Adobe® Acrobat® Connect™ Pro

Security Assessment

Prepared by Security Innovation

October 4, 2007

Security Innovation, Inc
187 Ballardvale Street, Suite A170
Wilmington, MA 01887

1.978.694.1008

www.securityinnovation.com

Boston | **Amsterdam** | **Seattle**

Table of Contents

1.0 Overview

About the Engagement

Security Innovation was been engaged by Adobe to evaluate Adobe® Acrobat® Connect™ Pro for proper security design and implementation. Adobe Acrobat Connect Pro, also called Acrobat Connect Pro, is built with many specific features designed to enhance the security of the application and subsequently the customers who use it. The purpose of this report is to examine the presence and effectiveness of these security features.

This report addresses the licensed version of the Adobe Connect Pro product. The licensed product is purchased by customers to run locally on their network whereas the hosted product runs in a hosted environment and is managed by Adobe. A separate report is available which evaluates the Acrobat Connect Pro Hosted service.

About Security Innovation

Security Innovation is the leading independent provider of risk assessment, risk mitigation and education services to mid-size and Fortune 500 companies. Global technology vendors and enterprise IT organizations such as IBM, Microsoft, ING, Symantec, Visa, SAP and GE rely on our expertise to understand the security risks in their software systems and facilitate the software and process change necessary to mitigate them.

The company has developed unparalleled expertise in the most dominant and demanding computing platforms and development environments. This practical experience gained through deep assessment of the world's most robust software applications combined with research on pressing security issues continues to position the company at the apex of the application security market.

2.0 Adobe Acrobat Connect Pro Overview

Acrobat Connect Pro is a web conferencing software that enables individuals and small businesses to instantly communicate and collaborate through easy-to-use, easy-to-access online personal meeting rooms. The Acrobat Connect Pro application, in its basic configuration, consists of the following components: the Acrobat Connect Pro Server, Flash Media Server, and a database.

The Acrobat Connect Pro Server is built using a J2EE architecture using components of JRun from Adobe. Also called the application server, it manages users, groups, on-demand content, and client sessions. Some of the application server's duties include access control, security, quotas, licensing, auditing, and various management functions.

Flash Media Server, also called the FMS, is installed with the Acrobat Connect Pro Server to handle real-time audio and video streaming, data synchronization, and rich-media content deliver. The FMS streams audio, video, and accompanying meeting data using Adobe's Real-Time Messaging Protocol (RTMP). The FMS can host many types of meetings, seminars and trainings, all of which are referred to as meetings in this assessment.

The application server requires a database for persistent storage of application data including users, groups, content, and reporting information. Acrobat Connect Pro customers can use the embedded database engine (MSDE) included in the Acrobat Connect Pro application server installer or they can install separately the full version of Microsoft® SQL Server 2000 or 2005.

3.0 Assessment

Acrobat Connect Pro employs a variety of measures to secure Acrobat Connect Pro customer's communications and data. These security measures must address issues in the following categories:

- **User Authentication**. Users must be required to authenticate prior to accessing private content and meetings and the authentication method itself must occur securely.
- **Authentication Failures**. When a user fails to authenticate, the failure must occur in a secure manner. Additionally, measures should be taken to prevent rapid authentication attempts.
- **Password Management**. Users should be required to choose strong passwords and change them regularly.
- **Data Management**. Strong encryption must be used to secure communications and sensitive data stored in the database. Queries to the database must prevent malicious injection.
- **User Privileges**. Access to resources must be configurable and properly allow or restrict access to content and meetings.
- **Auditing and Logging**. For auditing purposes, potentially malicious use must be logged along with time and source information.

Security Innovation investigated each of these categories and concluded that Acrobat Connect Pro properly implements security measures to handle each issue. The assessment for each category is provided below.

User Authentication

When accessing the application server, users are first required to authenticate. Security Innovation verified that access to the application server cannot be circumvented. Security Innovation tested several different bypass methods and found that the application server properly required authentication in all cases.

Acrobat Connect Pro supports the following authentication methods: username/password, PKI, NTLM, and HTTP header authentication. NTLM and HTTP header authentication both allow for Acrobat Connect Pro to be used in a Single Sign-On authentication solution.

By default Acrobat Connect Pro authenticates a user by requiring that they enter a valid username/password combination. Security Innovation verified that when an unauthenticated user attempts to access restricted resources the user is properly denied access. Security Innovation tested several different bypass methods and found that the application server properly required authentication in all cases.

Acrobat Connect Pro supports PKI based authentication. PKI based authentication is a public key based mechanism that is based upon certificates. With PKI authentication, in addition to the server authenticating itself

to the clients using public key certificates (as with SSL), the clients also use public key certificates to authenticate themselves to the server.

Acrobat Connect Pro supports the use of NTLM and HTTP header authentication. NTLM authentication is a challenge/response authentication protocol used on networks that include Microsoft based operating systems. Under this setup, NTLM must be configured to pass authentication results to Acrobat Connect Pro. HTTP header authentication is a method where a client passes the authentication credentials to a proxy server which authenticates the user and passes the authentication results to Acrobat Connect Pro.

