WHITE PAPER

5 Steps to Secure Internet SSO

Overview

This white paper, intended for a management-level audience, describes why and how any organization can implement secure Internet single sign-on with a federated identity management system. Employees today may need to access up to thirty different applications within the enterprise network and over the Internet in the performance of their daily jobs. Most businesses are struggling to secure their internal networked resources while still providing access to external applications, including Software as a Service (SaaS) and other business process outsourcing (BPO) arrangements. Fortunately, there are now standards-based solutions available that provide solid security in such a multi-party environment. The underlying capability is federated identity management, which provides for the portability and interoperability of identity information across organizational boundaries. For the user, federated identity eases access by delivering single sign-on to Internet-based applications, just as if the application were running on the local network. For the CISO, federated identity improves security. For the CIO, federated identity reduces operating costs.

PingIdentity®

Attacks on Enterprise Services

Employees today may need to access up to thirty different applications within the enterprise network and over the Internet in the performance of their daily jobs—often with different usernames and passwords for each one. Such a situation is not only cumbersome; it is inherently insecure, being especially vulnerable to phishing, Trojans and other malware that can quickly spread throughout the entire organization.

Willie Sutton was allegedly asked why he robbed banks; his famous reply, of course, is because "that's where the money is." Software as a Service (SaaS) offerings like Salesforce.com's are now where the money is—at least for many identity thieves. As more applications move outside the enterprise firewall, the number of potential targets increases. Other examples of popular SaaS targets include video conferencing and travel services where either the service itself or some personally-identifiable information (PII) is stolen. Sometimes the theft takes the form of industrial espionage, where the perpetrators attempt to steal customer lists, product plans, and other sensitive or proprietary corporate information.

Every external application creates a potential vulnerability into the enterprise. The more systems there are, the more vulnerable the enterprise becomes. These vulnerabilities come in many forms, but one of the most popular (based on its successful use by hackers) is phishing. Phishing is a technique employed by identity thieves to acquire usernames and passwords, mostly via fraudulent emails. The email appears to be authentic from a legitimate source, and the Website where users are directed may also appear to be authentic. The victims log in unaware that their usernames and passwords are about to be stolen, giving the identity thief access to their actual accounts. Users who log into these fraudulent Websites may also be subject to infection with a trojan that captures keystrokes to discover access credentials for other accounts.

Spear phishing is a special form of phishing targeted at small groups or even at select individuals. Salesforce.com was victimized by such an attack recently when an administrator was phished and his credentials were subsequently used to spear phish specific accounts. In this particular incident, a seemingly trustworthy Microsoft Word document was infected with a Trojan program that captured keystrokes to obtain user credentials.

The phishing incident at Salesforce.com mentioned above was quite well publicized, which can cause a vendor's reputation to suffer substantially. Despite the warning windows provided by Salesforce.com and other SaaS vendors, users continue to become victims. Phishers can be extraordinarily clever, which makes recognizing a phishing email extremely difficult, especially for busy workers who often fail to take the time to scrutinize suspicious emails. This means that even the very best user education programs provide no guarantee of real security.

The impact of phishing on SaaS providers includes:

- **Monetary Loss**
- **Legal Liabilities**
- **Reputational Loss**
- **Time to Resolve**
- **Brand Damage**
- **Competitive Disadvantage**
- **Regulatory Exposures**

Homegrown and Proprietary Security Mechanisms

Organizations that were early adopters of enterprise or Web SSO and outsourcing face an additional risk: insecure proprietary SSO mechanisms. Anyone who wanted to implement SSO over the Internet before 2003 basically had to solve the problem themselves due to a lack of relevant standards and commercial products. Today, some organizations still attempt to build their own proprietary SSO by starting with open source libraries they downloaded from the Internet.

From a security perspective, proprietary SSO projects are subject to numerous pitfalls including:

- A lack of understanding by providers and subscribers alike regarding proprietary SSO mechanisms
- A failure to routinely and accurately analyze information leakage from Web server and proxy logs

- No ability to review the cryptographic mechanisms of external security points
- Inadequate testing of the security software itself
- An inability to implement and/or validate appropriate security controls with solutions that leverage password vaults
- An increased risk associated with delegating authentication to third parties, not knowing how secure user credentials will be
- No plan for protecting against cross-site scripting attacks and the multitude of other potential attack vectors created
- No detailed analysis of crypto libraries to determine trustworthiness
- A lack of understanding of the best practices necessary to avoid introducing vulnerabilities when using industry standard technologies such as XML encryption
- A lack of availability of security expertise to maintain proprietary implementations
- No plan for securely handling logouts

While some enterprises force their SaaS and BPO service providers to use their proprietary SSO mechanism, it is more common for enterprises to us their service providers' SSO system. The permutations and combinations of mechanisms can require a separate, customized solution for each provider. This approach is neither scalable nor cost-effective. Moreover, attempting to make it so by taking shortcuts can introduce additional vulnerabilities.

