macromedia® white paper

Macromedia Flash MX-Sicherheit

von Mike Chambers

März 2002

Macromedia, Inc.
600 Townsend Street
San Francisco, CA 94103 USA
415-252-2000

Inhalt

Für Macromedia hat das Thema Sicherheit höchste Priorität. Wir unternehmen daher alle denkbaren Schritte, um sicherzustellen, dass Macromedia Flash eine sichere Technologie ist, die die Privatsphäre und Daten der Benutzer schützt. In diesem Dokument wird auf das Thema Sicherheit und Datenschutz im Zusammenhang mit Macromedia Flash-Inhalten eingegangen, darunter auf eine Reihe potenzieller Sicherheitsprobleme beim Abspielen von Inhalten vom lokalen Dateisystem, die aus zwielichtigen oder unbekannten Quellen stammen.

Einführung in Macromedia Flash MX

Was ist Macromedia Flash MX?

Das volle Potenzial des Internets ist noch nicht erschlossen. Bislang wurde es beschränkt durch das Benutzererlebnis im Web, das sich leider durch einen Mangel an benutzerzentrierten Designs und Technologien auszeichnet.

Die *Suche* nach Informationen, die im Internet von heute im Vordergrund steht, wird schon bald durch *aktives Handeln* im Internet abgelöst. Ob Sie nun einen Flug buchen, Ihre Firma managen oder mit Freunden kommunizieren, als Webbenutzer interagieren Sie in wachsendem Maße mit dem Internet. Damit dies erfolgreich sein kann, müssen Inhalte und Einsatzmöglichkeiten von Internetanwendungen noch beträchtlich verbessert werden.

Doch ab sofort weht frischer Wind. Das Internet wird durch standardmäßige Rich-Client-Technologie gesteuert, die das Erlebnis seiner Benutzer so umwandelt, dass Organisationen und Menschen Multimedia-Inhalte und -Anwendungen effizienter als je zuvor auf einer breiten Palette von Geräten und Plattformen einsetzen können.

Der Macromedia Flash Player, der Rich-Client von Macromedia, ist die am weitesten verbreitete Software in der Geschichte des Internets und wird mit Internet Explorer, AOL, Netscape Navigator, Opera und Windows XP ausgeliefert. Mehr als 414 Millionen Webbenutzer können Macromedia Flash-Inhalte sofort anzeigen, ohne einen Player herunterladen zu müssen. Der Macromedia Flash Player steht auch auf einer wachsenden Anzahl von Geräten mit Internetanbindung zur Verfügung, wie drahtlosen Handhelds, iTV und Spielkonsolen.

Die Macromedia Flash MX-Lösung verbindet die weit verbreitete Client-Technologie des Macromedia Flash Players mit der Macromedia Flash MX-Entwicklungsumgebung und optimierter, serverseitiger Konnektivität. Damit wird die Entwicklung von Rich-Media-Internetanwendungen drastisch beschleunigt. Das Erlebnis für Endbenutzer und Online-Kunden wird so lebendig, konsistent und interessant.

Warum ist Macromedia Flash MX sicher?

Der Macromedia Flash Player weist eine umfangreiche Liste an Kontrollen, Beschränkungen und Leistungsmerkmalen auf, mit denen die Sicherheit von Macromedia Flash-Inhalten gewährleistet wird. Dazu gehört Folgendes:

- Mithilfe browserseitiger Verschlüsselungsfunktionen wie SSL kann die gesamte Kommunikation zwischen Macromedia Flash-Filmen und Servern verschlüsselt werden.
- Ein umfassendes Sandbox-Security-System schränkt die Übertragung von Daten ein, die ein Sicherheitsrisiko darstellen.
- Der Macromedia Flash Player verhindert, dass Webinhalte Daten vom lokalen Festplattenlaufwerk lesen. Ausnahme: SharedObjects, die von der betreffenden Domäne erstellt wurden.
- Der Macromedia Flash Player kann nur Daten auf die Festplatte schreiben, die in SharedObjects enthalten sind.
- Der Macromedia Flash Player gestattet Webinhalten nur das Lesen von Daten auf einem Server, der sich in der gleichen Domäne befindet, es sei denn, der Zugriff wurde ausdrücklich genehmigt.
- Der Macromedia Flash Player verhindert, dass Webinhalte von einer einzigen Domäne aus mehr als 100 KB an Daten auf der lokalen Festplatte ablegen.
- Der Macromedia Flash Player ermöglicht dem Benutzer das Deaktivieren der Datenspeicherung für beliebige Domänen.
- Der Macromedia Flash Player gestattet das Senden von Daten von einer Kamera oder einem Mikrofon erst dann, wenn der Benutzer die Genehmigung für eine Domäne erteilt.

Wie schützt Macromedia Flash MX die Privatsphäre seiner Benutzer?

Macromedia weiß, wie wichtig die Privatsphäre der Benutzer ist, und hat dafür gesorgt, dass Macromedia Flash-Inhalte diese Privatsphäre in keiner Weise beeinträchtigen.

Dies wird wie folgt realisiert:

- Benutzer müssen den Zugriff auf lokale Webkameras und Mikrofone ausdrücklich genehmigen.
- Eine Domäne kann nicht auf gespeicherte Daten zugreifen, die von einer anderen Domäne stammen. Ganz ähnlich funktionieren auch Webbrowser-Cookies.
- Macromedia Flash hat keinen Zugriff auf persönliche Informationen, es sei denn, der Benutzer gibt sie eigens ein.

Sandbox-Modell des Macromedia Flash Players 6

Der Macromedia Flash Player 6 implementiert ein browserähnliches Sandbox-Security-Schema, um Schutz und Sicherheit des Macromedia Flash-Films und des Client-Rechners zu gewährleisten.

