Threat Mitigation and Prevention in ArcGIS Enterprise

Jeff Smith
Randall Williams
Agenda

• Focus: Security best practices for ArcGIS Enterprise

• ArcGIS Server
• Portal for ArcGIS
• Advanced Options

Strongly Recommend:
Knowledge of ArcGIS Server and Portal for ArcGIS
Security is Important

https://www.databreachtoday.com/news

Anti-Malware

Hackers Win Olympic Gold Medal for Disruption

Matthew J. Schwartz • February 12, 2018

Data Breach

$100,000 Fine in Case Involving Defunct Records Storage Firm

Breach Response

SEC Releases Updated Cybersecurity Guidance

Breach Notification

US Data Breaches Hit All-Time High

Matthew J. Schwartz • February 1, 2018

The number of data breaches reported by U.S. organizations reached an all-time high last year. In 2017, organizations that described how bad their breach was - and one-third did not - collectively lost 14 million payment cards and 158 million Social Security numbers, according to the Identity Theft Resource Center.
Defense In Depth Paradigm

- Security plans have many “layers” – multiple levels of security
- Layered security mechanisms increase the security of the system as a whole
- Each feature discussed is considered a “layer”
Review: ArcGIS Enterprise On-Premises
Enabling GIS Everywhere

Simple
Integrated
Open
ArcGIS Enterprise On-Premises: Behind the scenes

- Includes 3 components: Portal for ArcGIS – ArcGIS Server – ArcGIS Data Store
Agenda

- **ArcGIS Server**
  - Enable and use HTTPS
  - Disable services directory
  - Restrict cross domain requests
  - Restrict System folder permissions
  - Disable PSA account
  - Scan Server script

- **Portal for ArcGIS**

- **Advanced options**
Review: ArcGIS Server Administrator Directory

https://localhost:6443/arcgis/admin

- Web App, provides interface into an ArcGIS Server site
- Many security settings enabled via this interface

ArcGIS Server Administrator Directory

Home

You should use ArcGIS Server Manager for managing services and GIS servers. The Administrator Directory is intended for advanced, programmatic access to the server, likely through the use of scripts.

Site Root - /

Current Version: 10.6.0

Resources: machines clusters services security system data uploads logs kml info mode usagereports publicKey

Supported Operations: generateToken exportSite importSite deleteSite

Supported Interfaces: REST
Enable and Use HTTPS

- HTTPS – *Hypertext Transfer Protocol Secure*
- Initial step in creating a secure environment should always be to **encrypt traffic**
- Protects against a simple network sniffer
- Enabled by default in 10.4+
- Recommended to restrict to HTTPS only if possible
- **ArcGIS Server Admin Directory**
  - Security > config > update

[Image of SSL configuration]

**Update Security Configuration**

- **Warning**
  Changing Protocol will cause the web server to be restarted.

**Security Configuration**

- **Protocol:**
  - HTTP and HTTPS
- **SSL Protocols:**
  - HTTP Only
  - HTTP and HTTPS
  - HTTPS Only
- **SSL Cipher Suites:**
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
  - TLS_RSA_WITH_AES_256_GCM_SHA384,
Disable the Services Directory

- ArcGIS REST Services Directory exposes web services api in HTML format
  - `https://server.mydomain.com/arcgis/rest`
- Recommended NOT to expose REST services directory on Production Servers

**Before**

<table>
<thead>
<tr>
<th>ArcGIS REST Services Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home &gt; services</strong></td>
</tr>
<tr>
<td>**JSON</td>
</tr>
<tr>
<td><strong>Folder:</strong> /</td>
</tr>
<tr>
<td><strong>Current Version:</strong> 10.6</td>
</tr>
<tr>
<td><strong>View Footprints in:</strong> ArcGIS Online Map Viewer</td>
</tr>
<tr>
<td><strong>Folders:</strong></td>
</tr>
<tr>
<td>• Utilities</td>
</tr>
<tr>
<td><strong>Services:</strong></td>
</tr>
<tr>
<td>• <strong>Colorado</strong> (FeatureServer)</td>
</tr>
<tr>
<td>• <strong>Colorado</strong> (MapServer)</td>
</tr>
<tr>
<td>• <strong>SampleWorldCities</strong> (MapServer)</td>
</tr>
<tr>
<td><strong>Child Resources:</strong> Info Sell</td>
</tr>
<tr>
<td><strong>Supported Interfaces:</strong> REST SOAP Sitemap Geo Sitemap</td>
</tr>
</tbody>
</table>

