



RELATÓRIO

Segurança da Plataforma Macromedia® Flash® e Soluções Empresariais da Macromedia

Adrian Ludwig

Setembro de 2005

Copyright 2005 Macromedia, Inc. Todos os direitos reservados.

As informações contidas nesse documento representam a visão atual da Macromedia na questão discutida a partir da data de publicação. Como a Macromedia deve responder a mutantes condições de mercado, esse documento não deve ser interpretado como sendo um compromisso da parte da Macromedia e a Macromedia não pode garantir a precisão de qualquer informação apresentada após a data de publicação.

Esse relatório é para propósitos informativos somente. A MACROMEDIA NÃO FAZ NENHUMA GARANTIA, EXPRESSA OU IMPLÍCITA, NESTE DOCUMENTO. ESSE DOCUMENTO CONTÉM LINKS A SITES DE TERCEIROS QUE NÃO ESTÃO SOB O CONTROLE DA MACROMEDIA E A MACROMEDIA NÃO É RESPONSÁVEL PELO CONTEÚDO OU QUALQUER SITE LINKADO OU QUALQUER LINK CONTIDO EM UM SITE LINKADO OU QUAISQUER ALTERAÇÕES OU ATUALIZAÇÕES EM TAIS SITES. A MACROMEDIA NÃO É RESPONSÁVEL PELO WEBCAST OU QUALQUER OUTRA FORMA DE TRANSMISSÃO RECEBIDA DE QUALQUER SITE LINKADO. A MACROMEDIA ESTÁ FORNECENDO ESSES LINKS PARA VOCÊ SOMENTE COMO UMA CONVENIÊNCIA E A INCLUSÃO DE QUALQUER LINK NÃO IMPLICA QUE A MACROMEDIA ENDOSSA OU ACEITA QUALQUER RESPONSABILIDADE PELO CONTEÚDO EM TAIS SITES DE TERCEIROS.

A Macromedia pode deter patentes, solicitações de patentes, marca comercial, direitos autorais ou outros direitos de propriedade intelectual cobrindo o assunto desse documento. A não ser conforme expressamente contido em qualquer acordo escrito de licença da Macromedia, o fornecimento desse documento não lhe dá nenhuma licença a essas patentes, marcas comerciais, direitos autorais ou outra propriedade intelectual.

Macromedia, o logotipo da Macromedia Breeze, Flex, FlashCast e Flash são marcas comerciais, registradas ou não, da Macromedia, Inc. nos Estados Unidos e/ou outros países. Os nomes de companhias e produtos mencionados neste documento são marcas comerciais de seus respectivos proprietários. A Macromedia não patrocina, afilia ou endossa tais produtos e/ou serviços.

Macromedia, Inc.
601 Townsend Street
São Francisco, CA 94103 USA.

Conteúdo

Tratando de Preocupações com Segurança em Relação à Plataforma Flash.....	1
Autenticação	3
Exemplo de Solução: Macromedia® Breeze™	3
Controle de Acesso	4
Controles de Acesso no Lado Servidor	4
Controles de Acesso no Lado Cliente.....	4
Exemplo de Solução: FlashCast.....	4
Acesso Não Autorizado a Recursos de Sistema de hospedagem	5
Acesso Não Autorizado a Dados	5
Acesso Não Autorizado a Informações Particulares do Usuário.....	6
Código Malicioso	7
A Abordagem de Sandbox: Proteção Contra Código e Atividades Maliciosas	7
Injeção Minimizada de SQL e Vulnerabilidades de Scripting Cruzado.....	7
Exemplo de Solução: Macromedia Breeze.....	7
Transporte de Dados	8
Obediência a Padrões.....	8
Segurança Wireless (Sem Fio).....	8
Facilidade de Integração com Aceleradores SSL e Balanceadores de Carga.....	8
Suporte para Envolvimento Criptografado	9
Exemplo de Solução: Serviço Speedera Flash Video Streaming.....	9
Conclusão	10
Para Obter Maiores Informações	11
Referências	11

Em um mundo onde a maioria das experiências digitais é plana, a Plataforma Macromedia Flash oferece algo diferente. É um tempo de execução multiplataforma leve que pode ser usado não somente para mídia rica, mas também para aplicativos empresariais, comunicações e aplicativos móveis. A Plataforma Flash está estimulando um crescente número de Aplicativos Ricos para a Internet (RIAs). E, conseqüentemente, cada vez mais funcionários, parceiros e clientes têm acesso a dados e processos empresariais. Esse acesso, combinado com a exigência de obedecer a regulamentações do mercado como a Lei Sarbanes-Oxley e a Lei de Portabilidade e Responsabilidade de Seguro de Saúde (HIPAA) nos EUA, fez com que empresas ficassem interessadas no nível de segurança fornecido por essa estrutura de trabalho. A Plataforma Flash e a família de produtos Flex tratam dessa preocupação alavancando as atuais soluções e tecnologias de segurança de uma organização.

