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 engaged by Adobe to evaluate the Adobe® Acrobat Connect™ Pro service for proper security design, implementation and deployment. This report examines the presence and effectiveness of security features in the Acrobat Connect Pro as deployed in the Adobe hosted environment. The report also covers the hosted environment to examine the security controls of its infrastructure, i.e., network, servers, and services.

A separate report addresses the independently conducted Application Security Assessment of the Adobe Acrobat Connect Pro licensed product.

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 Hosted Overview

Acrobat Connect Pro is web conferencing software that enables instant communication and collaboration through easy-to-use, easy-to-access online personal meeting rooms.

Acrobat Connect Pro enables anyone with a Flash software-enabled web browser to join a web meeting without having to download cumbersome software. Because the Adobe Flash Player is installed on more than 97 percent of Internet-connected computers worldwide, the experience of joining an online meeting is hassle-free.

The Acrobat Connect Pro hosted service gives organizations the benefit of maintaining control over the administration of users, groups, and meeting resources while outsourcing the management of the systems and infrastructure.

3.0 Server Assessment

The Acrobat Connect Pro Server employs a variety of measures to secure its 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 date, time and source information.

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

User Authentication

When accessing the Acrobat Connect Pro Server, users are first required to authenticate. Security Innovation tested several different bypass methods and found that the application server properly required authentication in all cases.

While capable of supporting additional authentication mechanisms, the Acrobat Connect Pro hosted service only offers the username/password authentication method. Security Innovation found that when an unauthenticated user attempts to access restricted resources the user is denied access and prompted to first authenticate.

Authentication Failures

When a user attempts to authenticate, the Acrobat Connect Pro Server records the attempt in its log files. By reviewing the logs in the hosted environment, Security Innovation checked and confirmed that the Acrobat Connect Pro Server accurately records all access attempts, but does not record any passwords used for login attempts – successful or not.

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

Password Management

The Acrobat Connect Pro Server allows customers to control the password requirements of their users, allowing them to make it more difficult for attackers to discover passwords via brute force and dictionary attacks. Specifically, customers can configure:

- A minimum password length
- A password lifetime policy which can ensure that passwords are changed on a regular basis
- The requirement of certain character classes in passwords. The character classes that can be required are: capital letters, numbers, and any single character chosen by the administrator

Customers of the hosted service can configure these settings via the web-based administration interface to the service. Security Innovation tested the secure design and implementation of these features in the hosted service environment by using them and found them to be functioning as designed.

Data Management

SSL and TLS are protocols that provide a secure encrypted channel for information sharing. The Acrobat Connect Pro Server can be configured to support both SSL and TLS for the two communication protocols it uses, HTTP and RTMP. Security Innovation checked and confirmed that both of these types of communication can be secured via SSL or TLS.[1]

The Acrobat Connect Pro Server uses various credential storage mechanisms to authenticate users including passwords in a database, session cookies, and tickets. User credentials need to be properly encrypted when stored in a database. Security Innovation found that passwords are hashed when stored in the Acrobat Connect Pro Server's system database.

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

User Privileges

The Acrobat Connect Pro Server security features have been designed and implemented to enforce the assignment and management of user privileges. Those features are:

- Access to content, courses, and meetings is available only to authorized users that have been granted the appropriate permission
- The application of the access control mechanism on a file/folder basis
- Access control list entries specify what permissions are granted to principal entities consisting of individual users and groups thereof

[1] Security Innovation also tested that the server does not accept SSL version 2 requests, but instead requires the use of SSL version 3 or TLS, an industry best practice since there are known problems with version 2 of SSL.

[2] This is true for Breeze 5 and newer and all new accounts from this point forward have utilized the encrypted passwords. The older Breeze 3 and Breeze 4 passwords are stored in the database in plain-text. If an administrator requires those users to update their passwords, the new passwords will be stored in their hashed form.

Security Innovation found these user privilege statements in the Acrobat Connect Pro hosted environment to be accurate via use and testing of the service. Tests included allowing and denying resources to specific users and groups, applying different access controls to different files and folders, and assigning different permissions to various users and groups and testing the enforcement of those settings.

