**Capítulo 8. Segurança em Web Services**

A segurança é uma das principais questões que os desenvolvedores de serviços web enfrentam, particularmente no ambiente corporativo. Sem uma infraestrutura de segurança abrangente, os serviços web simplesmente não alcançarão seu maior potencial. Não é surpresa que estejamos começando a ver novas batalhas surgirem no mercado à medida que as empresas competem pela posição dominante em segurança.

A autenticação é um dos principais componentes que surgiram. Atualmente, existem três infraestruturas de autenticação de serviços web amplamente conhecidas, concorrentes (e infelizmente, incompatíveis) disputando posição no mercado:

**Passport**  
Serviço proprietário da Microsoft de logon único (single sign-on) que fornece autenticação e serviços de carteira digital para milhões de usuários.

**Magic Carpet**  
Serviço próprio da AOL de logon único e carteira digital para uso pelos membros da AOL.

**Projeto Liberty da Sun**  
Um esforço colaborativo entre as comunidades de desenvolvimento Java e open source para desenvolver uma alternativa ao Passport.

Das três, o Passport é a arquitetura mais conhecida e compreendida. Discutiremos essa arquitetura neste capítulo, mas antes vamos examinar mais de perto a segurança em serviços web em geral, incluindo uma análise das especificações de assinatura digital XML e criptografia XML.

**8.1 O que é um Serviço Web “Seguro”?**

Serviços web tratam do envio de informações; não importa realmente que tipo de informação está sendo transmitida. Um serviço web “seguro” é aquele em que o remetente da informação confia que o destinatário realmente é quem afirma ser, e vice-versa. Além disso, um serviço web “seguro” é aquele em que a informação pode ser recebida e acessada apenas pelo destinatário pretendido.

Essa definição implica duas coisas:

1. Deve haver algum tipo de autenticação.
2. Deve haver algum tipo de proteção de privacidade e integridade, como criptografia e autorização.

**8.1.1 Autenticação**

A autenticação levanta questões como:

* Quem sou eu?
* Como provo quem eu sou?
* Por que você deveria confiar em mim quando digo quem sou?
* Quem é você?
* Como posso provar que você é quem diz ser?
* Por que devo confiar em você quando diz quem é?

No mundo dos serviços web, responder a essas perguntas é vitalmente importante. De igual importância é criar um método padrão para fazer e responder a essas perguntas.

É aí que entram protocolos como o **SAML (Security Assertions Markup Language)**. No Capítulo 5, discutimos brevemente o SAML e demonstramos de forma simples como ele pode ser usado para fornecer capacidades de logon único, mas há mais do que isso.

Asserções SAML podem fornecer uma expressão padronizada e legível por máquina da identidade de uma pessoa, aplicação ou dispositivo. Essa identidade pode ser validada, compartilhada e usada como prova de que você realmente é quem diz ser. Como a asserção é assinada digitalmente, podemos estabelecer um tipo de confiança não baseada na minha palavra, mas sim na palavra de uma terceira parte confiável (o emissor da asserção).

Embora o SAML ainda tenha obstáculos a superar até sua conclusão, há um enorme potencial para fornecer uma estrutura padrão abrangente para implementar logon global.

A Microsoft propôs recentemente uma abordagem alternativa de autenticação baseada na inclusão de estruturas como tickets Kerberos dentro do cabeçalho SOAP. Essa abordagem, definida por duas especificações relacionadas chamadas **WS-Security** e **WS-License**, é usada extensivamente no projeto **.NET My Services** da Microsoft (anteriormente conhecido como Hailstorm).

Atualmente, não há padrões (reais ou de fato) que definam como transportar informações de autenticação dentro de um Envelope SOAP.

**8.1.2 Privacidade**

Existem duas questões importantes para garantir a privacidade, ambas tratando da proteção de ativos.

A primeira é a proteção das informações pessoais de um indivíduo. Por exemplo, se eu lhe der meu endereço residencial e número de cartão de crédito, espero que você proteja essa informação e não a envie pela Internet sem proteção.