Tratando de Preocupações com Segurança em Relação à Plataforma Flash

A abordagem da Macromedia é a implementação de robusta segurança dentro seus próprios produtos, evitando novas exposições do resto do ambiente. Contudo, as tecnologias da Plataforma Flash não são produtos de segurança—elas somente alavancam atuais ferramentas e abordagens de segurança já instaladas, enquanto minimizam investimentos adicionais em segurança. Por exemplo, a Plataforma Flash se integra completamente na arquitetura existente de uma organização em nível do navegador através de um plug-in e na camada de apresentação através de software Flex ou uma solução HTML estática com script e Flash (veja a Figura 1). A segurança é controlada por soluções e protocolos de segurança existentes (veja a Figura 2). Como a Plataforma Flash alavanca tecnologias de SSL e autenticação e não requer nenhuma mudança ao controle de acesso ou outras configurações de segurança, as organizações não precisam implantar soluções adicionais de segurança para usarem a Plataforma Flash.

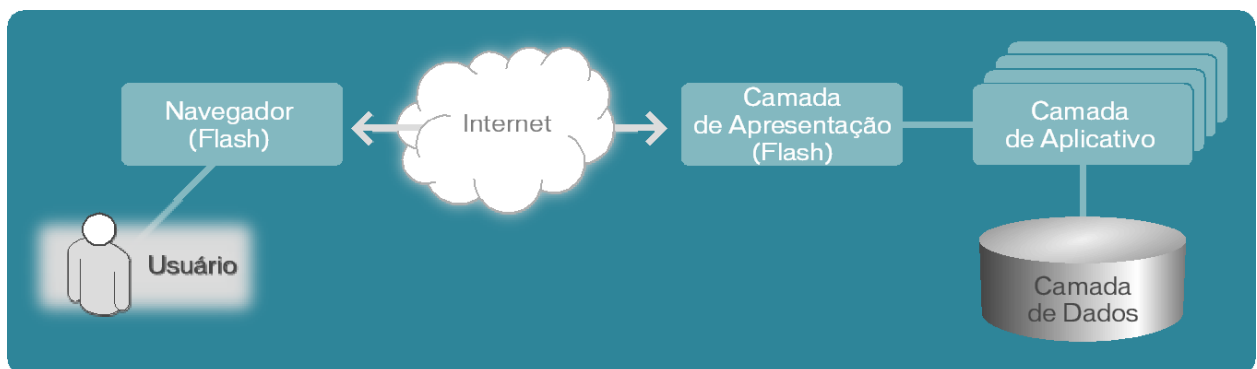


Figura 1: A Plataforma Macromedia Flash alavanca a infra-estrutura existente de uma organização.

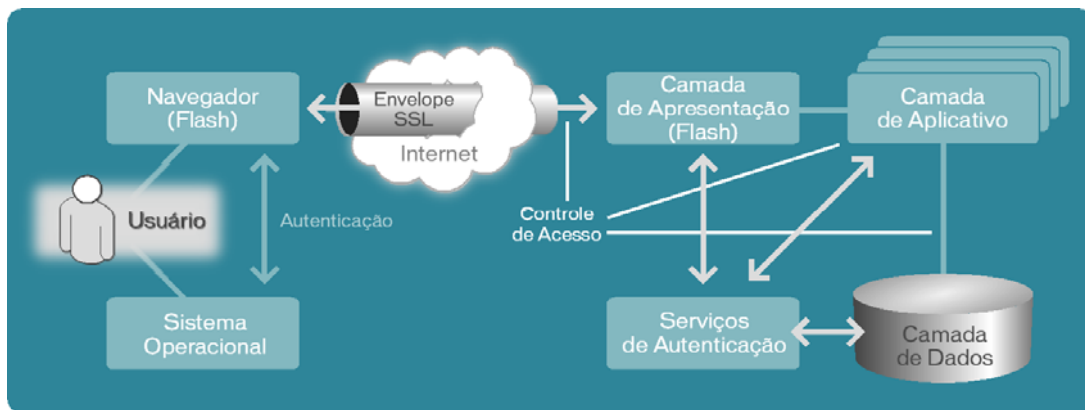


Figura 2: Em ambientes Flash, a segurança é gerenciada por soluções e protocolos de segurança existentes.