Audit and Logging

The Acrobat Connect Pro Server logs both successful and unsuccessful login attempts. Through inspection of the hosted log files, Security Innovation confirmed that the Acrobat Connect Pro Server records all successful and unsuccessful login attempts.

The Acrobat Connect Pro Server logs the creation of user accounts. Security Innovation confirmed that the Acrobat Connect Pro hosted log files contain entries for newly created user accounts.

The Acrobat Connect Pro Server records the IP address of remote clients which connect and the date and time of all logged events. Security Innovation confirmed that all entries written to the hosted log files include the remote IP address of the client and the date and time of the logged event.

4.0 Deployment Environment Assessment

The Acrobat Connect Prohosted environment (henceforth, the hosted environment) employs a variety of measures to secure the communications and data of its users. The verification of these security measures is divided into the following categories:

- **Privacy Policy**. The privacy of users and their shared resources in the hosted environment must be protected from attack and misuse.
- **Information Security Audits**. The security of the hosted environment must be periodically assessed and tested by both Adobe and third-party personnel.
- **Personnel Security**. Personnel who have physical or logical access to the hosted environment must be qualified, security aware, and deserving of the trust and control granted them.
- **Physical & Environmental Security.** The physical and environmental state of the hosting environment must be well secured and closely monitored for any potential threats to the security or functioning of the hosted service.
- **Operations Management**. The management of the hosted environment and its day to day operations must be conducted to ensure the security and privacy of customers and their assets, and to plan for future capacity and operational requirements.
- **Systems Development and Maintenance.** The initial development and deployment of systems, as well as their ongoing maintenance, must be accomplished using current security best practices.

Security Innovation has investigated each of these areas and found that the Acrobat Connect Pro hosted environment properly implements security measures to handle each issue in all of these categories. The assessment for each category is included below.

Privacy Policy

The Acrobat Connect Pro hosted service has documented policies and controls in place to protect their customer's sensitive information (meeting content and credentials). Security Innovation has found that the

protection of meeting content is covered by the "Content" and "Privacy" sections of the "Adobe Acrobat Connect Terms & Conditions," the "Adobe Acrobat Connect and Adobe Acrobat Connect Pro Terms of Use," and the "Adobe Online Services Agreement."[i]

In the hosted environment, credentials consist of a user ID (a.k.a., unique customer ID) and a password, which are "Registration Information" as discussed in the Acrobat Connect Pro "Privacy Policy," and their protection is described in the section "Protection of your personal information."

Security Innovation found that network level and system level controls are in place in the hosted environment to protect content and credentials via discussions with select architects, administrators, and managers, plus via a review of network diagrams, firewall rule sets, IDS/IPS log files and server operating system events. Security Innovation also confirmed that credentials can be protected via secured logins over encrypted channels (SSL and TLS), and that new passwords are stored in a hashed form in the database[3].

Adobe has a privacy policy in place that prohibits the use of sensitive customer information. The "Adobe Acrobat Connect Privacy Policy" and the "Adobe Online Privacy Policy" are available online for Acrobat Connect Pro hosted clients and prospects to review. Security Innovation reviewed these documents and found that they clearly define the information that can be collected, how it can be used, and the Acrobat Connect Pro hosted customer's options and rights as a service user.

Information Security Audits

Adobe and third-party security firms perform periodic application security assessments and penetration tests to ensure the security and privacy of customer sensitive information and assets. Security Innovation found that Adobe has conducted infrastructure security reviews, threat modeling, and penetration testing on versions 4 and 5 of the Acrobat Connect Pro (then known as Macromedia Breeze) hosted environment. Security Innovation also found that a third-party threat model of Breeze 4 was done, and third-party web application audits of versions 5 and 6 of the Connect hosted staging environment were conducted. Adobe has also already scheduled security assessments and penetration tests in the Acrobat Connect Pro 7 scheduling documents. Finally, the results of past penetration tests have been added to the Adobe internal bug tracking system and are prioritized, addressed, and managed via that system.

[3] Passwords created prior to the use of Breeze 5 are stored in the database in plain text format. Passwords created or updated since Breeze 5 was installed in the hosted environment are stored in the hashed form.

