Purpose of This Document

This document provides the Interplay Central (IPC) Administrator with an overview of the security architecture for the IPC environment and recommended best practices for a secure operation. The document also provides an analysis of the IPC application against the most common security flaws for Web-based applications.

Intended Audience

This document is intended for anyone responsible for system security, including Interplay Central System Administrators, Chief Security Officers, and IT administrators.

Product Version

Interplay Central version 1.3

Revision History

<table>
<thead>
<tr>
<th>Date Revised</th>
<th>Changes Made</th>
</tr>
</thead>
<tbody>
<tr>
<td>February 22, 2013</td>
<td>Edited reference to automatic timeout</td>
</tr>
</tbody>
</table>
Overview of Interplay Central

Interplay Central delivers workflow tools for media professionals through both Web and mobile applications. Interplay Central allows individuals in different media production roles to access the tools they need to complete tasks with greater access to assets, team collaboration, and workflow agility. Through Interplay Central, users can access existing Interplay Production assets and iNEWS story/rundown information.

Overview of Interplay Central Security

This section describes some common Web application concerns and how they are addressed by the Interplay Central (IPC) architecture.

- Internet Security and Availability

  The Interplay Central client accesses the IPC server functionality through a Web-based client. As with any Web-based application, information is passed over the Internet for the user to log in and operate the application. IPC utilizes standard HTTPS Internet transfer protocols for secure information transfers, such as user login credentials. IPC relies on consistent Internet access for successful operation. If the application is disconnected due to faulty Internet access, the user session closes and users are required to re-enter their credentials when access is restored.

- Data Privacy

  Interplay Central provides the client with access to existing Interplay Production assets and iNEWS story/rundown information. As part of the login to IPC, the user is also logged into associated Interplay Production and iNEWS sessions using their existing Interplay
Production and iNEWS credentials. Access to these assets is controlled by the underlying applications themselves, based on the user’s existing account privileges. The IPC client does not provide users access to any assets for which they do not have existing privileges.

In order to provide for a single login experience, IPC stores user login credentials (IPC, iNEWS, Interplay Production, and other customer user account information) in a central user management database. All data is stored in this central database and all passwords are maintained in an encrypted form. Note that IPC leverages the existing iNEWS and Interplay Production credentials (no modifications are made to existing accounts).

• Control of Data

IPC stores system configuration information, some of which includes login credentials to other applications (such as iNEWS, Interplay Production). IPC also stores user configuration information (roles) and login credentials. An IPC administrator does not have access to any user private information. Access to user and system settings is limited as described below.

There are three categories of settings:

- Home > User Settings (Basic, Video, Logging layouts), which are accessed only through a user login. An IPC administrator can access them only by logging in as the user.

- System Settings (System Settings layout), which are accessed only through an administrator login. These settings define the overall IPC environment.

- User Management settings (Users layout), which are accessed only through an administrator login. These settings include settings for individual users, groups, and roles.

Specific information about the settings is available in the Interplay Central documentation. See “Where to Find More Information” on page 15.

• Security Incident Tracking

IPC does not have the ability to track security incidents related to the application. The administrator does not have access to user session information (who is logged in and for how long) and does not currently have the ability to manually terminate a specific user session. The administrator can review information contained in /var/log/audit/audit.log and /var/log/secure, which contain a history of remote logins, authentication and authorization privileges.

Example:

Jan 7 14:39:59 localhost sshd[3781]: Accepted password for root from 172.24.41.133 port 43239 ssh2
• Disaster Recovery and Business Continuity
  - The IPC application can operate within a clustered server configuration, providing Active/Passive failover for continuity of services.
  - The Interplay Common Playback Service (ICPS), which supports the player functionality in the IPC UI, is also load balanced, providing performance and failover support for video streaming.
  - The underlying IPC database, which stores the user settings and system configuration data, can be configured for data replication and failover. The current database recovery point is 10 minutes of transaction history.
    Additional details are provided in the *Avid Interplay Central Installation and Configuration Guide*.
  - All ICS services (Boot, Broker, Attributes) are highly available using Active/Passive failover. All services are managed as a single resource and will fail over as a group. ICS services are not currently load balanced.

• Regulatory Compliance
  Due to the nature of the application and the information that is accessed and stored, the IPC application is not currently validated against any existing security compliance standards (such as HIPAA, DSS, ISO 19779/27001).

