



Document Library

Die InterLake GmbH bietet Ihren Kunden in der Document Library Zugriff auf interessante Informationen. Wir stellen Ihnen Inhalte unserer Partner und aus frei zugänglichen Online Quellen zur Verfügung, die mit unserer Tätigkeit und der IT- und Medienbranche zu tun haben. Bitte beachten Sie, dass die Inhalte dem Copyright der jeweiligen Herausgeber unterliegen und diese Inhalte nicht ohne Referenz auf das jeweilige Copyright weitergegeben werden dürfen.

Weitere Informationen zu InterLake und weitere Dokumente finden Sie unter

www.interlake.net

Die InterLake Document Library steht den Nutzern der InterLake.Network zur Verfügung:



InterLake engagiert sich ehrenamtlich beim Münchener IT- und Medienverband FIWM, dem unser Geschäftsführer Sven Slazenger als Vorstandsmitglied angehört, sowie in der Macromedia ColdFusion User Group Central Europe, die unter unserer Leitung seit 1998 ein deutschsprachiges Forum für über 700 Macromedia Entwickler in Deutschland, Österreich und der Schweiz bietet.

Weitere Informationen zu diesen beiden Initiativen erhalten Sie bei Sven Slazenger (slazenger@interlake.net)

InterLake offers its customers and business partners access to an extensive document library. We are offering information from our partners and have also compiled freely available papers from the internet that we consider of value to you. Please be advised that the copyright belongs to the issuer of the information and that you may not distribute this content without referring to these copyrights.

Additional information about InterLake and more documents can be accessed free of charge at

www.interlake.net

The InterLake Document Library is available through the websites of the InterLake.Network:

InterLake is also an active member of the non-profit Munich IT- and Media Association FIWM. With InterLake CEO Sven Slazenger we provide one of the board members of the FIWM. We are also the founders (1998) of the Macromedia ColdFusion User Group Central Europe, the German language forum for Macromedia Developers from Austria, Germany and Switzerland and one of the largest Macromedia Communities worldwide.

For further information please contact Sven Slazenger (slazenger@interlake.net)



SEPTEMBER 2002

Secure Design with Flash Communication Server MX

Macromedia's Flash Communication Server MX platform enables the creation of compelling applications through the exchange of streaming media content. Because security features are essential in the widespread deployment of applications, Flash Communication Server MX provides functionality that protects both application and host platform. This brief identifies design and development practices that make effective use of the security features within Flash Communication Server MX.

@stake partnered with Macromedia to assess the design and operation of the Macromedia Flash Communication Server MX with respect to industry best practices in security.

- An **Application Architecture Assessment** included a review of the application's design, its interactions with the operating system and external components, and its handling of potentially confidential data.
- An **Application Penetration Assessment** provided a practical demonstration of the security aspects of Flash Communication Server MX by attempting to circumvent those features intended to protect the confidentiality and integrity of the application, its data, and its host platform.

Like all software, Flash Communication Server MX functions according to the requirements and expectations of its design scope. This document describes the boundaries within which Flash Communication Server MX meets requirements to protect its operation, data, and host platform. Developers should design and develop their applications within these boundaries to retain the intended security properties of this platform.

Flash Communication Server MX Architecture Overview

Flash Communication Server MX is comprised of two functional components that manage different aspects of the product's operation:

- A back-end administration server controls operation of Flash Communication Server MX.
- Flash Communication Server MX provides the environment in which server applications run, network connectivity for the applications, and interactions with the host operating system.

It is important to note that a Flash Communication Server MX application generally does not work in isolation—it requires interaction either with a Flash Player application (SWF), with other Flash Communication Server MX applications, or with other components capable of interacting with it.

Server applications run within the confines of the ActionScript Interpreter, which provides objects and methods to interact with entities outside the server, either on the host system or elsewhere on the network. Flash Communication Server MX implements the protocols that the server application uses to communicate across the network, and it places limitations on the nature of the server application's interactions. Finally, Flash Communication Server MX constrains an application's use of the file system by performing file I/O operations for the application.

Flash Communication Server MX Security Features

This section analyzes the key Flash Communication Server MX security features.

Domain Oriented Access Control

Domain Name Service, or DNS, is the infrastructure component of the Internet that acts as a directory, allowing the use of mnemonic names, such as “www.macromedia.com,” to identify computers. The Flash Communication Server MX remote shared object implementation relies on the accuracy of DNS to identify Flash Player applications that are authorized to access specific shared objects. Distributed server applications rely on DNS to locate peer servers.

DNS query results can be trusted within certain narrowly defined limits:

- The DNS server and any forwarders upon which it relies are trusted to provide accurate lookups and are authoritative for every domain being queried.
- DNS queries are not subject to eavesdropping or interception at any point on the network.

Generally, these constraints are difficult to meet except within carefully controlled corporate environments.

Flash Communication Server MX Application Security

The security of a Flash Communication Server MX application depends on effectively using the features available to it. The following sections describe key features that affect the secure operation of applications.

Remote Shared Objects

Developers can choose to store data in remote shared objects that Flash Communication Server MX implements. These objects facilitate synchronization among either multiple clients or various components within an application. By default, Flash Communication Server MX relies on DNS for access control to remote shared objects. Applications should either provide an alternate access control mechanism meeting their security requirements, or store only non-sensitive or public information in remote shared objects.