Was versteht man unter einer Sandbox?

Die so genannte Sandbox („Sandkasten“) ist nichts anderes als ein klar abgegrenzter Bereich, in dem ein Macromedia Flash-Film, der im Macromedia Flash Player abgespielt wird, operieren darf. Hauptzweck einer Sandbox ist die Gewährleistung optimaler Integrität und Sicherheit sowohl des Client-Rechners als auch der Macromedia Flash-Filme, die im Player ablaufen.

Das Konzept der Sandbox ist simpel. Ein Macromedia Flash-Film wird in einer Sandbox ausgeführt. Alle Informationen in der Sandbox können nur an die Domäne übertragen werden, aus der der Film stammt. Der Zugriff auf Informationen in der Sandbox von außen ist stark eingeschränkt.

Die Sandbox eines Macromedia Flash-Films setzt sich aus folgenden Bestandteilen zusammen:

- dem kompletten Inhalt der SWF-Datei
- Benutzeraktionen, die an den Flash-Film gerichtet sind
- Servern in der Domäne, aus der der Macromedia Flash-Film stammt (siehe dazu den Abschnitt *Domänenbasierte Authentifizierung* weiter unten)
- lokalen SharedObjects, die von Macromedia Flash-Filmen aus der gleichen Domäne geschrieben wurden (siehe dazu den Abschnitt *E/A-Zugriff auf lokale Dateien* weiter unten)
- beschränkten Konfigurationsinformationen zu dem Computer, auf dem der Macromedia Flash-Film ausgeführt wird

Damit Entwickler lokale Entwicklungs- und Testarbeiten an Macromedia Flash-Filmen durchführen können, weisen Filme, auf die als lokale Dateien zugegriffen wird (entweder auf der lokalen Festplatte des Endbenutzers oder auf LAN-Servern), keinerlei Sandbox-Beschränkungen auf. Dies steht im Einklang mit der bewährten Grundregel, dass Benutzer beim lokalen Ausführen von Dateien grundsätzlich besondere Vorsicht walten lassen sollten.

Domänenbasierte Authentifizierung

Wie bereits erwähnt, umfasst die Sandbox sämtliche Server der Domäne, aus der der Film stammt, oder um genau zu sein, der „Subdomäne der *n*ten Stufe“. Die Mitgliedschaft in der Domäne wird durch Vergleich der Servernamen überprüft.

Zwei Server sind in der gleichen Domäne, wenn die folgenden Bedingungen erfüllt sind:

1. Die Servernamen weisen die gleiche Anzahl an Token auf.
2. Es gibt mindestens 3 Token.
3. Alle Token mit Ausnahme des ersten Token sind gleich, abgesehen von Unterschieden in der Groß- und Kleinschreibung.

Wenn der Name eines Servers nur in einem oder zwei Token ausgedrückt ist (beispielsweise „foo“ für „foo.macromedia.com“), befindet sich der Server in einer eigenen Domäne. Wenn ein Server durch seine IP-Adresse identifiziert wird, befindet er sich ebenfalls in einer eigenen Domäne.

Beispiele:

- „A.B.macromedia.com“ und „C.b.macromedia.com“ sind in der gleichen Domäne.
- „A.b.macromedia.com“ und „www.macromedia.com“ sind nicht in der gleichen Domäne (unterschiedliche Anzahl an Token).
- „A.b.macromedia.com“ und „a.c.macromedia.com“ sind nicht in der gleichen Domäne (zweites Token ist unterschiedlich).

Der Grundgedanke hier ist, dass eine große Domäne in voneinander abgeschirmte Subdomänen eingeteilt werden kann, indem zusätzliche Token in Servernamen verwendet werden. Dieser Algorithmus gilt auch für URLs, die Länderabkürzungen enthalten (wie etwa „http://www.hrp.org.uk/“).

Durch Beschränkung auf Servernamen mit einem und zwei Token und Server, die durch IP-Adressen identifiziert werden, lassen sich schwer zu berechnende Fälle vermeiden, wie etwa wenn ein Benutzer in seiner TCP/IP-Konfiguration mehrere Suchdomänen hat. Es folgen zwei Beispiele, die ein Resultat dieser Beschränkung sind:

- „foo“ und „bar“ befinden sich nicht in der gleichen Domäne, aber „foo.macromedia.com“ und „bar.macromedia.com“ schon.
- „www.macromedia.com“ und „macromedia.com“ befinden sich nicht in der gleichen Domäne, obwohl sie den gleichen Server ansprechen.

Durch diese Domänenbeschränkung soll verhindert werden, dass Server hinter Firewalls von Rechnern außerhalb der Firewall angegriffen werden können. Ein Film von „outside.hacker.org“ darf nicht in der Lage sein, Dateien auf „inside.macromedia.com“ zu lesen, wenn der Film auf einem Computer hinter der Macromedia-Firewall abgespielt wird.

Wie wird die Sandbox implementiert?

E/A-Zugriff auf lokale Dateien

Mithilfe von SharedObjects ermöglicht der Macromedia Flash Player 6 das eingeschränkte Speichern lokaler Dateien. SharedObjects, die Sie sich als eine Art Webbrowser-Cookies vorstellen können, ermöglichen Entwicklern das Speichern und Abrufen von Daten auf dem lokalen Dateisystem der Benutzer.

SharedObjects weisen folgende Einschränkungen auf:

- Daten können nur in ein bestimmtes Verzeichnis geschrieben werden. Der Entwickler hat keine Kontrolle über dieses Verzeichnis.
- Der Benutzer kann bestimmen, welche Datenmengen gespeichert werden können, und kann die Speicherung je nach Domäne deaktivieren.