A Plataforma Flash é um verdadeiro ambiente multiplataforma que alavanca as principais capacidades de segurança dos sistemas operacionais, navegadores e servidores de aplicativos subjacentes. A Plataforma Flash é baseada em padrões de segurança aprovados e comprovados, como SSL e HTTPS, para o transporte de dados. Ela tem uma arquitetura em camadas que engloba os principais elementos exibidos na Figura 3. Esse relatório se concentra nos servidores e tempos de execução (por exemplo, Macromedia Flash Player e software Macromedia Flex), que são usados para entregar aplicativos, conteúdo e comunicações Flash e que agem como a plataforma, fornecem os controles e especificam a arquitetura. O relatório também inclui exemplos de soluções como o Macromedia® Breeze™ e Macromedia® FlashCast™ que são implementados usando essa estrutura de trabalho.

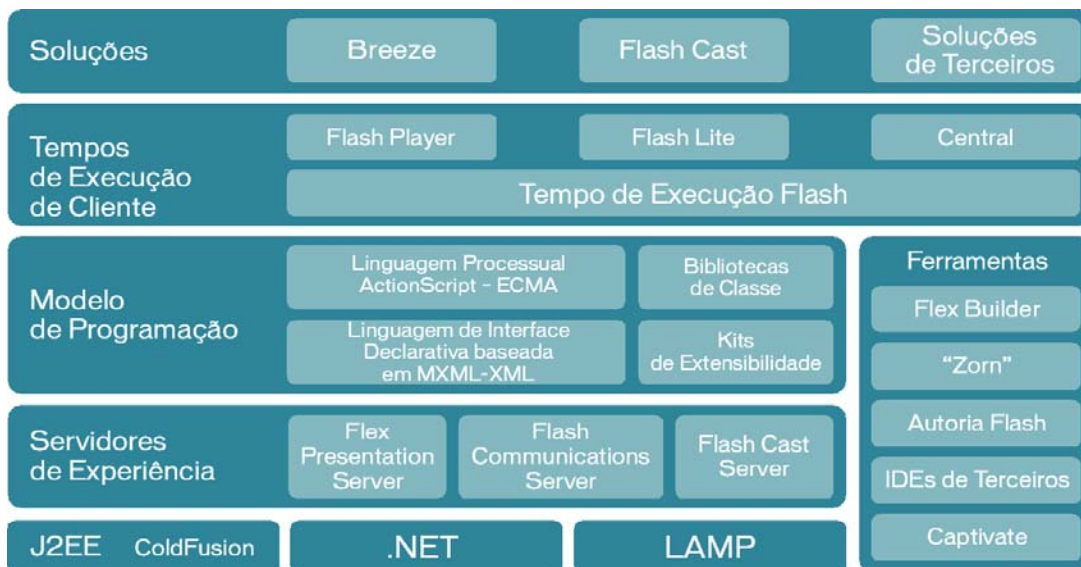


Figura 3: A Plataforma Flash tem uma arquitetura em camadas que engloba os principais elementos mostrados aqui.

Para obter maiores informações sobre a Plataforma Flash, veja o relatório Macromedia intitulado "Entregando Aplicativos, Conteúdo e Comunicações Empresariais com a Plataforma Flash®".

Autenticação

Devido às crescentes pressões para seguir uma gama de regulamentações do mercado e o fato que um crescente número de parceiros, contratados e clientes terem acesso a redes corporativas, as empresas estão investindo quantias significativas em serviços de autenticação e autorização. Esses incluem *sign-on* único, integração VPN, hardware especializado (por exemplo, cartões inteligentes), PKI, RSA SecurID® e outros *tokens* físicos. Simultaneamente, exigências específicas do mercado estão obrigando as organizações a implantar soluções de autenticação. Por exemplo, tanto agências federais quanto organizações de serviços financeiros são obrigadas a utilizarem medidas de autenticação de dois fatores para protegerem transações eletrônicas. Do mesmo modo, organizações farmacêuticas e de cuidados com a saúde estão sendo muito pressionadas para protegerem a privacidade de indivíduos através de regulamentações tipo HIPAA.

