Security Fading As Barrier To Web Services

Rebecca Wetzel

The right organizational approaches and network devices are emerging.

Businesses are on the cusp of embracing Web services for external use. The desire to use Web services to interact with partners, customers and remote offices is strong, and a successful track record is building—albeit slowly. In a July 2003 Gartner survey, 54 percent of companies planned to use Web services outside their corporate firewall within 12 months, and 65 percent planned to do so within 24 months. This suggests that lack of security—long cited as the primary roadblock to Web services adoption beyond the firewall—is fading as a barrier. And that's good news for commerce, because Web services make it easier, faster and cheaper for companies to do business with one another.

"There is clearly awareness that Web services are like a power tool, which in the wrong hands can represent huge potential danger," said Lawrence Wilkes, an analyst with Web services research firm CBDI. But according to Wilkes, lack of security is a perceived rather than an actual barrier, and once organizations get the hang of deploying Web services, then projects proliferate. "Organizations move quickly past the pilot project stage, and having generally had a good experience completing the first project, they quickly move on to more."

Among the pioneers is the National Student Clearinghouse (NSC), which uses Web services to provide university enrollment and matriculation data to a variety of interested parties including lending agencies, employers, auto and health insurers, housing providers and credit card issuers. NSC uses Flamenco Networks' product to secure its Web services, and while Mark Jones, NCS vice president of marketing and business development acknowledges, "I hear about security being an issue," he goes on to say, "but honestly, it almost never comes up—and student data must be protected by law. The security that's available is not merely sufficient, it's better than it was when we offered just straight Web access or hard copy."

According to Jones, the bigger problem has been convincing others to join the game. "We learned that the hardest thing was getting the business part done. We had to convince [our partners and customers] why they should do this with us, because they had to do some [integration] work. The technology itself is not a big deal. It's not that difficult."

Although the number of deployments continues to rise, consensus among Web services security vendors is that it will be another 18 months or so before external Web services become commonplace. Indeed, finding pioneers willing to share their experience for this article proved challenging, and two reasons were most often cited: First, many initial deployments are in the financial services and government sectors, which are reluctant to talk about security; and second, external Web services projects are in early stages.

Organizational Issues

Security remains a gating factor in Web services adoption, but the primary issue is organizational—who will be responsible for security and how will it be managed—rather than technical. According to Mark O'Neill, chief technical officer of Web services security vendor Vordel, situations often unfold like this: "When a new Web services application is being developed and rolled out, chances are that the software architects and the team working on it may not know much about security. But at some stage, it will come to the attention of the security people at the company.

"At that stage, which is usually later than would be ideal, they think about how to put security into the application or service," he continued. "Quite often we'll be invited to a meeting with application people and security infrastructure people who may not have actually met or spoken much with each other before, but they need to have security."

Eugene Kuznetsov, chairman and CEO of DataPower, often sees Web services projects derail when application owners tell the network

Rebecca Wetzel is an industry analyst, consultant and writer. She is president of Wetzel Consulting LLC, and is an associate with network technology and performance analysis firm NetForecast. She can be reached at rwetzel@rwetzel.com

group: "I'm going to launch this and I just wanted to let you know. The network security group says: What do you mean you're going to launch this? This is not OK. We've got to throttle this down."

Jurisdictional issues are beginning to work themselves out, as departments cooperate and educate themselves as well as each other about Web services security. Most vendors agree that ultimately the data networking and security groups within larger organizations will manage the solutions. "There is a natural law that moves security to the edge versus back by the application," said Wes Swenson, chairman and CEO of Forum Systems. "Application architects, developers and business people don't want to manage security on a daily basis, especially at a content or context level like XML. They want the network security people to be responsible for it."

John Lilly, vice president and CTO of Reactivity, describes what's entailed in introducing his firm's product to customers. "We try to make sure that the [application] architect evaluates side by side with network operations people, because architects want to evaluate on function and what it does, and ops wants to evaluate on how it does it and how easy it is to run in a cost-effective way."

Swenson predicts the emergence of a new job function within security groups. "In a couple of years, I expect you will see somebody who is responsible for business context security. This person will make sure that the Web services application is tied to a security policy, and that is tied to the data, so everything is turning together."

XML/SOAP Security Gateways

The reason pulse rates rise at the thought of Web services security is because Web services require partners and customers to expose their internal business systems over the Internet. To do this safely requires restrictions on what is allowed, as well as which machine or individual can have access to which resources.