- Lokal gespeicherte Daten sind binär und serialisiert und werden vom Macromedia Flash Player gesteuert. Die Dateien weisen einen Standard-Header auf und haben die Erweiterung .SO. Dadurch wird verhindert, das ausführbarer Code bzw. Anwendungsdaten gespeichert werden, die vom Benutzer versehentlich gestartet werden könnten.
- Der Datenzugriff wird durch die domänenbasierten Authentifizierungsregeln des Macromedia Flash Players eingeschränkt (siehe dazu den Abschnitt *Domänenbasierte Authentifizierung* weiter oben).

Der Dateiaustausch über den Macromedia Flash Player ist auf ein bestimmtes Verzeichnis auf dem Client-Rechner beschränkt, das vom Macromedia Flash Player 6 erstellt wird. Für das Verzeichnis gelten die folgenden Einschränkungen, wenn der Zugriff von einem Macromedia Flash-Film aus erfolgt, der in einem Webbrowser abgespielt wird:

- Der Benutzer steuert, welche Datenmenge für eine bestimmte Domäne gespeichert werden kann. Standardmäßig kann jede Domäne 100 KB auf dem Computer des Benutzers speichern. Jedes SharedObject ist in einer eigenen Datei gespeichert. Zu Kalkulationszwecken wird davon ausgegangen, dass jede Datei mindestens 1000 Bytes belegt; bei einem Standardgrenzwert von 100 KB sind also pro Domäne bis zu 100 unterschiedliche SharedObjects möglich.
- Die Daten für jede Domäne werden in einem separaten Verzeichnis im Verzeichnis mit den Anwendungsdaten gespeichert. Der Benutzer hat Zugriff auf dieses Verzeichnis.

Durch diese Einschränkungen wird Folgendes sichergestellt:

- Nicht-Flash-Daten auf dem Benutzercomputer können nicht durch einen Macromedia Flash-Film überschrieben werden, der in einem Browser ausgeführt wird.
- Das Risiko von „Denial of Service“-Angriffen, die durch ein Datenbombardement der Festplatte des Benutzers herbeigeführt werden, wird stark eingeschränkt.

Der Player steuert das Format der Daten, die vom Macromedia Flash Player auf dem Dateisystem des Benutzers gespeichert werden. Entwickler können das Format dieser Daten nicht beeinflussen. Bei den Daten handelt es sich um eine binäre Serialisierung der zu speichernden Daten; daher können sie nicht zu Angriffen auf den Clientcomputer verwendet werden.

Auf Daten in SharedObjects kann nur im Einklang mit den oben erläuterten Domänenregeln zugegriffen werden. Dies bedeutet beispielsweise, dass ein Film aus der Domäne www.domain2.com nicht auf Daten in einem SharedObject zugreifen kann, das durch einen Film aus der Domäne www.domain1.com erstellt wurde.

Filmübergreifende Kommunikation

Das Macromedia Flash Player-Sandbox-System gilt auch, wenn eine SWF-Datei in einen vorhandenen Macromedia Flash-Film geladen wird. Filme, die von separaten Domänen aus geladen werden, existieren jedoch in einer eigenen Sandbox und sind vor anderen Filmen isoliert, die gegenwärtig im Player ausgeführt werden. Inhalte in der Sandbox eines Films können nicht über die Sandbox hinaus vordringen, und Inhalte außerhalb der Sandbox haben keine Einsicht in die Sandbox.

Filme können miteinander über das LocalConnection-Objekt kommunizieren. Das Sandbox-Sicherheitsmodell trifft auch auf die filmübergreifende Kommunikation unter Verwendung dieser Methode zu. Die wichtigste Regel hier ist, dass ein Film in Domäne A keine Daten aus einem Film in Domäne B extrahieren kann, es sei denn, der Film in Domäne B erteilt Domäne A ausdrücklich die Zugriffsgenehmigung. Wie bereits erwähnt, muss diese Regel unter allen Umständen eingehalten werden, um zu verhindern, dass eine SWF-Datei aus öffentlichen Bereichen des Internets eine SWF-Datei hinter einer Firewall lädt und Daten extrahiert. Als Ergebnis erhält jede Sandbox eine eigene Kopie des Scope-Objekts `_global`. Code in einer bestimmten Sandbox kann nur auf das Global-Objekt für die betreffende Sandbox zugreifen.

Manchmal kann es jedoch vorkommen, dass zwei Filme, die in unterschiedlichen Domänen residieren, gegenseitig auf ihre Daten zugreifen müssen. Das Macromedia-Bedienfeld **Antworten** wird zum Beispiel vom Macromedia Flash-Authoring-Tool von der lokalen Festplatte aus geladen, muss jedoch gelegentlich durch Zugriff auf die Macromedia-Website aktualisiert werden. In diesem Fall ist es erforderlich, dass ein Film, der von www.macromedia.com geladen wird, Daten mit dem Film austauscht, der von der lokalen Festplatte geladen wurde.

Dies wird mithilfe der so genannten Tunneling-Funktion der Sandbox erzielt. Das Tunneling erfolgt über dieActionScript-Methode `System.security.allowDomain` und weist die folgende Syntax auf:

```
System.security.allowDomain(domäne1, ..., domäneN);
```

Dieser Befehl ermöglicht Domäne1 bis Domäne*N* Zugriff auf die Sandbox der SWF-Datei, die den Befehl ausführt.