Felizmente, as organizações que usam a Plataforma Flash podem alavancar sua infra-estrutura existente e investimentos em segurança para tratar dessas exigências. O servidor de apresentações Flex fica em cima de um servidor Java e se integra com protocolos padrão para autenticação, como LDAP e outros serviços de diretório. No lado cliente, o tempo de execução de cliente Flash aproveita as tecnologias comuns de segurança disponíveis em tecnologias web, como o manuseio transparente de autenticação por navegadores.

Exemplo de Solução: Macromedia® Breeze™

O Macromedia Breeze, uma rica solução de comunicação web que entrega comunicações on-line de alto impacto que pode ser acessada instantaneamente através do Flash Player, é construído sobre a Plataforma Flash. As organizações podem entregar dados, voz e vídeo com segurança entre aplicativos Breeze e usuários usando a criptografia Secure Socket Layer (SSL) de 28 bits. Além disso, o Breeze possibilita a integração com um sistema atual de gerenciamento de usuário de uma organização, como LDAP, para que organizações possam gerenciar os usuários e grupos de um único local. Por último, o Breeze Single Sign-On suporta a integração direta de sistemas corporativos de autenticação, como o eTrust™ SiteMinder® da Computer Associates. Isso fornece uma experiência única para os usuários através da eliminação de necessidade de múltiplos nomes de usuários e solicitações de senha.

Durante uma avaliação de penetração de aplicativos conduzida pela Symantec Professional Services, a Symantec considerou que o Breeze é projetado e implantado com as melhores práticas de segurança e observou que o modelo de segurança do Breeze oferece proteção integrada para os dados e o ambiente do aplicativo. Especificamente, a avaliação mostrou que o Breeze 5 previne que usuários não autenticados e não autorizados tenham acesso a elementos do Breeze.

Controle de Acesso

Além da autenticação, o controle de acesso tem sido usado cada vez mais para determinar quem tem acesso a que conteúdo e aplicativos dentro de uma rede corporativa. Apesar de exigências de controle de acesso variarem entre aplicativos, a Plataforma Flash incorpora uma série de recursos que ajudam as organizações a lidarem com essas necessidades. Alguns desses recursos de controle de acesso vêm pré-definidos e, em alguns casos, administradores ou usuários podem personalizá-los para as suas necessidades.

Controles de Acesso no Lado Servidor

Através do servidor de apresentação Flex, a Plataforma Flash oferece controle de acesso a dados no lado servidor utilizando controles existentes de acesso no servidor de hospedagem. Além disso, os administradores podem usar uma *white list* para controlar o acesso a todos os dados. Através da utilização de um sofisticado modelo de permissões que regulamenta solicitações de acesso a dados, o Flex pode prevenir a decodificação e interpretação de caracteres.

A @stake, Inc., uma das principais empresas de segurança digital, testou o recurso de *white list* do servidor de apresentação Flex de forma independente contra ataques simulados e validou a habilidade do servidor para lidar com os ataques mais comuns na Internet de maneira apropriada. Na verdade, no seu Macromedia Flex Product Briefing (Relatório de Produtos Macromedia Flex), a @stake concluiu que a “robusta validação de entrada [do Flex] comprovou ser poderosa na diminuição da habilidade de um atacante malicioso obter informações confidenciais ou interromper serviços de aplicativos Flex”.

Controles de Acesso no Lado Cliente

Muito parecido ao modelo usado para Java e JavaScript, o Flash Player executa conteúdo dentro de uma máquina virtual que implementa uma *sandbox* de segurança. Nessa *sandbox*, todos os recursos do Flash Player (aplicativos, dados, URLs de rede e assim por diante) são essencialmente isolados do resto do ambiente de computação, bem como outras ocorrências de *sandbox*. Essa abordagem fornece uma vantagem sobre aplicativos tradicionais ativados para a web, como soluções ActiveX, que muitas vezes têm acesso total ao ambiente dos sistemas operacionais. Apesar dos aplicativos do Flash Player poderem interagir livremente com recursos dentro do mesmo *sandbox*, a *sandbox* do Flash Player previne acesso não autorizado ao ambiente do sistema operacional bem como a outras ocorrências locais do Flash Player.

Exemplo de Solução: FlashCast

A abordagem de *sandbox* é utilizada para suportar aplicativos móveis como o software Macromedia® FlashCast™. Similar ao Flash Player, o cliente FlashCast que reside em dispositivos móveis se comunica com o servidor FlashCast para atualizações de conteúdo e executa conteúdo e gerencia recursos—como a armazenagem local dentro de uma *sandbox*. Essa abordagem de *sandbox* possibilita que as organizações se comuniquem através de múltiplos canais enquanto minimiza os riscos de segurança.