**After**

<table>
<thead>
<tr>
<th>ArcGIS REST Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Home</strong></td>
</tr>
<tr>
<td><strong>Error:</strong> Services Directory has been disabled.</td>
</tr>
<tr>
<td><strong>Code:</strong> 403</td>
</tr>
</tbody>
</table>
How to Disable the Services Directory

- **Server Administrator Directory**
  - System > Handlers > Rest > Servicesdirectory > edit
  - Uncheck *Services Directory Enabled* option

**Help topic:** Disable the Services Directory
Restrict Cross-Domain (CORS) Requests

enterprise.arcgis.com > Search “cross-domain requests”

- **For JavaScript** applications, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing)
- Required when making POST requests to Feature or GP services on a different server
How to Restrict Cross-Domain Requests

- By default, ArcGIS Server allows all cross-domain requests
- These can be restricted in the Server Administrator Directory
  - system > handlers > rest > servicesdirectory > edit
  - AllowedOrigins - specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services
- Does NOT restrict overall access to the web services

ArcGIS Server Administrator Directory

Home > system > handlers > rest > servicesdirectory

Services Directory

- Services Directory: Enabled
- Javascript API URL: https://js.arcgis.com/4.5/
- Javascript API CSS URL: https://js.arcgis.com/4.5/esri/css/main.css
Demo

Restrict Cross-Domain Requests
Restrict System Folder Permissions in Manager

- Verify System folder permissions are limited to Administrators and Publishers only
  - Prevents potential Denial of Service due to resource consumption, service deletion, etc.
  - Usually changed from default when troubleshooting
Disable Primary Site Administrator (PSA) Account

- Recommend disable the PSA account to remove an alternate method of administering ArcGIS Server outside of your enterprise users
- Access the Server Administrator Directory
  - Security > PSA > disable
Scan GIS Server for Security Checks

- serverScan.py is a script in the Server installation directory
  - Located: `<install directory>\ArcGIS\Server\tools\admin`
- Script checks for security settings → generates a report that makes recommendations to improve security

### ArcGIS Server Security Scan Report - 02/27/18

(10.6.0)

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS02</td>
<td>Critical</td>
<td>Standardized queries</td>
<td>Enforcing standardized queries is disabled. To provide protection against SQL injection attacks, it is critical that this option be enabled. <a href="#">More information</a></td>
</tr>
</tbody>
</table>
| SS09 | Important | Dynamic workspace | Map service: SampleWorld\Cities
One or more dynamic workspaces are registered with this map service. To prevent a malicious party from obtaining the workspace ID and potentially gaining access, these dynamic workspaces should be removed. [More information](#) |
| SS07 | Important | Rest services directory | The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. [More information](#) |
| SS12 | Recommended | Feature service operations | Feature service: Colorado
This feature service has the update and/or delete operations enabled and is open to anonymous access. This allows the feature service data to be changed and/or deleted without authentication. [More information](#) |
| SS11 | Recommended | PSA account status | The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your identity store. [More information](#) |
Demo

Run *serverScan.py*

Security Check
Agenda

- ArcGIS Server
- **Portal for ArcGIS**
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory (aka Sharing API)
  - Restrict proxies
  - Disable the ‘Create An Account’ button on the sign-in page
  - Restrict cross-domain (CORS) requests
  - Trusted servers list
  - Scan Portal script
- Advanced options
Enable HTTPS Communication