Das Bedienfeld **Antworten** im Macromedia Flash MX-Authoring-Tool weist beispielsweise eine Shim-SWF-Datei auf, die als lokale Datei geladen wird. Die SWF-Datei für das Bedienfeld **Antworten**, die von macromedia.com geladen wird, benötigt Zugriff auf die Shim-Variablen. Die Shim-Datei ruft also Folgendes auf:

```
System.security.allowDomain("macromedia.com");
```

Mit diesem Befehl wird macromedia.com zur „Vertrauten“-Liste der Shim-Datei hinzugefügt. Eine SWF-Datei, die von macromedia.com oder Subdomänen wie sub.macromedia.com aus geladen wird, kann nun auf Variablen in der Shim-SWF-Datei zugreifen.

Wenn der Zugriff einmal gestattet wurde, kann er nicht widerrufen werden, und es kann keine Liste zugelassener Domänen abgerufen werden.

Zwischen Sandboxen ist eine eingeschränkte Kommunikation möglich. ActionScript-Code in einer Sandbox kann einen Bezug auf das Top-Level-Objekt einer anderen Sandbox erhalten und die Movieclip-Eigenschaften modifizieren. Wenn movie1.swf beispielsweise movie2.swf in den Movieclip _level0.mcHolder lädt, trifft Folgendes zu:

- movie1.swf kann auf _level0.mcHolder zugreifen und die Movieclip-Eigenschaften modifizieren.
- movie1.swf kann auf keine weiteren Eigenschaften von _level0.mcHolder zugreifen.

Die verfügbaren Movieclip-Eigenschaften sind im Ordner **Eigenschaften** in der Werkzeugleiste des Bedienfelds **Aktionen** aufgelistet. Hierzu gehören folgende Eigenschaften:

- _alpha
- _currentframe
- _droptarget
- _focusrect
- _framesloaded
- _height
- _name
- _quality
- _rotation
- _soundbuftime
- _target
- _totalframes
- _url
- _visible
- _width
- _x
- _xmouse
- _xscale
- _y
- _ymouse
- _yscale

In der folgenden Tabelle sind die grundlegenden ActionScript-Funktionen und die jeweiligen Sicherheitsbeschränkungen aufgelistet.

Tabelle 1: *Sicherheitsbeschränkungen für grundliegende Aktionen*

Funktion	Sicherheitsbeschränkung
gotoAndPlay/gotoAndStop	Keine Sicherheitsbeschränkung, es sei denn, ein Pfad ist angegeben, wie etwa: `gotoAndPlay("mc:1");` Ist ein Zielpfad angegeben, muss sich der aufrufende Movieclip in der gleichen Sandbox befinden wie der Ziel-Movieclip.
play	Keine Sicherheitsbeschränkung
stop	Keine Sicherheitsbeschränkung
toggleHighQuality	Keine Sicherheitsbeschränkung
stopAllSounds	Keine Sicherheitsbeschränkung
getURL	Keine Sicherheitsbeschränkung
FSCommand	Der aufrufende Movieclip muss sich in der gleichen Sandbox befinden wie die HTML-Seite
loadMovie	Keine Sicherheitsbeschränkung
loadMovieNum	Keine Sicherheitsbeschränkung
unloadMovie	Keine Sicherheitsbeschränkung
unloadMovieNum	Keine Sicherheitsbeschränkung
loadVariables	Der aufrufende Movieclip muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
loadVariablesNum	Der aufrufende Movieclip muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
tellTarget	Der aufrufende Movieclip muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
ifFrameLoaded	Keine Sicherheitsbeschränkung
print	Keine Sicherheitsbeschränkung
printNum	Keine Sicherheitsbeschränkung
printAsBitmap	Keine Sicherheitsbeschränkung
printAsBitmapNum	Keine Sicherheitsbeschränkung

Die Sandbox-Beschränkungen gelten nicht für Macromedia Flash-Filme und -Projektoren, die vom lokalen Dateisystem aus geladen werden. Es gibt jedoch eine Ausnahme:

Eine Sandbox eines Flash-Films, bei dem es sich nicht um eine lokale Datei handelt, kann nicht auf die Sandbox einer lokalen Datei zugreifen. Wenn beispielsweise movie1.swf auf der lokalen Festplatte eines Benutzers movie2.swf von einem HTTP-Server lädt, treffen die folgenden Aussagen zu:

- movie1.swf und movie2.swf erhalten separate Sandboxen.
- movie1.swf kann auf den Inhalt von movie2.swf zugreifen.
- movie2.swf kann nicht auf den Inhalt von movie1.swf zugreifen.

Flash-JavaScript-Kommunikation

Der Macromedia Flash Player unterstützt eine JavaScript-API zum Steuern von Filmeigenschaften, zum Einstellen und Abrufen von Variablen und zum Aufrufen von Funktionen. Auch diese Fähigkeiten werden durch das Sandbox-Sicherheitsmodell des Macromedia Flash Players eingeschränkt.

LiveConnect-API

Die Netscape-Plug-In-Version des Macromedia Flash Players stellt eine API über die LiveConnect-Schnittstelle von Netscape Navigator zur Verfügung. Auf diese API kann von Java und JavaScript direkt von Netscape Navigator aus zugegriffen werden.

Die Sicherheitsbeschränkungen für die LiveConnect-API sind die gleichen wie die Sandbox-Beschränkungen für ActionScript. Eine ähnliche Sandbox wird für die HTML-Seite anhand ihrer URL erstellt. Für diese Sandbox gelten die normalen Regeln. Auf Variablen in einer Sandbox kann nicht von einer anderen Sandbox aus zugegriffen werden. Movieclips in einer anderen Sandbox lassen sich nicht steuern. Die Movieclip-Eigenschaften eines Top-Level-Movieclips in einer anderen Sandbox können gelesen, aber nicht geändert werden.

