2006-08
Service Oriented Architecture Security Elements

Introduction:

Service oriented architectures, whether based on the XML protocols or more specialized IP protocols like DNS or SMTP, have emerged as increasingly vital components of enterprise infrastructure, and thus security infrastructure.

SOAs for Security

Service oriented architectures (SOA) is the natural evolution of client-server computing. Services are readily created by anyone and provisioned to users by making them available at an IP address on a port. This is core to the design of the Internet, where anyone can throw up a service and provide it to anyone who wants to use it. But everyone doing what they want does not cut it in most enterprise environments today. They generally want a little bit more control over how people spend their time and what they spend it on. So SOA in enterprises today is largely about (1) herding the cats before the enterprise gets out of control and (2) coming to group consensus about the shared services that will be most helpful, the protocols for using them reliably, and how they will continue to operate and be cared for over time.

In the security arena, there are emerging SOA capabilities for things like authentication services and audit trail collection. In the case of an SOA for security, unlike a new benefits application or an internal Web site, the security element (SE) can rapidly become a critical component of enterprise operations. Like a domain name server (DNS) that translates the name of a site into the numerical Internet Protocol (IP) address value necessary to send packets to that service, an SE that is useful becomes a critical component in the operation of large numbers of enterprise systems. And like the risk aggregation effects of DNS servers whose failure results in rapid collapse of operations, the failure of an SE can have serious negative consequences to the enterprise that uses it.

What could possibly go wrong?

One of the most common SOA SEs today is the emerging identity management service. Active Directory (AD) is the Microsoft version of the lightweight directory access protocol (LDAP) that creates security tokens exchanged between servers clients. As AD becomes integrated into enterprise operations, applications abstract out security decisions relating to identification, authentication, and authorization and place them in commonly used calls to AD which makes security decisions monitors use.

Like the *Master Control Program (MCP)* from the movie *Tron*, AD and other similar systems are in the real-time decision cycle of many enterprise systems. This gains control and reduces costs, but risk is also aggregated. Control comes when the human resources department (HR) makes an administrative change that is almost immediately reflected in altered access to information resources. This completely automates some processes, like eliminating terminated employee access across the enterprise at the termination meeting, provisioning new access to enterprise systems when someone is hired, or eliminating access to a project when someone is moved into another role.

And like the MCP in Tron, SOA SEs create enormous potential for havoc. Suppose someone in HR decides to enter data as if you were terminated? Getting back your access may be a challenge. Suppose someone who operates AD for the enterprise has a breakdown and decides to terminate everyone's access all at once? Getting back access for all of the workers who are now sitting idle may be a very much bigger and far more expensive challenge. A more subtle attack might create new users and grant them access to key systems for a period of time, allowing them to plant Trojan horse back doors for reentry. Once planted, AD access is no longer needed and no evidence of ongoing access in AD remains. Instead of only doing this to a few systems manually, AD allows me to do this to the entire enterprise all at once. Arbitrary global capabilities for corruption, service denial, leakage, loss of control over use, and loss of accountability are now available from one console.

Conclusions:

Risk management is about balancing the risks against the benefits. The cost savings of SOA SEs are often sold as immediate and substantial, but much of the benefit is nebulous and unproven. The risks of enterprise-wide collapse are, however, very real and demonstrated.

- In one case, an attacked enterprise antivirus control system yielded global infestation.
- In another case, a 2-day global outage was caused by a single point of failure.

The risks can be balanced with the benefits, but this requires thoughtful effort, not just good wishes. It requires an ongoing and indefinite commitment to the technology solution with adequate redundancy and controls at a high enough surety level to justify the risk. As more and more enterprise systems are integrated, the cost of removal becomes extreme along with the risks of failure. Be careful what you ask for... you may get it.

Fraud of the month

Every month, we take an example from "*Frauds Spies and Lies and How to Defeat Them*" and describe a recent example. From page 20, section 2.3.5.4 we present:

"Vendor Kickbacks"

> *"This one is easy and completely outside of the bookkeeping of your company. You simply tell the vendor that they need to pay a "fee" to get the deal. It certainly happens all of the time, especially for deals in [other countries]... just about everywhere you find some of it."*

Vendor kickbacks can range from the subtle to the outrageously obvious. A subtle form of kickback is the giving of small gifts. Even a book, a pen, or a lunch may be over the line if you are a government procurement officer. But most companies recognize that doing business and being friends enhances both the friendship and the business and gets more reliable results as long as it doesn't go to extremes.

While psychologists have shown that the chances improve for getting deals when even very small gifts are exchanged, apples for the teacher have been around for a long time and aren't likely to go away. The key is to eliminate tit-for-tat exchanges and to avoid anything beyond the cost of a meal at a conference that is offered to everyone present, or a copy of a book that is helpful in day-to-day work.

Chet's Corner

The wireless space is particularly interesting to me in the area of disaster recovery and continuity planning. After Katrina, the wireless business has picked up for us, and we are starting to deploy wide area wireless networks to replace destroyed infrastructure. Pop-up wireless may not be secure in the sense of warding off all malicious attackers, but in recovery operations from natural disasters, availability to the relatively small number of people on the ground and in need of communication trumps secrecy every time. To get more availability, we started testing balloon-based wireless. The wireless business is... looking up!

"Always look on the bright side of life"!

Service Summary

Every month we feature one of our services and give an example of how it benefited one of our clients. This month it's policy creation and recreation:

Security policy creation is one of the most painful experiences of many security specialists' careers. We feel your pain. A few times a year we are asked to write a complete policy set for a large enterprise. In a recent effort, we helped the new CISO create a complete from-scratch ISO17799:2005 policy set. They decided to scrap the old policies because they were too complex and never meaningfully approved or deployed.

> The new policy set took about 6 months to get written and approved, It will take another 18 months to be fully implemented. We helped them walk through the minefield of gaining internal acceptance, adapted the policies to the many internal forces, and they eventually gained approval by the CEO and board of directors. In the end, it was the group processes we facilitated that made the policy work, and not simply the ability to codify one person's ideas into a series of unused documents fulfilling an administrative need.

You can buy an off-the-shelf policy for a few hundred dollars, and it's worth everything you pay for it. Writing real policies for real enterprises means creating the enterprise control structures, identifying how power and funding will work, creating an appeals process, and imposing duties on a wide range of executives, managers, and workers. It takes a serious effort by a group of people over a substantial time frame to create and implement a real policy that helps secure an enterprise.

Mollie gets the last word in

My young sister is growing up, and I sometimes get a bit worried about the way she uses the Internet. She created her own blog, and we taught her not to put her personal information on it. She uses instant messaging instead of the telephone, so we told her she can only safely message people she already knows and helped her limit her footprint. The list goes on and on. When are they going to start teaching this stuff in grade schools?