**Interplay Central Security Architecture**

The diagram below provides an overview of the IPC architecture with specific references to application and data security. This diagram shows a clustered IPC server configuration.
An IPC client requires user login credentials in order to gain access to the underlying functionality. All data transfer to and from the IPC client (user credentials, session information, user configuration settings, media images and files, text, and machine instructions) are transported in a secure manner to the IPC server using HTTPS protocol.

IPC clients that connect through the public Internet require VPN access into the server network. All connections pass through the VPN router/firewall through identified ports. Once the data has passed into the “house network” it is secured using the customer’s existing network security infrastructure.
Users connected within the corporate LAN/WAN would not typically use VPN access but would likely need to pass through firewalls and other network security devices with ACLs before accessing the Avid Interplay network.

The following table lists the ports used by Interplay Central that should be allowed through the VPN firewall.

<table>
<thead>
<tr>
<th>Component</th>
<th>Port</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interplay Central Web application</td>
<td>80</td>
<td>Interplay Common Playback Service (ICPS) HTTP calls</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>IPC HTTPS calls</td>
</tr>
<tr>
<td></td>
<td>843</td>
<td>Loading the Flash Player for playback</td>
</tr>
<tr>
<td></td>
<td>26000</td>
<td>Inbound ICPS data</td>
</tr>
<tr>
<td></td>
<td>5000</td>
<td>Serving outbound JPEG images to the Flash player</td>
</tr>
<tr>
<td>Interplay Central mobile applications</td>
<td>80</td>
<td>ICPS HTTP calls</td>
</tr>
<tr>
<td></td>
<td>443</td>
<td>IPC HTTPS calls</td>
</tr>
</tbody>
</table>

*Outbound ACLs should be used to allow packets from the ICS server to the IPC client over “established” TCP sessions only.*

Note that the IPC web service and IPC application services operate on the same server so there are no proxies or firewalls between these components. Access to the IPC database is also direct, with no database firewall protection required.

All system data stored within the user management database (user credentials, user settings, system attributes) can only be accessed and modified by an IPC Administrator.

The following items describe the IPC security architecture in more detail.

- **User Authentication**
  
  Access to the IPC client application requires the use of user or administrator identity credentials. All user credentials are passed from the web browser to the IPC server using SSL / HTTPS protocol. User authentication is through single factor authentication (username/password) and is provided by the IPC User Management Service, which resides on the IPC server. IPC can authorize users through Active Directory as well as through local IPC user management.
User sessions are managed with an Avid Session ID, which is stored within a client cookie. These client-side cookies are used to identify a specific user session within the Interplay Central Middleware Service, which stores necessary user connection information. The client cookie carries an identifier of the server-side session and does not contain any user credentials. It is possible for a malicious party to use the session identifier to execute requests on behalf of an already signed in user, but this is unlikely as the session communication is encrypted over HTTPS.

IPC also uses a form of federated identity management in order to log the user into the underlying Interplay Production and iNEWS applications. User authentication is managed by each of these applications locally. At initial login, user login credentials are passed over the house network from the IPC server to the Interplay Production and iNEWS server.

- **User Authorization**

  User rights and privileges are managed through role-based access lists stored within the IPC User Management Service. Roles can be assigned to users directly, or a user can inherit a role from a user group assignment. Roles control user access to features and specific IPC UI layouts. (Additional information can be found in the *Avid Interplay Central Administration Guide*.)

  IPC queries the User Management Service to determine which IPC layouts are to be made available to the user upon login. IPC provides two access levels (Basic and Advance, labeled Browse Media and Edit Media in the Users layout), which determine access to underlying application functionality. Access to all assets (media, metadata, rundowns, stories) is managed by the backend systems themselves (Interplay Production, iNEWS). The IPC User Management Service authorizes all client requests against the privileges for the current session.

  All requests to an IPC service require a session ID that is authenticated by the IPC User Management Service.

- **User Accountability (Non-Repudiation)**

  IPC logs both user session creation and termination. IPC user activity is not logged as part of the IPC session management function. Session logs are stored locally on the IPC server and are not replicated. Log access is file-system based; any individual who has access to the IPC server can access the User Management logs.

- **Securing Data at Rest**

  The IPC database stores user credentials, user settings, and system attributes information. User credentials (user name/passwords) are stored in a local database with user password information encrypted using SHA512 algorithm with a single hash (user names are not encrypted). User settings and system attributes are not encrypted. System attributes only contain server path information, with the exception of the ICPS service, which also includes a root login password.
When using Active Directory (AD) synchronization, the IPC User Management Service does not store the main passwords of the users (nor can the AD password be overwritten).