Adobe conducts regular scans of the Acrobat Connect Pro hosted environment for application, OS, and network level vulnerabilities. Security Innovation found that regular, periodic vulnerability scans are conducted on the Acrobat Connect Pro hosted environment. Reviewing consecutive monthly vulnerability scan reports confirmed that the hosted environment components were properly scanned. By reviewing the meeting notes from Adobe's regularly conducted "scanning and remediation forum" project meetings we found that the reported issues are tracked and addressed. Adobe is currently reviewing and improving the process of managing the results of vulnerability scans, focusing on the issue of dealing with false positive results from the scanner.

Personnel Security

Adobe performs background checks for all full-time employees, including those who will be administering systems or have access to customer information. Security Innovation discovered that Adobe uses a third-party firm to conduct background checks on all job candidates. Checks include previous employment verification, education verification and criminal checks.

All Adobe employees must sign a Proprietary Rights agreement stating they are obligated to keep customer information confidential. Security Innovation reviewed the Adobe Proprietary Rights agreement and learned that all employees must sign this form when they join the company. This agreement applies to all proprietary information that the employee may have access to including personal (identity) information which is defined and covered by the Adobe Online Privacy Policy. All content used in a Acrobat Connect Pro hosted service meeting is covered by the Adobe Connect Terms & Conditions document which states that Adobe personnel will not access any content except as needed to perform the Service or at the request of the Acrobat Connect Pro hosted service customer.

All employees and contractors are required to report any observed or suspected threats or vulnerabilities to the designated point of contact. Security Innovation reviewed the applicable Adobe Security Vulnerability Incident Response policies and procedures as well as the documentation trail of the discovery and resolution of a known vulnerability in a component of the Acrobat Connect Pro product. We were also debriefed on the daily updated threat and vulnerability awareness process by the process owners.

Upon an administrator or Adobe Acrobat Connect Pro support person leaving Adobe or moving to another project their access is terminated. Security Innovation has confirmed this process via discussion with the Web Services Team Manager, who is responsible managing logical access to the hosting environment. To date the user account of anyone leaving the team has been deleted within four hours on average.

The Information Services team staff members have an incident response process in place that includes daily meetings to assess security incidents and vulnerabilities. Security Innovation was informed of the daily meeting, process, and how items (incidents and vulnerabilities) are managed. We reviewed the applicable Adobe Security Vulnerability Incident Response policies and procedures as well as a copy of the meeting minutes from one of these daily meetings.

Physical & Environmental Information Security

Hosting facilities are physically protected from unauthorized access. Access is logged and logs are reviewed and securely maintained. Security Innovation discovered, via interviews and review of service capabilities, service agreements, and auditing documents, that the hosting facilities used by the Acrobat Connect Pro hosted service are protected by multiple layers of physical security. This configuration significantly reduces the physical threat to the service and its information from unauthorized physical access.

Equipment has physical protections in place to prevent data theft and environmental hazards in order to prevent loss, damage or compromise of assets and interruption to business activities. Security Innovation has learned, via

interviews and review of service capabilities, service agreements and auditing documents, that the hosting facilities of the Acrobat Connect Pro hosted service have physical protections in place, both a) to prevent data theft, and b) to ensure that environmental issues do not negatively impact the service in any way.

Operations Management

Future capacity requirements are projected and planned to help ensure system availability and reduce the risk of systems overload. Operational requirements for new systems are established, documented and tested prior to the system's acceptance and use. Security Innovation found that SNMP based monitoring and trending tools are used to track resource usage, history, and trending. We have reviewed the meeting notes from a number of the weekly meetings of the team that designs, deploys, and manages the hosted environment. These minutes show that this information is being used to project future capacity requirements and plan for changes to support those requirements.

Virus protection software is used to prevent and detect the introduction of viruses. Security Innovation reviewed the Adobe Malicious Code Protection Standards and has been told that a specific anti-virus product is in use. Furthermore, we received information indicating that this product is installed on servers when they are first deployed in the Acrobat Connect Pro hosted environment and that it provides 24x7 real-time anti-virus validation.