In der folgenden Tabelle sind die Eigenschaften und Methoden der LiveConnect-API sowie die entsprechenden Sicherheitsbeschränkungen aufgelistet.

Tabelle 2: *Sicherheitsbeschränkungen für die Macromedia Flash Player-LiveConnect-API*

Java/JavaScript-Methode	Sicherheitsbeschränkung
boolean IsPlaying();	Keine Sicherheitsbeschränkung
void Play();	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
void StopPlay();	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
int TotalFrames();	Keine Sicherheitsbeschränkung
int CurrentFrame();	Keine Sicherheitsbeschränkung
void GotoFrame(int position);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
void Rewind();	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
void Back();	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
void Forward();	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
int PercentLoaded();	Keine Sicherheitsbeschränkung
boolean FrameLoaded(int frameNum);	Keine Sicherheitsbeschränkung
int FlashVersion();	Keine Sicherheitsbeschränkung
void Pan(int x, int y, int mode);	Keine Sicherheitsbeschränkung
void Zoom(int percent);	Keine Sicherheitsbeschränkung
void SetZoomRect(int left, int top, int right, int bottom);	Keine Sicherheitsbeschränkung

Java/JavaScript-Methode	Sicherheitsbeschränkung
void LoadMovie(int layer, String url);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
void TGotoFrame(String target, int frameNum);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TGotoLabel(String target, String label);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
int TCurrentFrame(String target);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
String TCurrentLabel(String target);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TPlay(String target);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TStopPlay(String target);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void SetVariable(String name, String value);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
String GetVariable(String name);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
void TSetProperty(String target, int property, String value);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
String TGetProperty(String target, int property);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TCallFrame(String target, int frameNum);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TCallLabel(String target, String label);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
double TGetPropertyAsNumber(String target, int property);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
void TSetProperty(String target, int property, double value);	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip

Hinweis: Falls LiveConnect nicht verfügbar ist, können diese Befehle nicht verwendet werden, und die Sicherheitsbeschränkungen treffen nicht zu.

ActiveX-Steuerungs-API

Beim Macromedia Flash Player für die Windows-Version des Internet Explorers handelt es sich um eine ActiveX-Steuerung. Diese ActiveX-Steuerung unterstützt eine COM-API zum Abfragen von Eigenschaften und zum Manipulieren von Macromedia Flash-Filmen.

Diese API wird am häufigsten von JavaScript-Code auf derselben HTML-Seite wie ein Macromedia Flash-Film verwendet. Die ActiveX-API weist starke Ähnlichkeiten mit der LiveConnect-API auf, die im Netscape Navigator für JavaScript bereitgestellt wird.

Die Sicherheitsbeschränkungen für die ActiveX-Steuerungs-API sind die gleichen wie die Sandbox-Beschränkungen für ActionScript. Eine ähnliche Sandbox wird für die HTML-Seite anhand ihrer URL erstellt. Für diese Sandbox gelten die normalen Regeln. Auf Variablen in einer Sandbox kann nicht von einer anderen Sandbox aus zugegriffen werden. Movieclips in einer anderen Sandbox lassen sich nicht steuern. Die Movieclip-Eigenschaften eines Top-Level-Movieclips in einer anderen Sandbox können gelesen, aber nicht geändert werden.

In der folgenden Tabelle sind die Eigenschaften und Methoden der ActiveX-Steuerungs-API sowie die entsprechenden Sicherheitsbeschränkungen aufgelistet.

Tabelle 3: *Sicherheitsbeschränkungen für die Macromedia Flash Player-ActiveX-Steuerungs-API*

Eigenschaft/Methode	Sicherheitsbeschränkung
Eigenschaft SWRemote	Keine Sicherheitsbeschränkung
Methode TGetPropertyNum	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TSetPropertyNum	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TCallLabel	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TCallFrame	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TGetProperty	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TSetProperty	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode GetVariable	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
Methode SetVariable	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
Methode TStopPlay	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
Methode TPlay	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie das Container-Objekt der Variablen
Methode TCurrentLabel	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TCurrentFrame	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TGotoLabel	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Methode TGotoFrame	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie der Ziel-Movieclip
Eigenschaft Quality2	Keine Sicherheitsbeschränkung
Eigenschaft BGColor	Keine Sicherheitsbeschränkung
Eigenschaft EmbedMovie	Keine Sicherheitsbeschränkung
Eigenschaft DeviceFont	Keine Sicherheitsbeschränkung
Eigenschaft Scale	Keine Sicherheitsbeschränkung
Eigenschaft Base	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Eigenschaft Menu	Keine Sicherheitsbeschränkung

Eigenschaft/Methode	Sicherheitsbeschränkung
Eigenschaft SAlign	Keine Sicherheitsbeschränkung
Eigenschaft WMode	Keine Sicherheitsbeschränkung
Eigenschaft PercentLoaded	Keine Sicherheitsbeschränkung
Methode Pan	Keine Sicherheitsbeschränkung
Methode Zoom	Keine Sicherheitsbeschränkung
Methode SetZoomRect	Keine Sicherheitsbeschränkung
Eigenschaft FrameNum	LESEN: Keine Sicherheitsbeschränkung; SCHREIBEN: Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Eigenschaft Movie	Keine Sicherheitsbeschränkung
Eigenschaft Loop	LESEN: Keine Sicherheitsbeschränkung; SCHREIBEN: Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Eigenschaft BackgroundColor	Keine Sicherheitsbeschränkung
Eigenschaft AlignMode	Keine Sicherheitsbeschränkung
Eigenschaft ScaleMode	Keine Sicherheitsbeschränkung
Eigenschaft Quality	Keine Sicherheitsbeschränkung
Eigenschaft Playing	LESEN: Keine Sicherheitsbeschränkung; SCHREIBEN: Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Eigenschaft TotalFrames	Keine Sicherheitsbeschränkung
Eigenschaft ReadyState	Keine Sicherheitsbeschränkung
Methode FlashVersion	Keine Sicherheitsbeschränkung
Methode FrameLoaded	Keine Sicherheitsbeschränkung
Methode CurrentFrame	Keine Sicherheitsbeschränkung
Methode GotoFrame	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Rewind	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Forward	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Back	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
IsPlaying	Keine Sicherheitsbeschränkung
Stop	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
StopPlay	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Play	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
LoadMovie	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0
Eigenschaft FlashVars	Die HTML-Seite muss sich in der gleichen Sandbox befinden wie _level0