Acesso Não Autorizado a Recursos de Sistema de hospedagem

O acesso não autorizado a recursos de sistema de hospedagem inclui ganhar o controle de aplicativos, dispositivos ou recursos anexados ao sistema para o propósito de desativar, negar ou redirecionar acesso a esses recursos, por exemplo, através de *overruns de buffer* ou ataques de *denial-of-service* (DoS). O Flash Player permite somente acesso limitado a recursos específicos. Por exemplo, o Flash Player não permite que o conteúdo aloque sua própria memória, modifique configurações do sistema operacional ou efetue alterações no registro do sistema. Diferentemente de outras tecnologias no lado cliente, o Flash Player contém um conjunto controlado de objetos e operações que são predominantemente construções exclusivas dentro do ambiente de execução do Flash. Como a funcionalidade do sistema que o Flash Player pode acessar é limitada, o risco de criar conteúdo que recebe acesso não autorizado ao sistema de hospedagem ou recursos anexados a ele é minimizado.

Através do monitoramento da sua utilização de recursos chave de sistema, como espaço no HD e memória do sistema, o Flash Player limita o potencial de ataques DoS. O Flash Player define limites padrão iniciais em 100K pra cada domínio para conservar o espaço no HD. Se necessário, o Flash Player ou o conteúdo que ele executa pró-ativamente pedirá ao usuário para que ele aumente a alocação do espaço no disco. Contudo, o limite do espaço de disco é mantido até que o usuário dê permissão para o aumento da alocação de um domínio em particular.

O tempo de execução do Flash Player fornece interfaces seguras bem definidas para outros aplicativos web e conteúdo. O design inerente do tempo de execução de cliente previne contra o desenvolvimento de aplicativos Flash maliciosos que poderiam assumir o controle de aplicativos que não são baseados na arquitetura Flash. Apesar dos aplicativos Flash poderem se comunicar entre si, o modelo de segurança de *sandbox* assegura que conteúdo originando de diferentes domínios seja agregado em *sandboxes* lógicas. Aplicativos e conteúdo podem se comunicar livremente dentro da *sandbox* e a comunicação além do perímetro da *sandbox* é protegida. Isso inclui cenários onde múltiplos aplicativos Flash estejam executando dentro de uma única ocorrência do Flash Player e onde a comunicação é tentada entre duas ocorrências discretas do Flash Player.

Acesso Não Autorizado a Dados

Acesso não autorizado a dados se refere a dados no disco local, discos da rede ou servidores web que se comunicam pela rede ou são armazenados na memória por um aplicativo ou processo (por exemplo, listas de senhas, agendas de endereços, documentos privilegiados e código de aplicativos).

Um programa de ActionScript em um Flash Player não pode escrever, modificar ou excluir nenhum arquivo na máquina do cliente fora objetos compartilhados (pequenos arquivos específicos do Flash) e somente pode acessar objetos compartilhados por domínio. Aplicativos Flash baseados na Internet não podem ler nenhum outro arquivo local nem dados sensíveis ou particulares. Na verdade, nenhum método de ActionScript disponível a aplicativos Flash pode criar, modificar ou excluir diretórios ou arquivos diretamente.

Para que conteúdo Flash Player baseado na web acesse dados de servidor, o domínio servindo o conteúdo Flash Player deve obter permissão explícita do domínio hospedando os dados solicitados (ou seja, o domínio do provedor). Sem permissão, o carregamento falhará. Essas permissões são especificadas por um arquivo de política localizado no servidor do domínio provedor. Esse arquivo possibilita o controle de acesso listando explicitamente os domínios que têm permissão para acessar dados naquele servidor.

Acesso Não Autorizado a Informações Particulares do Usuário

Dados pessoais e financeiros—bem como informações sobre as configurações de segurança dos usuários para o Flash Player—muitas vezes residem na máquina do usuário e os usuários têm razão em se preocupar com outros acessando essas informações. Contudo, os usuários devem saber que o Flash Player não coleta informações sobre eles.

Os usuários têm controle sobre o comportamento do Flash Player quando se deparam com decisões sobre privacidade. Através da interface com o usuário Flash Player Settings e o Settings Manager (Gerente de Configurações), os usuários podem fazer a sintonia fina das seguintes configurações relacionadas à privacidade e segurança:

- Armazenagem local de dados usando o mecanismo local de objetos compartilhados
- Acesso a câmeras e microfones conectados ao sistema
- Notificações de atualizações para o Flash Player

Em um ambiente empresarial, os administradores de redes podem controlar configurações para o Flash Player centralmente para se assegurarem que todos os clientes obedeçam à política de segurança corporativa.

