Federated Identity Theft

By John C. Checco, CISSP

Many factors vie for attention in today's financial IT enterprise. Virtualization, grid computing, web services, outsourcing, resource flexibility, business intelligence, data warehousing, et al. have all been in the forefront at one time or another. However, three distinct efforts – regulatory compliance, identity management and service-oriented architectures – rely on the proper foresight of federated identity management. The relations between these seemingly disparate technologies are part of a much larger *information governance* initiative.

Regulatory Compliance: The industry will look back in history and see regulatory compliance as a major shift in business. Like Y2K, regulatory compliance should be the grand motivator for enterprises to make major paradigm shifts and rework poor implementations. Not only does compliance take resources and a culture that embraces change, but regulations can leave many requirements open to interpretation. It is these grey areas of user/account activity auditing that can impact an effective implementation of federated identity management.

Identity Management: Enterprises have had a history of troubles implementing individual identity management solutions within their organizations in the past. In fact, many organizations are on their second or third attempt. Those companies claiming success have taken the time to design a top-down approach. A well-organized team will review and reverse engineer business processes to classify proper roles and access controls. These teams responsible for designing the policy model need to look beyond the immediate internal needs of single sign-on towards federated identity management.

Service-Oriented Architectures: The evolution to SOA actually started decades ago, around the introduction of Yourdin's methodology to system design. The ideas of business logic modularity eventually converged into extranets to share business processes among the entire supply chain. This distributed and collaborative computing evolution will continue, so it is important that SOA design teams gear module design around proper authorization of business logic, assuming any piece of that logic will eventually be exported through the extranet portal to partner companies. SOA teams should be engaging partner companies to identify the business processes on the other side of the extranet portal, and *document* how partners are dealing with authorization.

Federated Identities: A Matter of Trust

Federated identities allow one enterprise to share information or business logic with another enterprise in a trusted relationship. The management of these types of relationships need to be efficient (due to the large number of extranet interactions with the onset of SOA), flexible (to support/extend existing individual identity management policies), secure and traceable (to comply with regulations). Federated identities can be of two flavors: trusted individual identities or enterprise-level extranet tokens.

Trusted Individual Tokens: A trusted individual token is simply an employee account that has access to a defined set of business systems. Trusted individual tokens allow fine-grained access control to extranet services, but are difficult to instantiate and maintain. And trusted individual tokens fail when a company does not properly eliminated the identity upon employee termination. For example, how many instances have you heard of where terminated employees still have access to their corporate voicemail?

Enterprise-Level Extranet Tokens: An enterprise-level extranet token is a single account issued for each trusted enterprise relationship, so the number of authentication tokens are minimal, but lack user-level auditing capabilities. An enterprise-level extranet token fails when a rogue employee uses it for an unintended purpose, often with no tracking ability. Again, using the corporate phone system as an example, how many terminated employees still have access to their managers' bridge numbers?

Federated Identity Theft

So, exactly, what is federated identity theft? Similar to individual identity theft, federate identity theft is the use of a false or stolen enterprise identity to gain trusted access to extranet portals. Because it is the extranet portals that are exploited, there may be a great latency to detection – if detection occurs at all. The negative effects for such breaches resonates to all companies in the chain – whether involved directly or not: loss of customers, financial retribution, branding weakness, stockholder dissatisfaction and SEC downgrading

A real-world (albeit non-technical) example of federated identity theft is ChoicePoint. In this situation, a team of individuals posing as many as 50 check-cashing companies gained access to third party client data through ChoicePoint. The vendor companies feeding this data to ChoicePoint had no reason not to trust the information repository, given the assumption that ChoicePoint had done due diligence with the identity of any requesting company.

Given that federated identity theft can have high-risk valuations as well as major latencies in detection, endpoint validation should be paramount. This is the first wall any criminal community will need to breach. Endpoint spoofing is done very easily today through hijacking, DNS-attacks and various other methods. Turning this minor hacking obstacle into a major hacking obstacle will weed out all but the most determined criminal element.

The following design techniques can minimize potential problems. The underlying notion is to validate three entities: the endpoints, the organizations and the users.