Sicherheit der Datenübertragung

Datenverschlüsselung mit SSL

Für einen Macromedia Flash-Film, der in einem Browser abgespielt wird, gelten weitgehend die gleichen Sicherheitsauflagen wie für eine in einem Browser angezeigte HTML-Seite. Dazu zählt etwa die Sicherheit des Macromedia Flash-Films, während er in den Browser geladen wird, sowie die Sicherheit der Kommunikation zwischen Macromedia Flash und dem Server, nachdem der Film geladen wurde und im Browser abgespielt wird. Insbesondere die Datenkommunikation zwischen Browser und Server ist sehr anfällig für Lauschangriffe durch Dritte. Bei HTML besteht die Lösung für dieses Problem darin, die Kommunikation zwischen Client und Server zu verschlüsseln, um Daten, die von Außenseitern abgefangen werden könnten, unverständlich und damit nutzlos zu machen. Dies erfolgt durch einen SSL-fähigen Browser und Server.

Da Macromedia Flash-Filme, die in einem Browser abgespielt werden, den Browser für praktisch die gesamte Kommunikation mit dem Server verwenden, können sie die in den Browser integrierte SSL-Unterstützung nutzen. So kann die Kommunikation zwischen dem Macromedia Flash-Film und dem Server verschlüsselt werden. Auch die eigentlichen Bytes des Macromedia Flash-Films werden verschlüsselt, wenn sie in den Browser geladen werden.

Wenn Sie also einen Macromedia Flash-Film in einem SSL-fähigen Browser über eine HTTPS-Verbindung zum Server abspielen, können Sie davon ausgehen, dass die Kommunikation zwischen dem Macromedia Flash Player und dem Server verschlüsselt und sicher ist.

Eine Ausnahme bildet die Verwendung persistenter Sockets durch Macromedia Flash (über das ActionScript-XMLSocket-Objekt); hierbei wird zur Kommunikation mit dem Server der Browser nicht eingesetzt. Aus diesem Grund können die in den Browser integrierten Verschlüsselungsfunktionen nicht verwendet werden. Es ist allerdings möglich, in ActionScript verfasste unidirektionale Verschlüsselungsalgorithmen zu verwenden, um die zu übertragenden Daten zu verschlüsseln.

Unidirektionale Datenverschlüsselung in Macromedia Flash MX mit md5

Bei md5 handelt es sich um einen unidirektionalen Verschlüsselungsalgorithmus, der in *rfc1321* beschrieben ist. Dieser Algorithmus wurde auf ActionScript portiert und sorgt dafür, dass Entwickler unidirektionale Daten mithilfe des md5-Algorithmus verschlüsseln können, bevor sie vom Macromedia Flash-Film an den Server gesendet werden. Weitere Informationen zu rfc1321 finden Sie unter http://www.faqs.org/rfcs/rfc1321.html und http://www.rsasecurity.com/rsalabs/faq/3-6-6.html.

Der md5-Algorithmus erstellt einen sicheren, unidirektionalen Hash aus einem String. Der Hash kann nicht zurück in den Originalstring entschlüsselt werden, lässt sich allerdings mit anderen Daten vergleichen, die mithilfe des md5-Algorithmus verschlüsselt wurden. Diese Methode bietet zwar nicht die gleichen Möglichkeiten zum Ver- und Entschlüsseln wie SSL, kann allerdings nützlich sein, wenn Sie sensitive Daten übertragen müssen und nicht die SSL-Funktionen eines Browsers verwenden können.

Beispiele:

- Ein Film muss in einem Browser ausgeführt werden können, der nicht SSL-fähig ist.
- Sie haben keinen Zugriff auf einen SSL-fähigen Webserver.
- Sie müssen über einen XLM-Socket mit dem Server kommunizieren.
- Sie verwenden zum Ausführen des Films einen Macromedia Flash-Projektor.

Der Prozess der Datenverschlüsselung sieht wie folgt aus:

1. Macromedia Flash verschlüsselt die Daten mit einem unidirektionalen Hash.
2. Macromedia Flash sendet die Daten an den Server.
3. Der Server empfängt die Daten.
4. Der Server validiert den unidirektionalen Hash auf Grundlage eines bereits vorhandenen Hash.

Ein in ActionScript geschriebener md5-Algorithmus kann von der folgenden Website heruntergeladen werden: http://flashexperiments.insh-allah.com/#MD5.

Sicherheit der Datenübertragung bei Macromedia Flash MX-Projektoren

Da Macromedia Flash-Projektoren ausführbare Dateien sind, die außerhalb eines Browsers ausgeführt werden, können sie die SSL-Funktionen eines Browsers nicht nutzen. Aus diesem Grund sollten Sie vor der Übertragung sensitiver Daten zwischen dem Projektor und einem Server entweder:

- die Daten selbst mit einem ActionScript-Algorithmus wie md5 (siehe oben) verschlüsseln oder
- von Ihren Benutzern verlangen, dass sie eine sichere Netzwerkverbindung zum Server verwenden, wie beispielsweise eine VPN-Verbindung (Virtual Private Network).