The impact of phishing on SaaS clients includes:

- Loss of Confidence in SaaS
- Loss of Productivity
- Information Leakage
- Legal Issues
- Time to Resolve
- Operational Impact

Five Steps to Securing Internet SSO

Based on its industry-leading experience implementing secure Internet SSO, Ping Identity has established a set of best practices embodied in these five steps:

1. Review the Security Ramifications of Internet Applications
2. Implement Standards-Based Federated Identity Management
3. Integrate with Existing Identity Infrastructure
4. Retire Proprietary and Open Source SSO
5. Expand Protection to the Whole Organization

1. Review the Security Ramifications of Internet Applications

One of the most important steps to ensuring secure access involves understanding the vulnerabilities. Without such an understanding, it is difficult, if not impossible, to implement a secure solution. These vulnerabilities and their ramifications include:

- Repeated entry of usernames and passwords onto Internet forms that are each vulnerable to phishing
- External connections that are not fully secured and, therefore, fail to protect the users and the enterprise
- Incorrectly developed SSO mechanisms that are themselves vulnerable to attack
- Multiple SaaS access methods, including Internet browser, mobile browser and desktop client software, that provide multiple hacker attack points
- The use of different SSO methods for each partner connection, which dramatically increases overall complexity and, in doing so, diminishes security

Application and business process outsourcing is a trend that continues to increase with no sign of slowing. As a result, the need for a scalable mechanism to secure these connections continues to grow.

2. Implement Standards-Based Federated Identity Management

The key to avoiding this problem is to implement an Internet SSO solution that uses a capability called federation. Burton Group defines identity federation as “the agreements, standards, and technologies that make identity and entitlements portable across autonomous domains.”

For the user, federated identity eases access by delivering single sign-on to Internet-based applications, just as if the application were running on the local network. For the CISO, federated identity improves security. For the CIO, federated identity reduces operating costs. In addition, over 100 SaaS and business process outsourcing suppliers have already incorporated one of these standards into their service offering, meaning a single federated identity system can provide secure Internet SSO with all of these suppliers.

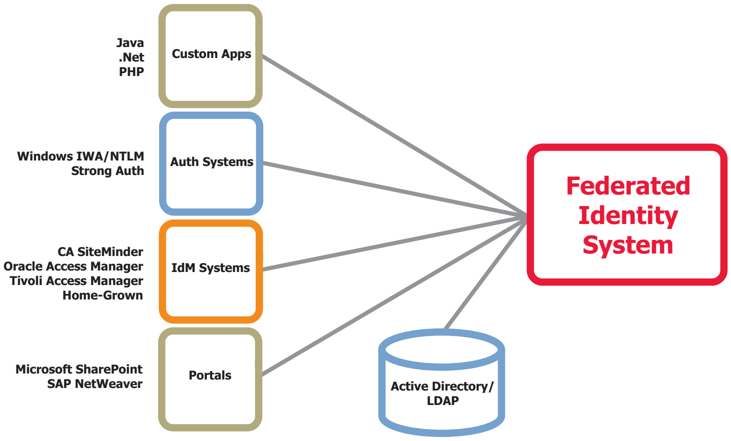
A key aspect of federated identity is that it is based on industry standard Security Assertion Markup Language (SAML) and WS-Federation. SAML is the predominant protocol for browser-based identity federation for some very good reasons. The standard is quite mature, having gone through three revisions since 2001. Over the past five years, over 300 security professionals have thoroughly reviewed the specification and amended it to ensure its robustness. And more than 20 security solution vendors have already implemented secure, interoperable products during the past four years, proving its effectiveness in practice.

3. Integrate with Existing Identity Infrastructure

Most medium and large organizations have already made significant security investments in their identity management infrastructure. Ideally, a federated identity management system should be able to layer on top of all of this existing infrastructure so it can leverage existing capabilities while also being able to establish secure connections with external partners.

Standalone federated identity products from specialist vendors have a significant advantage over federation modules from identity suite vendors in that they are designed to work with any identity infrastructure component, while suite products usually only work with products from their own suite.

Larger organizations also have the challenge of multiple identity infrastructure components. It is not at all unusual for these companies to have multiple identity suites from different vendors, or a combination of vendor-supplied and homegrown suites. Either way, the federated identity product should quickly and easily integrate with all of these components.



Standalone federated identity management systems integrate with a wide variety of identity infrastructure components. Such infrastructure can by commercial software, homegrown systems or a combination of both.

Secure Internet SSO is an effective anti-phishing measure because it:

- Reduces login frequency
- Optionally eliminates requirement for a login page
- Authenticates the service provider
- Makes stronger, multi-factor authentication more feasible/cost effective
- Reduces the risk of phishing attacks being distributed across SaaS customer base
- Gives SaaS customers optional control of phishing mitigation

4. Retire Proprietary and Open Source SSO

Once they have implemented a SAML-based system with strong integration capabilities, most organizations quickly realize they can improve security and reduce operating costs further by migrating any proprietary SSO mechanisms they may be supporting over to SAML.