A segunda questão diz respeito a como efetivamente proteger esses dados; isso implica políticas de autorização que detalham quem pode acessar as informações e o que pode fazer com elas, e métodos de criptografia que garantem que partes não autorizadas não possam acessá-las.

Atualmente, existe pouca infraestrutura de privacidade na Internet. Embora haja mecanismos simples para ocultar informações durante a transmissão (como o SSL), não há como garantir que suas informações pessoais sejam usadas apenas para o propósito específico para o qual foram fornecidas, uma vez enviadas.

O mais próximo que temos de uma infraestrutura de privacidade é a **Plataforma para Preferências de Privacidade (P3P)** do W3C, que especifica uma linguagem baseada em XML para criar perfis de privacidade.

Os provedores de serviços criam esses perfis para informar aos consumidores como pretendem usar as informações pessoais fornecidas por eles. Embora seja um primeiro passo valioso, esses perfis não são juridicamente vinculantes, podem mudar a qualquer momento — e frequentemente mudam. Assim, se uma empresa decidir usar suas informações de maneira que viole os termos originais do perfil, não há leis que a impeçam. Isso está mudando, e espera-se que leis sejam aprovadas em um futuro muito próximo para tornar as políticas de privacidade juridicamente vinculantes.

Outro problema com a privacidade na Internet é que as pessoas confundem autenticação com autorização. Isso pode ser visto na versão do serviço **Passport** da Microsoft atualmente utilizada em uma ampla gama de sites de comércio eletrônico. Quando um usuário se autentica com o Passport, quase todas as informações pessoais contidas em seu perfil são automaticamente compartilhadas com os sites habilitados para Passport que o usuário visita. O problema de autenticar usuários está resolvido, mas a autorização das empresas que podem acessar suas informações não está.

A autenticação da identidade de um usuário e o gerenciamento de suas informações pessoais precisam ser completamente separados. Serviços como Passport, Magic Carpet e Liberty confundem essas linhas.

**8.2 Microsoft Passport, Versões 1.x e 2.x**

A versão atual do **Microsoft Passport** foi projetada para fornecer serviços de logon único e carteira digital para serviços baseados em navegador. É simples de entender:

1. Um usuário, Jane, visita um site habilitado para Passport (por exemplo, MSN.com).
2. Ela recebe um link “Passport Sign-on” que redireciona seu navegador para [**http://www.passport.com/**](http://www.passport.com/), onde digita seu ID de usuário e senha do Passport.
3. Após validar o nome de usuário e senha, o Passport.com cria um cookie no computador de Jane que contém seu perfil de usuário criptografado (todas as suas informações pessoais).
4. O Passport então a redireciona de volta ao site original, que verifica a existência do cookie, acessa-o e extrai as informações necessárias sobre Jane para fornecer um serviço mais personalizado.

**8.2.1 Desvantagens**

Existem vários problemas nessa arquitetura. Primeiro, seria muito simples para uma pessoa mal-intencionada enganar Jane para que ela, voluntariamente, comprometesse seu ID de usuário e senha, simplesmente criando uma página falsa de login do Passport.

O usuário médio, redirecionado para a página falsa em vez da verdadeira página do Passport.com, não perceberia a diferença. Ela digitária suas credenciais, pressionaria **Enviar**, e nunca saberia que na verdade não fez login. Enquanto isso, o criminoso agora teria a senha de Jane e poderia acessar todas as suas informações pessoais e até se passar por ela em sites reais habilitados para Passport.

Um segundo problema é que nada impede que uma pessoa mal-intencionada configure um site habilitado para Passport de forma legítima e, assim, se aproveite do Passport, divulgando livremente as informações pessoais de Jane quando ela visitar o site.

Em qualquer um dos casos, é provável que nem Jane nem o Passport descubram que suas informações foram comprometidas, pois o Passport não inclui nenhuma capacidade de auditoria que permita a Jane verificar posteriormente a atividade de sua conta.

Outro grande problema é a insegurança natural de usar cookies para armazenar informações de perfil — mesmo que criptografadas. Bastaria um simples vírus tipo “worm” direcionado a localizar e descriptografar esses cookies criptografados do Passport para causar um problema de segurança muito sério para milhões de usuários.