Routine backup procedures are established and adhered to for carrying out a well-defined backup strategy, such as taking backup copies of data, storing backups off-site, and rehearsing their restoration. Security Innovation reviewed the Adobe IS Backup and Restore Standard, which is sufficient for backing up the Acrobat Connect Pro hosted service data. We also reviewed a written description of the database backup procedure which also adheres to this backup strategy.

Adobe uses clustered servers for data redundancy. Security Innovation reviewed Adobe' network diagrams for the Acrobat Connect Pro hosted environment indicating that clustered servers are used, and properly deployed, for data redundancy.

The design of Acrobat Connect Pro hosted service's internal and external networks represents a commitment to secure networking. The design is documented, on paper or in an electronic chart, including notes. Security Innovation has checked the accuracy of this statement by a review of Adobe's network diagrams of the hosted environment and supporting documentation such as DNS records, firewall rule sets, etc.

The use and administration of systems are monitored. The monitoring system produces an audit trail that allows the Acrobat Connect Pro hosted team to respond quickly to high-risk events. Security Innovation has found that the monitoring system of the Acrobat Connect Pro hosted service creates an audit trail that identifies users by their session identifier, IP address, and domain, and correlates events by the user that performed them. This enables more effective response to potential misuse of the service.

The Acrobat Connect Pro hosted service team members are required to use 2 factor authentication for VPN and remote administration of Acrobat Connect Pro services. Security Innovation confirmed that the use of a one-time password token combined with the user's VPN password is required for remote access into the Adobe corporate LAN and that remote administration of Acrobat Connect Pro services are allowed only from the Adobe corporate LAN.

Adobe has agreements in place with external organizations regarding logical access to the Acrobat Connect Pro hosted network or systems. Security Innovation has checked the accuracy of this statement by reviewing Adobe's "Accessing Adobe Network and Account Services Agreement," and by testing that access to those networks and systems is denied without signing that agreement.

Systems Development and Maintenance

Acrobat Connect Pro hosted change control and segregation of duties – development, staging, and production – are implemented where appropriate to reduce the risk of negligent, inadvertent or deliberate misuse of information-processing facilities and systems. Security Innovation reviewed Adobe's Standard Operating Policy and Procedure documents related to segregation of duties and change management, as well as the documentation trail of a recent promotion of a release from Engineering through to Production showing the use of distinct development, staging, and production environments.

The Acrobat Connect Pro hosted service has and adheres to an established process for developing secure infrastructure, systems, and/or applications such as host (OS level) and network equipment (Routers and Switches) hardening. Security Innovation reviewed the Acrobat Connect Pro hosted application server configuration document, used to configure all new application servers prior to deployment in the production environment, and it showed that the Acrobat Connect Pro Application Servers adhere to the established process for developing secure systems. We also reviewed Adobe's Secure Software Engineering Product Release Checklist which also clearly adheres to the established process for developing secure applications.

The Acrobat Connect Pro hosted service uses internationally or nationally accepted cryptographic ciphers for credential storage and network transmission (SSL and RTMPS). Security Innovation reviewed the audit trail for changes to the Acrobat Connect Pro hosted production environment that indicates all of the servers have been configured to require 128 bit SSL ciphers. Furthermore, we attempted to connect to a number of these servers using a browser configured to only support weaker ciphers and our connection attempts were properly denied.

5.0 Summary

Security Innovation investigated Acrobat Connect Pro Server and the Acrobat Connect Pro hosted environment to evaluate the security design and implementation of the Acrobat Connect Pro hosted service. Security Innovation investigated numerous security measures taken by Adobe across several security related categories. Through the course of this investigation, Security Innovation concluded that the Acrobat Connect Pro hosted service was designed, implemented and deployed with security best practices in mind.

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

---

[i] See http://www.adobe.com/products/connect/term/, http://www.adobe.com/products/connect/terms/attendee/, and http://www.adobe.com/products/connect/terms/service_agreement/ respectively.

[ii] See http://www.adobe.com/misc/privacy.html.

[iii] See http://www.adobe.com/products/connect/privacy/ and http://www.adobe.com/misc/privacy.html respectively. Also see the Adobe Online Services Agreement, http://www.adobe.com/products/connect/terms/service_agreement/ referenced by the former.