The goal, of course, is to keep the bad guys out and the good guys from making mistakes that might inadvertently wreak havoc. This requires the usual arsenal of security features to be applied to the Web services protocols XML and SOAP—these necessary security features include validation, authentication, authorization, encryption, non-repudiation (i.e., preventing someone from disavowing authorship of their messages) and attack protection. It also requires each security

Web services require partners and customers to open up internal systems—a scary prospect

TABLE 1 XML/SOAP Security Gateway Products

Function Type	Feature	Data Power	Flamenco Networks	Forum Systems	Reactivity	Sarvega	Vordel	Westbridge
Content Inspection	Schema Validation	√		√	√	√	√	√
	Content Filtering	√	√	√	√	√	√	√
	XML Routing	√	√	√	√	√	√	√
	DoS Protection	√		√		√		√
Message-based Security	Machine Authentication	√	√	√	√	√	√	√
	Machine Authorization	√	√	√	√	√	√	√
	Encryption	√	√	√	√	√	√	√
	Non-repudiation	√	√	√	√	√	√	√
	Masking (Service Virtualization)	√	√	√		√		√
Identity-based Security	User Authentication					√	√	√
	User Authorization						√	√
Performance Enhancement	XML Acceleration	√				√		
	SSL Acceleration	√			√	√		
Operations Management	Logging	√	√	√	√	√	√	√
	Alerting		√		√	√	√	√
	Auditability		√	√	√	√	√	√
Trading Partner Management	Automated Provisioning		√		√	√		
	PKI Management		√	√	√	√		
	SLA Management					√		√
Form Factor	Software Server		√	√	√		√	√
	Software Agents		√				√	
	Appliance	√		√	√	√	√	√
	PCI Card			√				
	Crypto Hardware				√	√		√

Another key is limiting the effort required of partners and customers

solution to comply with the not-quite-jelled Web services standards.

One approach is to program and/or integrate security features directly into the linked applications. Unfortunately, this also means that the application itself must be updated any time a Web services standard changes, a new partner is added or deleted or a policy changes. This approach makes it challenging at best to centrally monitor and manage security.

A crop of young companies has recently begun releasing products that centralize Web services security, decoupling it from the applications themselves. The names for these products vary, but they share characteristics that are most accurately described by the term XML/SOAP security gateway, and they provide sound underpinnings for centralizing and managing Web services security. XML/SOAP security gateways are to Web services security what IP firewalls are to network security, with a number of "trust" features added. They operate in proxy mode to provide a variety of Web services security functions.

Table 1 shows the current lineup of XML/SOAP security gateway vendors, including DataPower, Flamenco Networks, Forum Systems, Reactivity, Sarvega, Vordel and Westbridge, along with a summary of their product capabilities.

XML/SOAP security gateways perform content inspection to control what is allowed through. This includes such functions as filtering content, performing schema validation, checking message size and examining individual message elements to enforce rules about numerical values or value ranges permitted in specific fields within forms. XML/SOAP security gateways also generally provide XML routing, as well as message and/or identity-based authentication, authorization, encryption and non-repudiation. Additionally, some products mask information about back-end infrastructure and applications, and/or protect against Web services-specific denial of service.

DataPower and Sarvega add XML and SSL acceleration to the mix. Although most current Web services deployments do not yet require line-speed performance, in time, speed will become important for high-throughput, time-sensitive applications.

Other vendors like Flamenco Networks differentiate themselves on advanced management functions, which address the issue of making it easy for partners and customers to connect to Web services. "After all," said John Hanger, Flamenco's vice president of marketing and sales, "you can build the world's greatest Web service and secure the hell out of it, but no business benefits are going to be realized until a critical mass of trusted parties begins consuming the service."

Other Approaches And Players

Enterprise application integration (EAI) tool vendors such as BEA Systems, IBM, Ascential, Tibco Software and WebMethods are eager to extend their reach into Web services security. Their tools allow developers to build Web services security directly into applications. This approach is a piece of the security solution, but when used alone, becomes difficult to manage when multiple Web services projects, departments and partners are involved.

Conclusion

Safely deploying Web services over the Internet, or extending internal Web services beyond the corporate firewall is technically feasible today. A harder task is evolving organizations to support a new type of security, which Forum Systems' Wes Swenson refers to as "business context security"—tying Web services applications to security policies, and security policies to the data itself. This entails fostering interdepartmental teamwork, thoughtfully assigning responsibilities and cross-training groups to understand each other's needs. Also, as Mark Jones of NSC learned through the school of hard knocks, another key to success is limiting the amount of effort that's required of partners and customers wanting to hop on board the Web services train.

A prerequisite for scaleable business context security is to decouple Web services security management from the applications themselves. While this doesn't mean that security shouldn't be incorporated into the applications, decoupling Web services security management will make it easier to administer and monitor multiple Web services projects with open-ended numbers of partners and customers.

Security is a surmountable barrier to Web services adoption, and once organizations master the melding of applications and networking, and can effortlessly add and drop partners and customers, Web services will become commonplace□

Companies Mentioned In This Article

Ascential (www.ascential.com)
BEA Systems (www.bea.com)
DataPower (www.datapower.com)
Flamenco Networks (www.flamenconetworks.com)
Forum Systems (www.forumsystems.com)
National Student Clearinghouse (www.studentclearinghouse.org)
IBM (www.ibm.com)
Reactivity (www.reactivity.com)
Sarvega (www.sarvega.com)
Tibco Software (www.tibco.com)
Vordel (www.vordel.com)
WebMethods (www.webmethods.com)
Westbridge (www.westbridgetech.com)