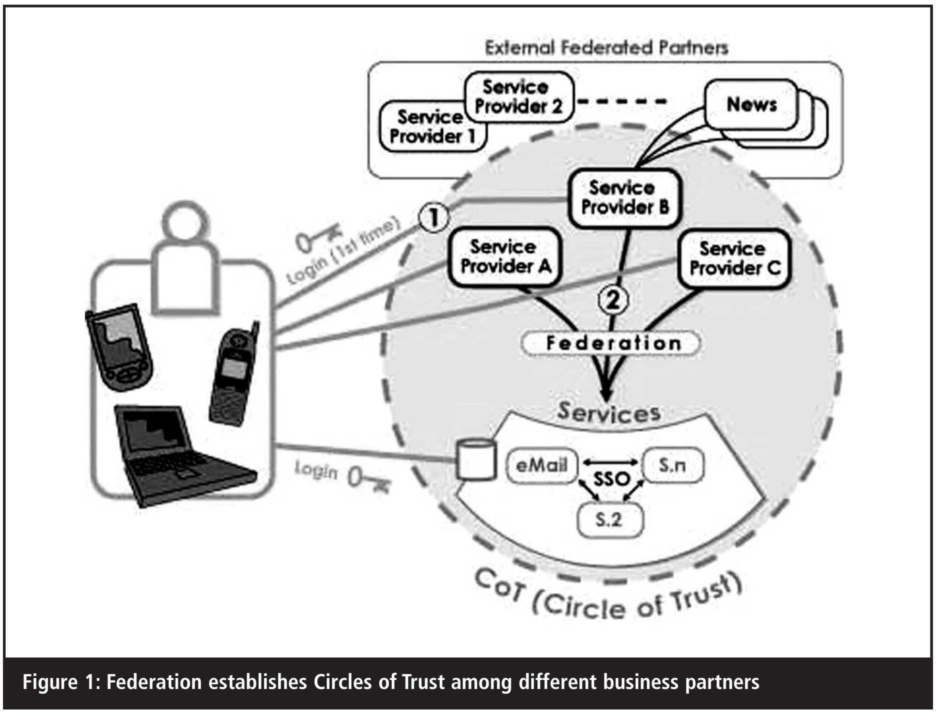

Figure 1: Federation establishes Circles of Trust among different business partners

American Express, a founding member of Liberty Alliance, is using the federated specifications to connect its intranet, Internet and extranet sites. American Express has also taken the lead in using the Liberty specifications to integrate their back-end architecture with the goal to ultimately Liberty-enable their front-facing applications.

Similarly several banks including JPMorgan Chase and Goldman, Sachs are part of a consortium that provides institutional customers investment research and other information from multiple sties. The group is using Liberty's specifications to enable secure sharing and improve interoperability across myriad platforms. The Bond Market Association has rolled out a similar programme.

On the consumer front, AOL is employing Liberty's ID-WSF specifications, particularly the authentication, discovery, permissions-based attribute sharing and security features within the specifications, to enable any consumer to access and personalize their Radio@AOL service using a mobile handset.

Vodafone, one of the world's largest mobile telecommunications network companies is building a Liberty-enabled multiplayer mobile gaming proof-of-concept. Using Liberty as the authentication mechanism, a user can discover a game site over Vodafone's network, access it and personalize his or her experience.

Retirement planning and federation

Today an employee in company A has to go outside the enterprise to access their investment plan at company B. With a federated relationship, that employee can access those investments through a Web portal that shares the employee identity information, and with the employee's permission, federate it with trading partner/investment company B. This is a classic example of B2B2E and one that is being rapidly deployed by mutual fund companies and companies such as Fidelity Investments, an early adopter of Liberty specifications.

But, federation can be initiated from any "side of the street." General Motors, for example, links employee benefits via a portal called MySocrates. MySocrates was originally just a single sign-on portal. It's now being extended to include Liberty Alliance federated relationships among its employee benefits providers. The insurance industry is also actively deploying federation. Nationwide is taking the lead in adopting partner-friendly identity management technologies.

Like most larger insurance companies, Nationwide private labels insurance policies through third parties who may in turn, sell those policies through a network of insurance agents. The more easily they can authenticate everyone in the trading chain using common technical and business standards, the larger market share they can capture.

The future of E-commerce is in identity

Identity security is the issue that will define the future of the Internet. Federation enables organizations to be defensive and gird against identity theft. At the same time that federation enables businesses to explore new and innovative business models, these standards provide mechanisms so that end-users can control their identities. What's more, the federated identity model enables organizations to look beyond the tactical issues of single sign-on, application provisioning and improving one-to-one core trading relationships. The most forward-looking organizations are exploring how digital identity can actually shift their business models and move them out of traditional B2B, B2C and B2E and into B2B2E and other models.

The standards and practices set forth by Liberty fully enable this third party model where identity supports trading relationships and then extends it outward to each partner's representatives. It goes back to the idea that A trusts B. B trusts C so A must trust C too.

The Liberty specifications empower not only business, but also those who use the business services. Identity is central to this empowerment and identity is defining the future of a secure Internet.

About the author

Roger K. Sullivan is Vice President of Business Development for Oracle's Identity Management solutions and serves on Liberty's Management Board and Chair of the Liberty Alliance Conformance Expert Group.