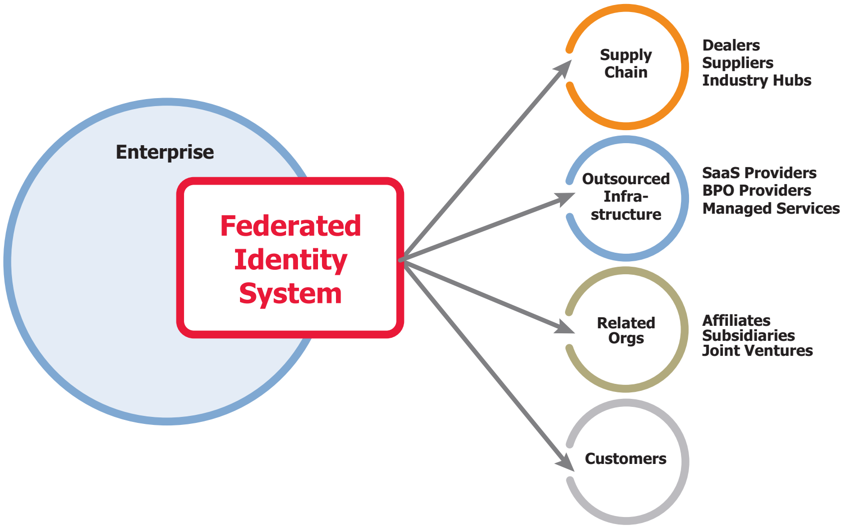
Due to its proprietary nature, an enterprise with twenty SaaS providers could potentially wind up supporting twenty different SSO mechanisms. Any proprietary connection that can be migrated to SAML means one less system to maintain and support.

One of Ping Identity's customers was quoted at a recent customer advisory board as saying they had established SSO with 50 different partners, and they were doing it 50 different ways. Now that the industry has standardized on federated identity as the way to deliver secure SSO over the Internet, this company is aggressively moving to replace all of its proprietary connections with SAML. The company believes this effort will pay for itself in operational cost savings alone, meaning they effectively get significantly improved security for free.

5. Expand Usage Across the Organization

With an Internet SSO solution based on federated identity management in place, it is possible to secure connections with literally every external business partner or entity the organization does business with. Examples of connections that can be protected include:

- Outbound SSO over the Internet for employees who access SaaS, BPO and managed services
- Inbound SSO for trading partners such as suppliers and dealers into a supply chain portal
- Internal SSO for employees who need access to systems operated by acquisitions, affiliates, subsidiaries and joint ventures
- SSO to third-party hosted industry hubs for information sharing by users, as well as application access among industry organizations
- SSO with major customers



Federated identity management provides secure Internet SSO for a broad variety of use cases including connections with supply chain partners, outsourcing providers, related organizations and customers.

Securing Internet SSO with PingFederate in 30 Days

PingFederate is the only standalone federated identity management software able to deliver secure Internet single sign-on to all external partner connections, including SaaS and BPO providers, trading partners, managed service providers, acquisitions, affiliates, subsidiaries and joint ventures. By implementing PingFederate with PingEnable—Ping Identity's expert methodologies, implementation services and support for each step of the identity federation process—most organizations are able to implement secure Internet SSO in thirty days or less, and turn around subsequent connections in less than a week.

More than 250 large enterprises, service providers and government agencies worldwide rely on PingFederate to secure, protect and control their identity interactions with other organizations. To see how PingFederate can help your organization, you can try it for free by going to www.pingidentity.com and downloading PingFederate, as well as whatever PingFederate integration kit or SaaS connection you might need. The process should only take you a few minutes. Then request your free evaluation license, install the software and put it through its paces. You will be well on you way to implementing secure Internet SSO in 30 days or less!

Additional Resources

You can find additional information on the topics addressed in this paper at www.pingidentity.com. Relevant resources that may be of interest include:

- Data sheet: PingFederate
- White Paper: Internet-Scale Identity Systems: An Overview and Comparison
- Webinar Archive: Federated Identity Management: What Is It and Why Should You Care?
- Download a Free Trial of PingFederate

About Ping Identity Corporation

Ping Identity's dedication to delivering secure Internet single sign-on software and services for over 150 customers worldwide has earned us recognition as the market leader in federated identity management. PingFederate®, the world's first rapidly deployable identity federation software, provides an organization's users safe access to Internet applications without the need to re-login. With PingFederate and PingEnable—Ping Identity's expert support, services, and methodologies—external connections can be operational in less than a week. Download a free trial at www.pingidentity.com.

© 2008 Ping Identity Corporation. All rights reserved. Ping Identity, PingFederate, and the Ping Identity logo are trademarks or registered trademarks of Ping Identity Corporation.
All other trademarks or registered trademarks are the properties of their respective owners.