NTLM, HTTP header, and PKI based authentication are all authentication methods provided by an outside third-party. The statements provided here are based upon Security Innovation's review of Acrobat Connect Pro documentation and discussions with members of the Adobe security staff and Acrobat Connect Pro development team, not an in-depth security assessment and penetration test.

Authentication Failures

When a user attempts to authenticate to the application server, Acrobat Connect Pro records the attempt in an access log file. Through extensive testing, Security Innovation verified that Acrobat Connect Pro accurately records all access attempts and that the access log file does not include any passwords used for login attempts, whether successful or unsuccessful.

Acrobat Connect Pro implements a time delay after each login attempt in order to prevent brute force and dictionary attacks. Security Innovation verified that when an invalid login is attempted, the user must wait three seconds prior to their next login attempt.

Password Management

For user authentication, Acrobat Connect Pro can be configured to integrate with NTLM, a Single Sign-On solution, or use its own username/password based authentication. When using LDAP-based authentication (NTLM or Single Sign On), passwords are managed in the corporate directory and governed by the LDAP password policies. When using its own username/password authentication, Acrobat Connect Pro allows for the configuration of a minimum password length to make user passwords more difficult to discover through brute force attacks. Security Innovation verified that the application can be configured to require a minimum password length and that this minimum length is enforced when new accounts are created and whenever passwords are changed.

When using username/password authentication, Acrobat Connect Pro can be configured to enforce a password lifetime policy to ensure that passwords are changed on a regular basis. This policy is to help protect against brute force and dictionary attacks. Security Innovation verified that a maximum password lifetime can be set and that users are required to change their passwords after they have expired. When changing passwords, Acrobat Connect Pro does not require the new password to differ from the old one. As such, Security Innovation recommends customers take additional measures to ensure that passwords are changed regularly.

When using username/password authentication, Acrobat Connect Pro can be configured to require certain character classes be used when updating passwords, ensuring that passwords are more difficult to obtain through brute force and dictionary attacks. The character classes that can be required are: capital letters,

numbers, and any single character chosen by the administrator. Security Innovation verified that the application properly enforces the character class policy when updating passwords. Security Innovation notes that although the administrator chosen single character class does not affect the strength of passwords, the other character classes are both effective means to strengthen user passwords.

Data Management

SSL and TLS are both communication protocols that provide a secure channel through which information can be shared. Acrobat Connect Pro can be configured to support both SSL and TLS. Acrobat Connect Pro utilizes both HTTP and RTMP for communication between clients and the servers. Security Innovation verified that both of these types of communication can be secured through the use of SSL or TLS.

Prepared statements are predefined database queries that allow parameterized queries to be passed to a database. They can help protect against certain kinds of input injection attacks. Acrobat Connect Pro uses prepared statements almost exclusively when communicating with the database. Security Innovation verified that Acrobat Connect Pro makes extensive use of prepared statements by auditing the source code to Acrobat Connect Pro and by reviewing relevant log files.

User Privileges

Acrobat Connect Pro allows administrators to control access to content, folders, and meetings through the use of Access Control Lists. Security Innovation verified that Acrobat Connect Pro implements Access Control Lists for all content, folders, and meetings and that access to each can be configured by an administrator. Through testing, Security Innovation found that Acrobat Connect Pro sometimes implements additional constraints in order to access resources. In such circumstances, the additional constraints served only to deny, not grant, access.

Whenever a user attempts to access some resource it is important for the application server to authorize the user before granting access. This ensures users are only granted access to the appropriate resources. Security Innovation verified that in most situations, Acrobat Connect Pro correctly restricts access to only authorized users, although in a situation where users are sharing browsers, the access restrictions may be circumvented. As a best practice, Security Innovation recommends Acrobat Connect Pro customers close their browser after logging out of the application server or a meeting when using Acrobat Connect Pro from a pubic or shared computer.

Audit and Logging

Acrobat Connect Pro logs both successful and unsuccessful login attempts. Through inspection of the access log file, Security Innovation verified that Acrobat Connect Pro records all successful and unsuccessful login attempts.

Acrobat Connect Pro allows new accounts to be created manually through the application server, in batch through the upload of a CSV file, and through a web service API call. Security Innovation verified Acrobat Connect Pro logs the creation of new accounts for each of these different methods.

Acrobat Connect Pro records the IP address of remote clients which connect and the date and time of all logged events. Security Innovation verified that all entries to the access log file include the remote IP address as

well as the date and time of the associated action.

4.0 Summary

Security Innovation performed this Application Security Assessment to evaluate the proper security design and implementation of Acrobat Connect Pro. Security Innovation investigated numerous security measures taken by Acrobat Connect Pro across several security related categories. Through the course of this investigation, Security Innovation concluded that Acrobat Connect Pro was designed with security best practices in mind and was implemented using a sound security model with the objective of protecting the confidentiality, integrity and availability of Acrobat Connect Pro customer data.

To learn more about Adobe Acrobat Connect Pro, visit Adobe online at:
http://www.adobe.com/products/acrobatconnectpro/

Printed in the U.S.A. 07/07