De fato, o serviço Passport da Microsoft foi recentemente alvo de críticas pesadas devido a uma falha grave de segurança que permitia que números de cartão de crédito e outras informações pessoais armazenadas pelo Passport fossem lidas por um hacker mal-intencionado.

**8.3 Microsoft Passport, Versão 3.x**

Embora os detalhes ainda sejam escassos, a Microsoft está trabalhando para implementar a próxima geração de seu serviço Passport — desta vez baseando-o no esquema de autenticação **Kerberos**, muito mais seguro, e oferecendo controles de privacidade mais robustos.

**8.3.1 Visão Geral do Kerberos**

O **Kerberos** é um protocolo de autenticação que existe há bastante tempo. Originalmente desenvolvido por uma universidade, muitas grandes empresas, como Microsoft e IBM, adotaram o Kerberos e incorporaram suporte a ele em suas linhas de produtos. A Microsoft é, de longe, a maior defensora do Kerberos atualmente na indústria.

O Kerberos é complexo demais para explicar em detalhes aqui. Aqui está um resumo bastante abreviado de como ele funciona:

* Primeiro, o usuário (novamente, usaremos Jane como exemplo) solicita ao servidor de autenticação Kerberos que valide suas credenciais. Jane faz isso criptografando um pacote de informações usando sua chave privada. O servidor Kerberos descriptografa esse pacote usando sua chave pública. Se a descriptografia for bem-sucedida, o serviço Kerberos determina que Jane realmente é Jane e envia para ela um **ticket** de autenticação.
* Sempre que Jane quiser usar algum recurso da rede, ela deve ir ao **Ticket Granting Service (TGS)** do Kerberos e solicitar explicitamente permissão para usar aquele serviço específico. O TGS validará seu ticket de autenticação e emitirá, conforme apropriado, um ticket de uso único para o serviço solicitado.
* Jane apresenta esse ticket de uso único ao serviço quando envia sua solicitação. Incluído na solicitação está um **autenticador** que prova que o ticket de uso único é autêntico e realmente veio de Jane, não de um impostor mal-intencionado tentando se passar por ela.

Embora seja uma simplificação grosseira, isso é tudo o que o Kerberos faz. O **Passport 3.0** implementará esse modelo, permitindo (esperançosamente) um modelo de autenticação mais robusto e seguro, que oferecerá melhor proteção aos mais de 160 milhões de usuários do serviço. Esse processo protege o usuário contra ataques de falsificação e **spoofing** que são possíveis na versão atual do Passport. É uma grande vantagem.

O gerenciamento de privacidade do Passport também é aprimorado. Os usuários poderão estabelecer políticas que determinem como suas informações serão compartilhadas e quem poderá acessá-las. Os detalhes ainda não foram definidos, mas ele usará as políticas de privacidade **P3P**. Isso não muda o fato de que as políticas P3P ainda não são juridicamente vinculantes, mas é um grande avanço para o Passport.

**8.4 Dê-me Liberty ou Dê-me ...**

Um novo participante na batalha pela segurança de serviços web é um projeto colaborativo chamado **Liberty**. Patrocinado pela Sun e um grupo de importantes atores da indústria, este projeto busca atingir três principais objetivos:

1. Permitir que consumidores e empresas mantenham informações pessoais de forma segura, viabilizando uma abordagem descentralizada para obtenção de informações pessoais ou proprietárias, e promovendo interoperabilidade ou entrega de serviços através de redes.
2. Fornecer um padrão universal e aberto para “logon único”, no qual usuários e provedores de serviço possam confiar e usar para interoperar.
3. Fornecer um padrão aberto para identidade em rede que abranja todos os dispositivos conectados à rede, permitindo que os provedores de serviços de rede e a infraestrutura que possibilita esses serviços adotem um padrão neutro e aberto, disponível onde quer que a Internet esteja disponível, garantindo autenticação de identidade confiável em celulares, automóveis, cartões de crédito — literalmente, qualquer dispositivo conectado à Internet.