Interplay Production and iNEWS passwords are also stored in the IPC user management database using the following encryption techniques:

iNEWS – AES encrypted with a fixed 32-character password
Interplay Production – NXNCrypt encrypted

- Security Data in Transit

IPC uses default HTTPS transfer from the Web client to the IPC server and all underlying IPC services (for example, User Management). HTTPS calls are sent over port 443; see Table 1 on page 6 for a complete list of ports. Note that a network firewall is recommended.

Communication between IPC and Interplay Production and iNEWS is sent over the house network in an unsecured fashion. Any user password information that is transported for login to Interplay Production and iNEWS is sent in an encrypted state.

All communication across IPC services (bus-based messaging) occurs within the IPC server and does not traverse the house network. This information is not encrypted and can only be accessed by logging into the IPC server. Applications and services do not need a service authorization token to register on the bus, but since all services are contained on the IPC server it is difficult for external services to obtain access to the IPC bus.

For video playback with the ICPS client, the client will forward video MOBID and associated relink policy to the IPC server, which responds with the timeline object, JPEG image, and audio to the ICPS player within the web client. The ICPS request data is not encrypted and the response data (JPEG images and PCM audio) is also not encrypted but is transferred securely over HTTPS.

The following table summarizes the types of data transfer security.

<table>
<thead>
<tr>
<th>Communication</th>
<th>Data Transfer Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interplay Central Client &lt;-&gt; Interplay Common</td>
<td>HTTPS transfer</td>
</tr>
<tr>
<td>Services Server</td>
<td></td>
</tr>
<tr>
<td>Interplay Central Client &lt;-&gt; Interplay Common</td>
<td>HTTPS transfer</td>
</tr>
<tr>
<td>Playback Service</td>
<td>No data encryption</td>
</tr>
<tr>
<td>Interplay Central Server &lt;-&gt; Interplay Production</td>
<td>HTTP transfer</td>
</tr>
<tr>
<td>Only Interplay Production password is encrypted</td>
<td>(TEA 128 bit)</td>
</tr>
</tbody>
</table>
• **Data Integrity**

  Any IPC user with iNEWS access has the ability to modify and delete stories in an iNEWS rundown. They do not have the ability to delete an entire rundown.

  Note that asset or story updates or deletions are not logged.

  In order to prevent improper modification or destruction, all changes to video assets from the IPC client create new versions of the video (no master essence is changed). In addition, there is no delete operation available in IPC for Interplay Production media assets.

  For user management, an IPC administrator has the ability to delete users and groups, but only for the IPC user management. An IPC administrator does not have access to Interplay Production or iNEWS user management features.

• **Data Availability**

  All IPC data is contained within a single database, which is replicated using batch replication (providing a 10-minute recovery point). This data includes user management information, system settings, and user settings. Database backup and recovery procedures are recommended and are documented in the *Avid Interplay Common Services Installation and Configuration Guide*. No other data or state information is required for long-term storage in order to operate IPC.

• **Network Security**

  IPC relies on VPN and associated firewalls for access to the house network (see diagram). The IPC network configuration does not utilize proxy servers or server firewalls. Additional network protection can be implemented within the house network.

  The server firewall IP-tables can be configured using IP whitelisting to allow only expected traffic. However, note that the ICPS player uses dynamic port assignment for media playback. See Table 4 on page 11.

  IPC can use either self-signed, no certificate, or commercially used certificates for HTTPS communication. Each certificate type provides a different user experience and has its own set of security implications, as listed in the following table.
### Table 3: Security Implications for Certificate Types

<table>
<thead>
<tr>
<th></th>
<th>No Certificate</th>
<th>Self-Signed</th>
<th>Commercially Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User experience</strong></td>
<td>User is prompted with “This site is untrusted” with options to back out or “Proceed Anyway.”</td>
<td>User is prompted with “This site is untrusted” with options to back out or “Proceed Anyway.” Login is transparent.</td>
<td>Login is transparent.</td>
</tr>
<tr>
<td><strong>Security Implications</strong></td>
<td>IPC operates behind the firewall and is a “trusted application” so security implications are minimal. Even with no certificate, HTTPS connections are still properly encrypted.</td>
<td>Deployment involves both server-side and client-side certificate management by a system administrator.</td>
<td>A system administrator must ensure that the certificate is installed on IPC server.</td>
</tr>
</tbody>
</table>

- **Service Security**
  All IPC service calls are made using signed API calls which rely on an authenticated session token.