Sicherheit von Daten und Algorithmen in einem Macromedia Flash MX-Film

Der folgende Abschnitt erläutert die Sicherheit und Integrität von Daten und Algorithmen, die in einer kompilierten Macromedia Flash-Filmdatei (SWF) enthalten sind. Er untersucht die Fähigkeit, Daten aus einer SWF-Datei zu extrahieren, und beschreibt erprobte Verfahren zur Gewährleistung der Sicherheit und Integrität von Daten und Algorithmen in einer SWF-Datei.

Sicherheitsthematik bei einer Technologie mit offenem Format

Wie bereits erwähnt, treten bei Macromedia Flash-Filmen ganz ähnliche Probleme auf wie bei Websites, wenn es um den Schutz der Datensicherheit geht. Da es sich beim SWF-Dateiformat um ein offenes Format handelt, ist es möglich, Daten und Algorithmen zu extrahieren, die in einem Macromedia Flash-Film enthalten sind. Dies ist ähnlich wie bei HTML- und JavaScript-Code, der mühelos von den Benutzern angezeigt werden kann. Macromedia Flash-Filme machen das Anzeigen von Code allerdings etwas schwieriger. Eine SWF-Datei ist eine kompilierte Datei und liegt nicht in lesbarer Form wie HTML oder JavaScript vor.

Die Sicherheit wird allerdings nicht durch bloßes Verdecken von Daten erzielt. Es gibt eine ganze Reihe von Drittanbieter-Anwendungen, mit denen sich Daten aus kompilierten SWF-Dateien extrahieren lassen. Das am weitesten verbreitete dieser Tools heißt ActionScript Viewer (ASV) und ist auf dieser Website erhältlich: http://www.buraks.com/. Diese Tools unterstützen zwar noch nicht alle Versionen von SWF-Dateien, der entsprechende Support für neuere Versionen wird aber mit Sicherheit in Bälde vorhanden sein.

Grundsätzlich gilt also: In einen Macromedia Flash-Film oder -Projektor kompilierte Daten, Variablen oder ActionScript-Code sollten nicht als sicher betrachtet werden.

Erprobte Verfahren zum Absichern von Daten in einem Macromedia Flash-Film

Nur weil in einen Macromedia Flash-Film kompilierte Daten und Algorithmen extrahiert werden können, bedeutet dies noch lange nicht, dass sensitive Daten nicht geschützt werden können. Es gibt eine Reihe von Methoden, mit deren Hilfe sensitive Informationen abgesichert und trotzdem in Macromedia Flash-Filmen eingesetzt werden können. Am besten befolgen Sie diese Regeln:

1. Hartkodieren Sie keine sensitiven Informationen wie Benutzernamen, Kennwörter oder SQL-Anweisungen in Macromedia Flash-Filmen.
2. Wenn ein Macromedia Flash-Film Zugriff auf sensitive Informationen benötigt, laden Sie die Informationen zur Laufzeit vom Server in den Film. Die Daten sind nicht Teil der kompilierten SWF-Datei und können daher nicht extrahiert werden. Verwenden Sie zum Laden der Daten einen sicheren Übertragungsmechanismus wie SSL.
3. Implementieren Sie sensitive Algorithmen auf dem Server und nicht in ActionScript.
4. Stellen Sie Ihre Webanwendungen ausschließlich über einen vertrauten Server bereit. Andernfalls könnte der serverseitige Aspekt Ihrer Anwendung beeinträchtigt werden.

Sicherheitsüberlegungen im Hinblick auf Viren und Trojaner

Macromedia Flash-Filme, die in einem Webbrowser ausgeführt werden, sind sicher. Bislang gab es noch keine Berichte über Viren oder Trojaner, die unter Verwendung von Macromedia Flash-Filmen, die in einem Webbrowser abgespielt werden, eingeschleust wurden. Der Macromedia Flash Player weist strikte Sicherheitsregeln auf und bietet nur eingeschränkten Zugriff auf lokale Systemressourcen; daher sind derartige Angriffe extrem unwahrscheinlich.

Macromedia Flash-Wiedergabe in Projektoren

Wie bei allen ausführbaren Dateien besteht es auch bei Macromedia Flash-Projektoren, die aus zwielichtigen Quellen stammen, ein gewisses Risiko. Probleme dieser Art sind jedoch in erster Linie auf die Ausführung suspekter Programmdateien zurückzuführen, und nicht auf den Macromedia Flash-Projektor selbst. Generell sollten Benutzer Programmdateien (einschließlich Macromedia Flash-Projektoren) nur dann ausführen, wenn sie wissen, woher sie stammen.

Der vorliegende Abschnitt gilt nur für lokal ausgeführte Macromedia Flash-Projektoren und für Macromedia Flash-Filme, die im eigenständigen Macromedia Flash Player abgespielt werden (der in der Regel nur für Macromedia Flash-Entwickler verfügbar ist). Die Ausführungen treffen nicht auf Macromedia Flash-Filme zu, die in einem Webbrowser ausgeführt werden.