- Enforce HTTPS so that all communication in your portal is sent using HTTPS
- Configure your portal and the web server hosting ArcGIS Web Adaptor to only allow communication through HTTPS
Disable ArcGIS Portal Directory (Production Servers)
https://<machinename>.domain.com/arcgis/sharing

- Provides a browsable HTML-based representation of all of Portal items
  - services, web maps, and content
- Recommend disable this to reduce the chance that your items can be browsed, found in a web search, or queried through HTML forms

Before

<table>
<thead>
<tr>
<th>ArcGIS Portal Directory</th>
<th>Home</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td></td>
</tr>
<tr>
<td></td>
<td>API Reference</td>
</tr>
<tr>
<td>Current Version: 4.4</td>
<td></td>
</tr>
<tr>
<td>Child Resources:</td>
<td>Search</td>
</tr>
<tr>
<td>Supported Operations:</td>
<td>Generate Token</td>
</tr>
</tbody>
</table>

After

<table>
<thead>
<tr>
<th>ArcGIS Portal Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Reference</td>
</tr>
</tbody>
</table>

How to Disable ArcGIS Portal Directory

- Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - Set property = ‘true’
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
  - Storing credentials (Single Sign On)
  - OGC Services
  - Non-CORS Systems
Restrict Machines Accessible by Portal

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on different machines
- By default the portal's proxy is open
  - Your Portal can be used to launch attacks against internal and external targets
How to Restrict Proxies

- Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - For Configuration field, add the `allowedProxyHosts` property and specify the list of approved addresses

```json
Portal Administrator Directory
Home > Security > Config

Security Configuration

Properties:
{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"defaultRoleForUser":"account_user","allowAdmin":false,"allowedProxyHosts": ".*.arcgis.com"}
User store configuration:
{"type": "BUILTIN","properties": {"IsPasswordEncrypted": "true"} }
Group store configuration:
{"type": "BUILTIN","properties": {"IsPasswordEncrypted": "true"} }

Supported Operations: Update Security Configuration  Update Identity Store  Test Identity Store
Supported Interfaces: REST
```
Disable ‘Create An Account’ on Sign In Page

- Disable the ability to create a new built-in Portal account
- **My Organization > Edit settings > Security**
Restrict Cross-Domain (CORS) Requests

- Limits external JavaScript applications making CORS requests to Portal items
- Does NOT restrict overall access to Portal items
Trusted Servers

- A list of servers to where web-tier credentials will be included when a web map or app makes a CORS request to a secured resource.
Trusted Servers

- Proxy request from Portal cannot be used to access GIS services secured with web-tier authentication
- A cross-domain request from the browser with credentials is required
Demo

Trusted Servers in Portal for ArcGIS
Allow Portal Access

- Needed to access layer from other Portals that use SAML authentication
SAML Access to any ArcGIS Enterprise
Bring secured services together from anywhere!
Demo

Allow Portal Access
Scan Portal for Security Checks

- **portalScan.py** is a script in the Portal installation directory
  - Location: `<install_directory>\ArcGIS\Portal\tools\security`
- When you run the script, it checks for security settings → generates a report that makes recommendations to improve security

---

**Portal for ArcGIS Security Scan Report - 02/28/18**

**Version:** (10.6.0)

### Potential security items to review

<table>
<thead>
<tr>
<th>Id</th>
<th>Severity</th>
<th>Property Tested</th>
<th>Scan Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS01</td>
<td>Critical</td>
<td>Proxy restrictions</td>
<td>The portal proxy capability is unrestricted. This should be limited to trusted web addresses. <a href="#">More information</a></td>
</tr>
<tr>
<td>PS03</td>
<td>Important</td>
<td>Portal services directory</td>
<td>The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. <a href="#">More information</a></td>
</tr>
<tr>
<td>PS06</td>
<td>Recommended</td>
<td>Anonymous access</td>
<td>To prevent any user from accessing content without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. <a href="#">More information</a></td>
</tr>
<tr>
<td>PS05</td>
<td>Recommended</td>
<td>Built-in account sign-up</td>
<td>By default, users can click the Create An Account button on the portal sign-up page to create a built-in portal account. If you are using enterprise accounts or you want to create all accounts manually, this option should be disabled. <a href="#">More information</a></td>
</tr>
<tr>
<td>PS09</td>
<td>Recommended</td>
<td>Cross-domain requests</td>
<td>Cross-domain requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. <a href="#">More information</a></td>
</tr>
</tbody>
</table>
Demo