- **Antivirus**
  Server side: Antivirus is not required due to the nature of the Linux operating system and the data that is passed from the IPC client to the IPC server. Avid recommends that no other application be loaded on the IPC server to ensure optimal performance.

- **Data Separation/Isolation**
  Data access control is managed by the Interplay Production and iNEWS systems and does not depend on any IPC user controls.

- **OS Patching**
  Avid does not support OS patching between official releases. It is up to the user to determine whether to implement a critical OS security patch prior to Avid qualification of the critical patch.
Strategies and Best Practices

Administrator Accounts

As part of the ICS installation process, default administrator accounts are created. After a successful installation, these account passwords must be updated.

- A default operating system user account is created on the IPC server using the following credentials:
  user: root
  password: Avid123
- A default administrator account is created on the IPC middleware using the following credentials:
  user: Administrator
  password: Avid123

Note that each cluster node will have a similar account.

- A default Interplay Central Administrator is created in the IPC User Management Service using the following credentials:
  user: Administrator
  password: Avid123

The IPC Administrator should verify that all updated passwords align with corporate security policy. Note that generic passwords might have been set by an Avid representative during the installation process.

The ICS server uses ports for communication with other Interplay Central components. The following table lists the ports used by Interplay Central that should be allowed through the ICS firewall.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interplay Central</td>
<td>80, 443</td>
</tr>
<tr>
<td>ICPS</td>
<td>843 (Flash), 80, 26000</td>
</tr>
<tr>
<td>Apache httpd</td>
<td>80</td>
</tr>
<tr>
<td>ICS</td>
<td>8000 (optional Admin UI)</td>
</tr>
<tr>
<td>ISIS</td>
<td>5000 - 5399 (UPD and TCP)</td>
</tr>
</tbody>
</table>
In /etc/sysconfig, add a required file named iptables-AvidAll that includes these entries. The following is an example for port 843.

```
-I INPUT -p tcp --dport 843 -j ACCEPT
```

Add a reference to this file in system-config-firewall:

```
# Configuration file for system-config-firewall
--enabled
--custom-rules=ipv4:filter:/usr/share/netcf/iptables-forward-bridged
--custom-rules=ipv4:filter:/etc/sysconfig/iptables-forward-bridged
--custom-rules=ipv4:filter:/etc/sysconfig/iptables-AvidISISClient
--custom-rules=ipv4:filter:/etc/sysconfig/iptables-AvidBenchmarkAgent-udp
--custom-rules=ipv4:filter:/etc/sysconfig/iptables-AvidBenchmarkAgent-tcp
--custom-rules=ipv4:filter:/etc/sysconfig/iptables-AvidAll
```

The following table lists additional ports that might be required. Check with your Avid representative.

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>ActiveMQ</td>
<td>61616 (openwire), 61613 (stomp+nio), 8161 (admin ui)</td>
</tr>
<tr>
<td>Postgresql</td>
<td>53087</td>
</tr>
<tr>
<td>System</td>
<td>22, ICMP, 111, 24007, 24008, 24009-(24009 + number of bricks across all volumes for gluster). If you will be using NFS, open additional ports 38465-(38465 + number of Gluster servers). Some MAM configuration might require additional NFS ports (111, 2049 tcp&amp;udp) or CIFS (137,138 udp and 137,139 tcp). Other filesystems will have to be checked individually (Isilon, Harmonic Omneon, etc.)</td>
</tr>
</tbody>
</table>
## Security Risk Assessment

The following table describes how IPC addresses security risks as described in the Open Web Application Security Project (OWASP). Each threat is a link to the corresponding section of the project Web site, available at [https://www.owasp.org/index.php/Top_10_2010-Main](https://www.owasp.org/index.php/Top_10_2010-Main).