Além das proteções fundamentais fornecidas pela *sandbox* e máquina virtual, o cliente Flash Player também fornece *stakeholders* (aqueles que detêm ou gerenciam um recurso) com controles flexíveis fáceis de usar para controlar (ou limitar) acesso a recursos sensíveis como arquivos de redes e bancos de dados. O modelo de segurança do Flash Player é organizado de tal forma que permite que as empresas deleguem o controle de permissões para o *stakeholder* apropriado (veja a Figura 4). Esse modelo também suporta as arquiteturas distribuídas que são comumente usadas para aplicativos construídos na Plataforma Flash.

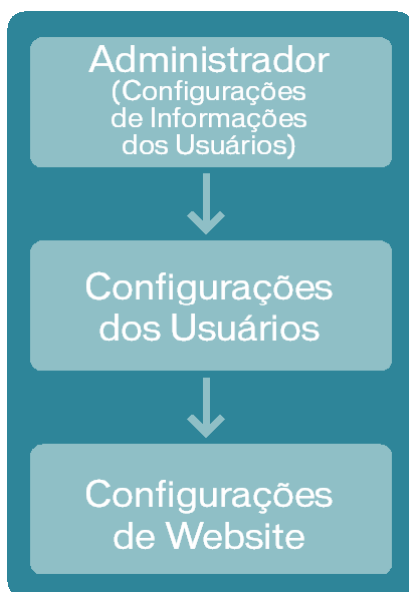


Figura 4: Controles de segurança para o Flash Player são organizados hierarquicamente.

Código Malicioso

Todas as organizações encaram o potencial de infecção por código malicioso que pode se espalhar rapidamente por toda a rede corporativa. Por exemplo, usuários de Internet poderiam fazer o download do que pareceria ser um programa legítimo que, na verdade, carrega uma ameaça como um programa de Cavalo de Tróia, o que poderia expor a rede a hackers. Ou código autorizando o acesso remoto a uma rede pode residir despercebidamente em cookies de navegador ou applets web.

A Abordagem de Sandbox: Proteção Contra Código e Atividades Maliciosas

Como discutido anteriormente, devido à abordagem de segurança de *sandbox* no lado cliente e a utilização de Java no lado servidor, a Plataforma Flash usa ferramentas de segurança locais para manter a resistência a código malicioso, como vírus, programas de Cavalo de Tróia, worms de back door e spyware. Além do mais, o design do Flash Player inclui características arquiteturais que minimizam ameaças de código malicioso em comparação com soluções ActiveX ou JavaScript. Como todos os recursos do Flash Player são isolados do resto do ambiente de computação—bem como de outras ocorrências de *sandbox*—através da abordagem de *sandbox*, o sistema de hospedagem é protegido contra atividade e programas maliciosos e conteúdo potencialmente danoso. Na verdade, em um memorando do Joint Chiefs of Staff (Chefes do Estado Maior) em relação às diretrizes de política para a utilização de tecnologia de dispositivos móveis nos sistemas de informação do Departamento de Defesa (DoD), o Flash Player consta sob a categoria 3, a mais segura das três categorias.

Injeção Minimizada de SQL e Vulnerabilidades de Scripting Cruzado

As soluções que usam linguagens interpretadas no tempo de execução baseadas em cadeia—como JavaScript e DHTML—são especialmente susceptíveis à injeção de SQL e scripting cruzado de site, itens listados como as 10 principais vulnerabilidades no site Open Web Application Security Project (www.owasp.org). Por outro lado, conteúdo Flash é entregue como uma série de instruções em um formato binário para o Flash Player sobre protocolos web no formato de arquivo SWF. Os próprios arquivos SWF são tipicamente hospedados em um servidor e depois descarregados para o computador do cliente e lá são exibidos quando solicitados. Como o Flash Player é binário e compilado, ele inerentemente inibe essas ameaças em comparação com soluções baseadas em cadeia que podem deixar dados de back-end vulneráveis e sem proteção.