Reciprocal PKI: DH/SSL, the encrypted communication mechanism used for HTTPS protocol, may no longer be enough for federated identity management use. Both ends of the communication channel need to verify the identity of the other. Extranet partnerships should begin by exchanging public keys designed specifically for federated identity management. This reciprocal use of a PKI infrastructure can ensure the privacy of the communication channel. In addition, the signing of messages dynamically during the communication provides a secondary checkpoint of enterprise identity. Traditionally, the downside of any PKI communication has been the cost of key maintenance as well as the cost of the transaction using PKI encryption/decryption. With federated identity management, the key maintenance costs are incurred solely during the creation of the partnership agreements. Depending on the risk level of the transaction, PKI transaction costs need only incur during authentication and authorization.

Encapsulating Identities: Encapsulated identities use an individual token wrapped by an extranet token. In essence, the individual token, once authenticated locally, is wrapped by the extranet token and it is this outer token that authorizes the communication to extranet services. This encapsulation technique can mitigate hijacking risks because an employee may know their individual identity, but the extranet tokens are handled only in the back-end communication. This technique has distinct benefits:

1. From a local perspective, individual tokens for local user authentication to applications, wrapped by extranet tokens in the backend for extranet communication. The end user has no knowledge of anything other than their individual token (usually from a SSO implementation).

2. From the remote perspective, extranet identities are used to authenticate the communication between partner companies, and individual tokens can be used to have tiered authorization and access levels.

3. The logging and auditing of both the extranet and individual tokens can provide more robust security points for fraud detection.

The encapsulation technique requires both parties to be able to unwrap and use the extranet token or the individual token when and where necessary. This token splitting process itself can occur at the extranet entry point, but additional designs and processes are needed to separate authentication from authorization, and to determine which token type is used where.

These requirements of encapsulation methodology must be visible during the design phase of a federated identity management implementation, and partnering companies need to be aware of these requirements. In the very real case where partners choose NOT to implement such a robust technique, two modifications still need to take place:

1. The extranet entry process on the partner side would need to unwrap the encapsulated token, discard the irrelevant token and use only the token their federated identity management implementation requires.

2. The extranet exit process on the process side would still need to generate an encapsulated token; the outer layer and inner layer would be the same token.

Identity Abuse Detection

The above steps will mitigate most federated identity theft attempts from external or rogue sources. However, measures are still needed for detecting internal resources that take advantage of trusted extranet relationships. Several existing technologies working together can provide a good base for extranet anomaly detection: workstation location awareness (usually implemented for securing wireless network connections), application heartbeat signaling (used for disaster recovery and failover) and heuristic log analysis.

Workstation Location Awareness: Assuming that all extranet traffic is tunneled through a gateway from your client to your partner's portal – which would be where the identity encapsulation would take place anyway – there would be a distinct log of workstation IP addresses, individual identities and request methods.

Application Heartbeat Signaling: A background process on both sides would take a time slice of this workstation location information and generate an MD5 signature. Actually two MD5 signatures would be generated for each partner company: one for incoming connections against that partner

company, and another for outgoing connections. These MD5 signatures will be sent as a heartbeat signal to the partner company every time slice. The partner company would then compare the signatures created locally for the same time slice / partner. If any difference is found, either side may request the audit log for that time slice and compare details to find the disparity in connections. This would trap any rogue traffic coming from outside the extranet gateway in a timely manner.

Heuristic Log Analysis: Over time, the extranet transaction logs can be heuristically analyzed for the following anomalies:

1. Workstations not normally used for extranet transactions
2. Logins not normally associated with workstations used in transactions
3. Exceedingly large number of transactions per period
4. Exceedingly broad or narrow breadth of transactions
5. Multiple individual/extranet tokens from same workstation

Although these checks cannot catch an inside perpetrator in real-time; they provide good evidence to build a case against anyone that abuses the trusted extranet relationships.

Conclusion

Regulatory compliance, identity management and SOA all play a large role in dealing with partners and extranets; it is imperative to define how sensitive data is transferred between companies and how that data is secured at both ends. There are a myriad of issues with implementing federated identity management. Although your company may not be ready for federated identity management implementations, there are security issues that overlap efforts in which your company may already be involved. Regulatory compliance, identity management and exposing of business processes through server-oriented architectures are not the type of projects to favor deadlines over a thorough design. Include federated identity management security a part of that design.

About the Author

John C. Checco, CISSP is a member of ASIS NY, Infragard NY, (ISC)2, the WSTA Advisory/Content Committee and president of bioChec™. Feel free to end comments to checco@checco.com.