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risk</th>
<th>Typical Security Measures</th>
<th>IPC Environment</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Injection Flaws</td>
<td>Executing of unintended commands</td>
<td>Avoid use of interpreters</td>
<td>The only user input commands within IPC are within the search function. IPC utilizes an abstracted search API that cannot accept direct SQL requests. There is no direct service access from UI components and no strings are passed directly into SQL queries.</td>
<td>Low</td>
</tr>
<tr>
<td>Cross Site Scripting</td>
<td>Hijacking of browser sessions</td>
<td>User input validation</td>
<td>This capability is not active in the IPC Web UI.</td>
<td>Low</td>
</tr>
<tr>
<td>Broken Authentication and Session Management</td>
<td>Compromised passwords and user identities</td>
<td>Protection of session IDs</td>
<td>IPC user sessions do not persist and are lost upon network drops, causing the user to re-log on. All user sessions close on exit.</td>
<td>Medium.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted user credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Session ID security</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log out/timeouts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insecure Direct Object References</td>
<td>Unauthorized data access</td>
<td>Access controls</td>
<td>IPC leverages existing access controls for Interplay Production and iNEWS. Note that requests for video playback into IPCS will expose the asset MOB IDs.</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indirect object references</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cross Site Request Forgery</td>
<td>Legitimizes forged browser requests</td>
<td>Unique session or request tokens</td>
<td>IPC uses unique user session tokens. All tokens are deleted upon session exit. Session IDs are mapped to specific machines.</td>
<td>Low</td>
</tr>
</tbody>
</table>
Table 6: Security Risk Assessment

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risk</th>
<th>Typical Security Measures</th>
<th>IPC Environment</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Security Misconfiguration | Inadequately defined security configurations | Port management  
Account management  
Auto Admin settings deletion  
OS patching  
Error handling  
Cookie management | Port settings documented for management  
Application errors display limited information regarding system functions.  
Session ID stored as a cookie.  
Note: OS patching and code library updates are not supported between releases. | Requires Auto Admin account password modification.  
OS patching limitations may affect security status |
| Insecure Storage   | Vulnerable sensitive data          | Strong standard encryption  
Encrypted backups  
Password hashing/salting  | Uses encryption for stored data. Key management is described in the *Avid Interplay Common Services Configuration and Installation Guide*  
Backups do not include encryption key information.  
Database master password is required to restore backup. | Low |
| Non-Restricted URL Access | Access to hidden URLs             | Page Authentication / Authorization  
Default of no access  | IPC UI components and associated URL access are controlled through user privileges.  
IPC bus monitoring URL is available but requires administrator credentials to launch (off by default). | Low |
Table 6: Security Risk Assessment

<table>
<thead>
<tr>
<th>Threat</th>
<th>Risk</th>
<th>Typical Security Measures</th>
<th>IPC Environment</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient Transport Layer Protection</td>
<td>Unprotected network traffic</td>
<td>SSL authentications, VPN, Backend SSL transport, Secure database connection</td>
<td>IPC configuration utilizes SSL transport protocol and VPN network access. All access requests to the IPC database requires a suitable username and password. Access from within the IPC server is considered trusted and does not require a password. Username/password for the IPC database is the same on every installation and is automatically sent to all IPC bus connected services for the cloud database. The cloud database contains bus service registration data and system attributes data. This username/password does not have privileges for other IPC databases containing user information or ICPS information.</td>
<td>Non-secure transport of IPC to iNEWS and Interplay Production across house network.</td>
</tr>
<tr>
<td>Unvalidated Redirects and Forwards</td>
<td>Modified forwarding data</td>
<td>Avoid redirects/forwards</td>
<td>Redirects are difficult as IPC and all underlying services operate on same physical machine.</td>
<td>Low</td>
</tr>
</tbody>
</table>

Where to Find More Information

Interplay Common Services v1.3 documentation can be found on the Avid Customer Support Knowledge Base. Version 1.3 documentation is located here:


Interplay Central documentation can also be found on the Knowledge Base. Version 1.3 documentation is located here:

Legal Notices

Copyright © 2013 Avid Technology, Inc. and its licensors. All rights reserved.

Attn. Government User(s). Restricted Rights Legend
U.S. GOVERNMENT RESTRICTED RIGHTS. This Software and its documentation are "commercial computer software" or "commercial computer software documentation." In the event that such Software or documentation is acquired by or on behalf of a unit or agency of the U.S. Government, all rights with respect to this Software and documentation are subject to the terms of the License Agreement, pursuant to FAR §12.212(a) and/or DFARS §227.7202-1(a), as applicable.

All trademarks contained herein are the property of their respective owners.

Avid Interplay Central Security Architecture • February 2013 • Created 2/22/13 • This document is distributed by Avid in online (electronic) form only, and is not available for purchase in printed form.