Media Streams

Interactive applications built with Flash Communication Server MX can receive and distribute audio and video media streams and accompanying data using Macromedia's Real Time Messaging Protocol (RTMP). This protocol, implemented by both Flash Communication Server MX and Flash Player 6, encapsulates media streams and data into a single data channel for transmission to the networking peer. The recipient reconstructs the original streams and handles them as appropriate. As RTMP is a cleartext protocol, applications should use it to convey only public or non-sensitive information when the network route between the client and server is not trusted.

Authentication and Authorization

Requirements for authentication and authorization vary widely by application—no solution satisfies all requirements. Flash Communication Server MX assumes that each server application will implement authentication and authorization operations appropriate to its needs.

Distributed Application Networking

With its Action Message Format (AMF) and RTMP protocols, Flash Communication Server MX permits the design and implementation of distributed server applications. For both AMF and RTMP, the server application typically identifies remote servers using their fully qualified host names, resolved through DNS. Distributed applications require accurate host name resolution: the host's system administrator should place trusted host names and their IP addresses in the local file used for name resolution, such as `lmhosts`, and ensure that the system will give precedence to these names and addresses over DNS resolution. Likewise, server applications that communicate across the network should maintain their own lists of trusted servers and services, rather than blindly connecting to arbitrary hosts that clients request. Finally, distributed application services should authenticate each other using an appropriate mechanism.

Server Administration Security

The Flash Communication Server MX administrator manages the server with an application that uses a Flash movie for its UI, and a Flash Communication Server MX application for its back end. The administration application implements username/password authentication, with the UI communicating these credentials and subsequent actions to the server using RTMP. To prevent disclosure of passwords

and configuration information via packet sniffing, server administrators should invoke the administration application using a trusted communications channel. These channels include Flash Communication Server MX host system itself, one or more trusted network segments, or a VPN between the administration console and a trusted network segment connected to Flash Communication Server MX. Because server administration occurs on a dedicated port, a network administrator can configure the networking components to block unauthorized traffic to that port.

Because Flash Communication Server MX relies on the host system's security features for maintaining authentication credentials, only individuals authorized to manage Flash Communication Server MX should have physical access or login credentials to the host system.

Server System Security

Flash Communication Server MX is designed to protect the host platform from direct access by server applications while still providing certain aspects of the platform for its use. Of primary interest is Flash Communication Server MX's ability to limit access to the file system, code execution, and network access.

File system

Flash Communication Server MX does not permit server applications to access the file system directly; instead, it requires indirect access through methods it provides. This encapsulation permits it to control the precise location of all the data a server application stores. Flash Communication Server MX stores data in files within a specific directory hierarchy, using naming conventions that preclude the server application's creation of arbitrary files within the host platform's file system. Flash Communication Server MX stores the names and contents of objects within the data files, permitting developers to use arbitrary names and data without interfering with the normal, secure operation of the host system or affecting other server applications.

Code Execution

A general concern is the interaction between a server application and the target operating system or machine, and the security consequences to the platform if the application behaves unexpectedly due to a programming error. Flash Communication Server MX provides an ECMA standard based, scripted execution environment with proprietary extensions. This environment, known as the ActionScript Interpreter, limits the interactions a server application can have with the host platform and other external entities by providing a set of objects and methods that constrain the interactions within safe boundaries.

ActionScript programs are not native to Flash Communication Server MX's server platform, so a program that runs within the interpreter cannot run in the host operating system. Furthermore, objects that an ActionScript program manipulates are neither executed by the interpreter or the host platform, nor stored or transmitted in a form that could eventually interact with the platform. These features work together to help prevent ActionScript programs from escaping to the host environment or otherwise interacting with the host in an uncontrolled manner.

Network

Flash Communication Server MX design prevents arbitrary access to the network by server applications. Instead, the server provides applications with a set of ActionScript objects to invoke outbound network data transfers. These objects support two protocols, AMF and RTMP, with neither providing access to arbitrary resources on the network.

Flash Communication Server MX accepts inbound RTMP connections, including those from Flash Player applications and other server applications. Flash Communication Server MX reconstructs data streams and objects, and passes these to the application without otherwise interpreting them. This aspect of Flash Communication Server MX design helps protect the platform from attempts to compromise it via RTMP.

Conclusion

Flash Communication Server MX provides a versatile platform for implementing streaming media Flash applications, providing security-conscious functionality with features that address security concerns in an externally facing placement. Developers with a basic understanding of the concepts represented in this document will be able to create server applications that retain the intended security properties of Flash Communication Server MX platform. The information presented here provides insights into the relationship and interactions among Flash Communication Server MX, its clients, peer servers, the target platform, and the network. As such, it will facilitate the introduction of Flash Communication Server MX into both externally facing placements, such as public web sites, and controlled environments, such as corporate intranets.

About @stake, Inc.

@stake provides corporations with digital security services that secure critical infrastructure and electronic relationships. @stake applies industry expertise and pioneering research to design and build secure business solutions. As the first company to develop an empirical model measuring the Return On Security Investment (ROSI), @stake works where security and business intersect. Headquartered in Cambridge, MA, @stake has offices in Denver, Hamburg, London, New York, Raleigh, San Francisco, and Seattle. For more information, go to www.atstake.com.

Reproduction guidelines: you may make copies of this document unless otherwise noted. If you quote or reference this document, you must appropriately attribute the contents and authorship to @stake. Opinions presented in this document reflect judgment at the time of publication and are subject to change. While every precaution has been taken in the preparation of this document, @stake assumes no responsibility for errors, omissions, or damages resulting from the use of the information herein. Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation and to the owner's benefit, without intent to infringe.