Run portalScan.py
Security Check
Agenda

- ArcGIS Server
- Portal for ArcGIS
- **Advanced Topics**
  - SSL protocols for Server and Portal
  - Define cipher suites to encrypt communications
  - Securely transmitting ArcGIS tokens
In 10.4, both Server and Portal can be configured to limit which SSL protocol is accepted and used.

For organizations that are very security-aware, restricting Server and Portal to TLS 1.2 is highly recommended.

TLS (and its predecessor SSL) are cryptographic protocols designed to provide secure network communication between a client and a server.
SSL Protocols and Cipher Suites

**SSL Certificates**
- **Portal Administrator Directory**
  - Security > SSLCertificates

**Server Administrator Directory**
- Security > Config

---

**Portal Administrator Directory**

**SSL Certificates**
- loaned
- portal
- exmoor
- samjcct

- **Web Server SSL Certificate**: loaned
- **Web Server SSL Protocols**: TLSv1.2, TLSv1.1, TLSv1
- **Web Server SSL Cipher Suites**: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA

---

**Server Administrator Directory**

**Security Configuration**

- **Configuration Properties**
  - **Protocol**: HTTPS Only
  - **SSL Protocols**: TLSv1.2, TLSv1.1, TLSv1
  - **SSL Cipher Suites**: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA
Securely Transmitting ArcGIS Tokens
enterprise.arcgis.com > Search “securely transmitting tokens”

• X-Esri-Authorization request header for tokens
  - Token not transmitted as a query parameter in GET requests
  - Reduces exposure of tokens

```plaintext
GET https://arcgis.mydomain.com/arcgis/rest/services/SampleWorldCities/MapServer?f=pjson HTTP/1.1
Host: arcgis.mydomain.com
X-Esri-Authorization: Bearer xMTuPSyPAbj8STTyfbZdV7tdEbYB1DKusVkmB3Fhz7zO1MVQD0zDsm1V3Cm-ZbFo-
```
Check for Updates / Patch Notification

Installed Components
- Portal for ArcGIS 10.5.1

Available Updates
- Portal for ArcGIS 10.5.1 Custom Basemap Extent Patch
  - Products: Portal for ArcGIS
  - Release Date: 08/03/2017
- Portal for ArcGIS Security 2018 Update 1 Patch (1)
  - Products: Portal for ArcGIS
  - Release Date: 02/14/2018
- ArcGIS Security Update for Flexera CVE-2016-10395 patch
  - Products: ArcGIS Server, Portal for ArcGIS
  - Release Date: 08/02/2017

Installed Patches
- Portal for ArcGIS
  (none)

To browse a full list of Esri patches and service packs, visit the Esri Support site:
http://support.esri.com/Downloads
Security Findings?

Esri PSIRT!


- **Vulnerability** - report a vulnerability found in our site or application.

- **Suspicious E-mail from Esri** - if you believe you were targeted by a possible phishing attack from an Esri e-mail address, or have received other suspicious e-mail correspondence from Esri.

- **Privacy Issue** - if you have a privacy concern related to our application or organization.

- **Other** - for all other security, privacy or compliance related concerns.
Please Take Our Survey!

Download the Esri Events app and find your event.

Select the session you attended.

Scroll down to the “Feedback” section.

Complete Answers, add a Comment, and Select “Submit”.

Attend this session to learn about concepts that will allow you to create ArcGIS Runtime apps for the devices. These apps will include UX design, content, patterns, map design and the like.

The title and description were consistent with the content presented.

The presentation was well organized and presented clearly.

The presenter exhibited strong public speaking skills.

The session provided information or techniques I can apply right away.

I would recommend this session to a colleague.

Comments

Enter your personal notes here.