Nenhum detalhe técnico foi divulgado sobre como essas metas serão alcançadas. No momento desta redação, o projeto Liberty é essencialmente **vaporware**.

**8.5 Um Magic Carpet**

Há tão pouca informação sobre a proposta **Magic Carpet** da AOL quanto sobre o Liberty. O pouco que se sabe indica que o Magic Carpet é uma extensão do serviço **Screen Name** da AOL.

O **Screen Name** tenta fornecer um logon único que pode dar acesso a muitos sites diferentes na Web. Você pode criar um perfil para os sites que visita e limitar o acesso desses sites a diferentes partes do seu perfil. No momento desta redação, o Magic Carpet da AOL ainda está em modo de sigilo e deve ser considerado **vaporware**, assim como o Liberty da Sun.

**8.6 A Necessidade de Padrões**

A Microsoft não é a única empresa trabalhando nesse problema. Infelizmente, aqueles que estão trabalhando nisso não estão necessariamente colaborando. Até o momento, temos três soluções incompatíveis sendo propostas para serviços web.

Em uma batalha que começa a se assemelhar às **Grandes Guerras dos Navegadores** do passado, inimigos tradicionais estão traçando linhas e se enfrentando para decidir quem vai controlar a segurança dos serviços web.

Uma abordagem melhor (a abordagem que os desenvolvedores precisam exigir) é que padrões sejam desenvolvidos e adotados por todos os diferentes participantes. Embora provavelmente demore muito para acontecer, o que não precisamos é desenvolver uma nova arquitetura aberta, voltada para interoperabilidade e integração, apenas para ver a interoperabilidade se perder quando realmente tentarmos fazer algo mais interessante, como logon global.

**8.7 Assinaturas Digitais XML e Criptografia**

Dois exemplos positivos de esforços de padronização atualmente em andamento na área de XML e serviços web são o **XML Digital Signature** e o **XML Encryption**, conduzidos principalmente pelo W3C (o IETF também está fortemente envolvido no esforço do XML Digital Signature).

Fornecer suporte abrangente para assinaturas digitais e criptografia será, de longe, uma questão mais importante do que a escolha dos serviços de autenticação.

O projeto **XML Digital Signature** está trabalhando para definir uma sintaxe padrão para assinar digitalmente dados (incluindo dados XML) e para codificar essa assinatura como XML. Assinaturas digitais são essenciais para proteger a integridade das transações comerciais na Internet e serão uma peça fundamental da infraestrutura geral de serviços web.

O projeto **XML Encryption** está trabalhando para definir como dados criptografados (incluindo dados XML) e as metainformações necessárias para descriptografar esses dados podem ser codificados como XML. A criptografia de dados XML é crítica para garantir a confidencialidade das informações trocadas entre participantes de serviços web.

Atualmente, apenas o **Web Services ToolKit** da IBM e as implementações de serviços web do **.NET** da Microsoft incluem suporte para assinar e criptografar mensagens SOAP. Embora ambos suportem os mesmos padrões de Criptografia XML e Assinatura Digital, eles têm ideias diferentes sobre como exatamente assinaturas e dados criptografados devem ser colocados dentro de um Envelope SOAP. Assim, embora cada conjunto de ferramentas ofereça suporte a criptografia e assinatura, eles não são compatíveis entre si.

Espera-se que essas diferenças de interoperabilidade sejam resolvidas em breve, levando a implementações compatíveis. Uma questão-chave será fazer com que outros fornecedores de ferramentas de serviços web ofereçam suporte a esses padrões de segurança em seus produtos.

**Seções do Capítulo 8:**

* 8.1 O que é um Serviço Web “Seguro”?
* 8.2 Microsoft Passport, Versões 1.x e 2.x
* 8.3 Microsoft Passport, Versão 3.x
* 8.4 Dê-me Liberty ou Dê-me ...
* 8.5 Um Magic Carpet
* 8.6 A Necessidade de Padrões
* 8.7 Assinaturas Digitais XML e Criptografia