Beim lokalen Ausführen von Flash-Filmen sind drei Hauptaspekte zu bedenken:

- Macromedia Flash-Filme als Träger von Viren
- Heimtückische Dateien, die als Macromedia Flash-Dateien getarnt sind
- Macromedia Flash-Filme, die bösartigen Code enthalten

Macromedia Flash-Projektoren als Träger von Viren

Leider gibt es immer wieder Entwickler, die aus purer Niedertracht eine Macromedia Flash Player-Projektordatei mit Viren versehen. Wenn jedoch alle Macromedia Flash-Projektordateien mit einem aktuellen Antivirenprogramm überprüft werden und noch dazu nur Projektoren aufgerufen werden, die aus einer verlässlichen Quelle stammen, ist dieses Problem irrelevant.

Auch hier gilt: Dies ist kein Sicherheitsproblem von Macromedia Flash, sondern generell von ausführbaren Dateien.

Heimtückische Dateien, die als Macromedia Flash-Dateien getarnt sind

Ein Trojaner ist eine Datei, die vorgibt, etwas Bestimmtes zu sein, in Wirklichkeit jedoch etwas vollkommen Anderes ist. Dadurch soll ein Benutzer dazu überredet werden, eine unsichere Datei auszuführen.

Aufgrund der weiten Verbreitung von Macromedia Flash-Inhalten gibt es immer wieder heimtückische Gesellen, die ihre Programme als Macromedia Flash-Filme tarnen, im sicheren Bewusstsein, dass sie von zahlreichen Personen ausgeführt werden.

Dies wird auf zwei verschiedene Methoden erreicht:

- Die verteilte Datei erhält einen Namen, der die Benutzer glauben macht, es handele sich um einen Macromedia Flash-Film, wie etwa „cooler_flash_film.exe“.
- Das Symbol der ausführbaren Datei wird in das Symbol für den Macromedia Flash Player geändert.

Benutzer sollten nur Dateien ausführen, die aus vertrauten Quellen stammen, und selbst dann nur unter größter Vorsicht. Dies ist besonders im Umgang mit Trojanerdateien wichtig, da diese nicht immer von Antivirenprogrammen erkannt werden.

Auch hier gilt: Dies ist kein Sicherheitsproblem von Macromedia Flash, sondern generell von ausführbaren Dateien.

Macromedia Flash-Filme, die bösartigen Code enthalten

Zwar ist dieser Fall bisher noch nicht in der Praxis aufgetreten, es ist theoretisch jedoch denkbar, dass ein Macromedia Flash-Projektor oder ein Macromedia Flash-Film, der im eigenständigen Macromedia Flash Player unter Windows ausgeführt wird, heimtückische Aktionen ausführen. Dieses Risiko tritt nur dann auf, wenn bösartige Inhalte in einem eigenständigen Macromedia Flash Player ausgeführt werden. Bei Filmen, die in einem Browser abgespielt werden, besteht diese Gefahr nicht.

Weitere Informationen zu diesem Thema finden Sie in der Macromedia Security Zone unter (http://www.macromedia.com/security/).

Benutzer sollten nur dann einen Macromedia Flash-Projektor oder -Film lokal ausführen, wenn er aus einer sicheren Quelle stammt und mit einem aktualisierten Antivirenprogramm überprüft wurde.

Noch einmal: Dies ist bisher reine Theorie und noch nicht in der Praxis beobachtet worden.

Macromedia Flash-Filme als E-Mail-Anhänge

Es gibt zwei Methoden, Macromedia Flash-Filme per E-Mail zu übertragen. Die erste ist, den Film einfach als E-Mail-Anhang zu senden. Die zweite Methode besteht darin, den Film in eine HTML-basierte E-Mail einzubetten, damit er beim Öffnen der E-Mail ausgeführt wird.

In beiden Fällen werden Macromedia Flash-Filme so angezeigt, als ob sie vom lokalen Dateisystem aus geladen würden. Aus diesem Grund sind sie nicht so sicher wie Macromedia Flash-Filme, die von einem Webserver stammen und in einem Webbrowser abgespielt werden.

Benutzer sollten nur dann einen Macromedia Flash-Film vom lokalen Dateisystem oder E-Mail-Client ausführen, wenn die Datei aus einer vertrauten und sicheren Quelle stammt. Bei Macromedia Flash-Filmen, die in E-Mails eingebettet sind, sollten Benutzer die Dokumentation zum E-Mail-Client zu Rate ziehen, um herauszufinden, wie die automatische Wiedergabe von ActiveX-Steuerungen in E-Mails deaktiviert werden kann.

Ressourcen

Macromedia Security Zone

http://www.macromedia.com/v1/developer/SecurityZone/

Enthält Sicherheitsbulletins und technische Artikel zu Sicherheitsfragen.

Macromedia Flash Player

http://www.macromedia.com/software/flashplayer/

Enthält Informationen und Ressourcen zum Macromedia Flash Player.

Macromedia Flash MX

http://www.macromedia.com/software/flash/

Enthält Informationen und Ressourcen für die Macromedia Flash MX-Authoring-Umgebung.

Macromedia Flash Support Center

http://www.macromedia.com/support/flash/

Enthält technische Ressourcen und Informationen zur Macromedia Flash-Entwicklung, u. a. auch zum Thema Sicherheit.

Macromedia Designer & Developer Center

http://www.macromedia.com/desdev/

Enthält Artikel, Tutorials und andere Informationen zur Macromedia Flash-Entwicklung.

Macromedia Flash Player: E-Mail-Adresse für Sicherheitsfragen

flashplayer_security@macromedia.com.

Diese E-Mail-Adresse kann für Fragen oder Kommentare zu den Sicherheitsaspekten des Macromedia Flash Players verwendet werden.

Danksagung

Mein besonderer Dank gilt Robert Hall (http://www.impossibilities.com/) für seine Hilfe bei der Darlegung des md5-Hash-Algorithmus.