Exemplo de Solução: Macromedia Breeze

Tipicamente, aplicativos acessam bancos de dados através de declarações SQL geradas dinamicamente, pois essas declarações são razoavelmente fáceis de implantar e fornecem uma coordenação mais solta com o banco de dados. Contudo, é difícil produzir declarações SQL geradas dinamicamente que sejam resistentes à injeção de SQL. Além do mais, declarações dinâmicas muitas vezes exigem vastas permissões de acesso a objetos de bancos de dados. O software Breeze usa declarações preparadas e procedimentos armazenados para chamadas ao banco de dados. Declarações protegem contra a injeção de SQL, enquanto procedimentos armazenados possibilitam que o banco de dados seja mais protegido.

Durante a avaliação de penetração de aplicativo conduzida pela Symantec Professional Services anteriormente mencionada, a Symantec encontrou que a implementação de procedimentos armazenados no software Breeze prevenia contra tentativas de comprometer dados de aplicativos através da utilização de injeção de SQL e ataques de manipulação.

Transporte de Dados

Claramente, o transporte seguro de dados entre as hospedagens Flash e Flex e aplicativos é crítico para assegurar a integridade dos dados, bem como se certificar que outros não usem aqueles dados para propósitos maliciosos.

Obediência a Padrões

Tanto o Flash Player quanto a linha de produtos Flex usam protocolos baseados em padrões para o transporte de dados. O Flash Player sabe se seus dados foram obtidos através de uma conexão HTTPS (HTTP sobre Secure Sockets Layer) segura e registra esse fato usando diferentes *sandboxes*. Dados carregados a partir de sites HTTPS são subseqüentemente tratados diferentemente de dados de HTTP ou outros recursos menos seguros. Essa segmentação de dados de clientes é uma extensão natural dos modelos PKI mais comuns, que usam certificados x509 para identificar clientes e servidores. Padrões criptográficos como certificados x509 são implementados pelos navegadores com os quais o Flash Player interopera. No lado servidor, esses padrões são implementados pelo ambiente de hospedagem. Usando padrões XML e SOAP para o transporte de dados, a linha de produtos Flex se beneficia das tecnologias comuns de segurança como HTTPS, que é suportada para todas as operações.

Segurança Wireless (Sem Fio)

Conforme a rede corporativa se estende para fornecer acesso a uma variedade de constituintes—como contratados, parceiros, clientes e tele-comutadores—as organizações precisam proteger um crescente número de usuários remotos. Sem segurança wireless efetiva, não só os dados em trânsito estão vulneráveis a acesso e manipulação, como a própria rede empresarial está vulnerável a ameaças da Internet e código malicioso que podem ser introduzidos através de dispositivos sem fio. Usando SSL, criptografia nativa, e a segurança nos sistemas operacionais, o Flash Player e a linha de produtos Flex minimizam as preocupações com segurança wireless.

Como os aplicativos Flash executando dentro de um navegador usam o navegador para quase todas as comunicações com o servidor, eles podem aproveitar o suporte pré-constituído para SSL para a criptografia. Além disso, os bytes de um aplicativo Macromedia Flash podem ser criptografados enquanto estão sendo carregados em um navegador. Executando um aplicativo Flash dentro de um navegador ativado para SSL através de uma conexão HTTPS com o servidor, as organizações e usuários podem assegurar que a comunicação entre o Flash Player e o servidor seja criptografada e segura.

Facilidade de Integração com Aceleradores SSL e Balanceadores de Carga

A integração com aceleradores SSL e balanceadores de carga padrão é simples. Por exemplo, como o servidor de apresentação Flex manuseia solicitações que são inicialmente recebidas por um servidor web, o servidor Flex não precisa saber qual protocolo está sendo usado. Para mudar de HTTP para HTTPS, o administrador do servidor simplesmente modifica o servidor web como ele o faria sem o servidor Flex instalado.

Suporte para Envelopamento Criptografado

Os aplicativos construídos com o Flash Media Server usam o Real-time Messaging Protocol (RTMP) para a transmissão de alto desempenho de áudio, vídeo e mensagens de dados em um único canal de dados entre o cliente e o servidor. Apesar do RTMP não incluir recursos específicos de segurança, os aplicativos de comunicações Flash podem executar transações seguras e autenticação segura através de um servidor web ativado para SSL. Ao executar dentro de um servidor web, o Flash Player pode usar envelopamento HTTPS criptografado seguro para se comunicar através de RTMP. Esse suporte para envelopamento fornece aos usuários por trás de uma firewall corporativa típica uma experiência transparente enquanto garante o transporte seguro de dados.

Exemplo de Solução: Serviço Speedera Flash Video Streaming

O parceiro da Macromedia, Speedera, fornece Flash Video seguro sobre SSL através do Flash Media Server. Os usuários visitam o site de um fornecedor de conteúdo e são autenticados através de uma senha. Uma chave com hashing é gerada e o usuário é redirecionado para o servidor Speedera após a verificação de maneira transparente. Com a entrega segura de Flash Video, o conteúdo pode ser executado somente no website intencionado; ele não pode ser colocado em outros sites. Além disso, a URL streaming não pode ser enviada em massa para usuários que não foram autorizados a usá-lo.

Conclusão

Com a Plataforma Flash, as organizações podem desenvolver, implantar e distribuir RIAs, aplicativos empresariais e móveis e comunicações para funcionários, parceiros e clientes com confiança. O Flash Player e a linha de produtos Flex alavancam a infra-estrutura de segurança existente de uma organização (o que significa que são independentes em relação à segurança) baseado em padrões existentes aceitos e usando tecnologias seguras. Devido à maneira que a Plataforma Flash e a linha de produtos Flex integram com as atuais soluções para autenticação, controle de acesso, transporte de dados e prevenção contra código malicioso, eles não afetam de maneira adversa a habilidade de uma organização de obedecer às exigências de segurança. Tão importante quanto isso, essa abordagem assegura a contínua obediência às melhores práticas e regulamentações de segurança como a Lei Sarbanes-Oxley de 2002 e a HIPAA. E, alavancando a atual infra-estrutura de segurança de uma organização, a Plataforma Flash possibilita a implantação de sucesso de aplicativos seguros sem maiores investimentos.

De acordo com uma avaliação independente de segurança da @stake, a Macromedia desenvolveu um forte modelo de proteção de informações contra ameaças no lado cliente. “A arquitetura [Flex] diminui muitas das ameaças comuns no lado servidor como scripting cruzado de site, *denial-of-services* [ataques], injeção de SQL, *man-in-the-middle* [ataques] e seqüestro de sessão.” Além disso, a segurança no lado servidor é mantida alavancando segurança J2EE para diminuir ataques comuns contra componentes da infra-estrutura, como estouros de buffer, corrupção de heap e scripting cruzado de site.

Para Obter Maiores Informações

Para obter maiores informações sobre a Plataforma Flash, ligue para um representante de vendas no número 1-888-649-2990 (EUA e Canadá) ou encontre uma linha internacional de vendas em www.macromedia.com/international/buy/numbers.html. Para comprar on-line, visite www.macromedia.com/store. Ou use qualquer um dos links abaixo:

- Para obter maiores informações sobre a Plataforma Flash, visite www.macromedia.com/br/platform
- Para obter maiores informações sobre o Flash Player, visite www.macromedia.com/software/flashplayer/
- Para obter maiores informações sobre a ferramenta de autoria Flash, visite www.macromedia.com/software/flash/
- Para obter maiores informações sobre o Flex Builder, visite www.macromedia.com/software/flex/flexbuilder/
- Para obter maiores informações sobre o servidor de apresentações Flex, visite www.macromedia.com/software/flex/
- Para obter maiores informações sobre o Flash Media Server, visite www.macromedia.com/software/flashcom/
- Para obter maiores informações sobre os Flash Video Streaming Services, visite www.macromedia.com/software/flashcom/fvss/
- Para obter maiores informações sobre O Breeze, visite www.macromedia.com/software/breeze/
- Para obter maiores informações sobre Segurança Macromedia, visite www.macromedia.com/resources/security

Referências

Defense in Depth: Information Assurance and Computer Network Defense (CJCSM 6510.01), Joint Chiefs of Staff, Agosto de 2004 (www.dtic.mil/cjcs_directives)

Macromedia Breeze 5 Security Assessment, Symantec, Julho de 2005 (www.macromedia.com/support/breeze/licensed_docs/macromedia-cfd-breeze5.pdf)

Macromedia Flash Player 8 Security, Macromedia, Agosto de 2005 (www.macromedia.com/deent/plashplayer/articles/flash_player_8_security.pdf)

Macromedia Flex Product Briefing, @Stake, Agosto de 2004 (www.macromedia.com/devnet/flex/articles/flex_security_wp.pdf)

OWASP Top Ten Most Critical Web Application Security Vulnerabilities, The Open Web Application Security Project (www.owasp.org/documentation/top10.html)

Policy Guidance for use of Mobile Code Technologies in Department of Defense (DoD) Information Systems Memorandum, U.S. Department of Defense, Novembro de 7, 2000 (www.dod.mil/nii/org/cio/doc/mobile-code11-7-00.html)