ArcGIS Enterprise Security: Advanced

Gregory Ponto & Jeff Smith
Agenda

- Focus: Security best practices for ArcGIS Enterprise
- ArcGIS Server
- Portal for ArcGIS
- 10.5.x Features

Strongly Recommend:
Knowledge of ArcGIS Server and Portal for ArcGIS
Security is Important
http://www.databreachtoday.com/news

Data Breach
Hackers Leak Data of 5 South Asian Banks
Varun Haran • May 11, 2016

Data Breach
LinkedIn Breach: Worse Than Advertised
Mathew J. Schwartz • May 18, 2016

Data Breach
32.8 Million Twitter Credentials May Have Been Leaked
Marianne Kolbasuk McGee

More than 32.8 million Twitter credentials e-mailed and are being sold on the darknet via the LeakedSource forum. The 29GB file appears to contain some security data, but most of the data is unencrypted and authentic.

Data Breach
$5.5 Million HIPAA Settlement for Florida Provider
Marianne Kolbasuk McGee • February 17, 2017

Federal regulators have signed a $5.5 million HIPAA settlement with a Florida-based healthcare system for breaches related to unauthorized employee access to more than 100,000 patients' information in a case that subsequently led to federal criminal charges.
ArcGIS Enterprise
Logical Architecture

Focus

ArcGIS Web Adaptor
ArcGIS Web Adaptor
ArcGIS Server
ArcGIS Data Store
(relational + tile cache)

Portal for ArcGIS
Agenda

- **GIS Server**
  - Enable and use HTTPS
  - Disable services directory
  - Restrict cross domain requests
  - Restrict file 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

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: 10.5.1

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
Disable the Services Directory

- ArcGIS Services Directory exposes GIS web services
  - [http://localhost/ArcGIS/rest](http://localhost/ArcGIS/rest)
- Recommend to NOT expose GIS web services on Production Servers

**Before**

- ArcGIS REST Services Directory
  - Home > services
  - Home > search
  - Folder: /
  - Current Version: 10.51
  - View Footprints In: ArcGIS Online map viewer
  - Folders:
    - Utilities
  - Services:
    - [Colorado](#) (FeatureServer)
    - [Colorado](#) (MapServer)
    - [SimpleWorldCities](#) (MapServer)
  - Child Resources: Info, Self
  - Supported Interfaces: REST, SOAP, Sitemap, Geo Sitemap

**After**

- ArcGIS REST Framework
  - Home
  - Error: Services Directory has been disabled.
  - Code: 403
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

<table>
<thead>
<tr>
<th>Services Directory</th>
<th>ArcGIS Server Administrator Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Services Directory : Enabled.</td>
<td>Home &gt; system &gt; handlers &gt; rest &gt; servicesdirectory &gt; edit</td>
</tr>
<tr>
<td>AllowedOrigins : *</td>
<td></td>
</tr>
<tr>
<td>Javascript API URL : <a href="http://js.arcgis.com/3.18/init.js">http://js.arcgis.com/3.18/init.js</a></td>
<td></td>
</tr>
<tr>
<td>Javascript API CSS URL : <a href="http://js.arcgis.com/3.18/dijit/themes/tundra.css">http://js.arcgis.com/3.18/dijit/themes/tundra.css</a></td>
<td></td>
</tr>
<tr>
<td>Javascript API CSS2 URL : <a href="http://js.arcgis.com/3.18/esri/css/esri.css">http://js.arcgis.com/3.18/esri/css/esri.css</a></td>
<td></td>
</tr>
<tr>
<td>ArcGIS.com Map Text : ArcGIS Online map viewer</td>
<td></td>
</tr>
<tr>
<td>ArcGIS.com URL : <a href="http://www.arcgis.com/home/webmap/viewer">http://www.arcgis.com/home/webmap/viewer</a></td>
<td></td>
</tr>
</tbody>
</table>

**Edit Services Directory**

<table>
<thead>
<tr>
<th>Services Directory Enabled : [ ]</th>
<th>edit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Javascript API SDK URL :</td>
<td><a href="http://js.arcgis.com/3.18/dijit/themes/tundra.css">http://js.arcgis.com/3.18/dijit/themes/tundra.css</a></td>
</tr>
<tr>
<td>Javascript API CSS URL :</td>
<td><a href="http://js.arcgis.com/3.18/esri/css/esri.css">http://js.arcgis.com/3.18/esri/css/esri.css</a></td>
</tr>
<tr>
<td>Javascript API CSS2 URL :</td>
<td>edit</td>
</tr>
<tr>
<td>ArcGIS.com Map Text :</td>
<td>ArcGIS Online map viewer</td>
</tr>
<tr>
<td>ArcGIS.com URL :</td>
<td><a href="http://www.arcgis.com/home/webmap/viewer">http://www.arcgis.com/home/webmap/viewer</a></td>
</tr>
</tbody>
</table>

Format: [HTML]
Restrict Cross-Domain (CORS) Requests

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

- By default, ArcGIS Server allows cross-domain requests so that client apps can invoke its services from any domain
How to Restrict Cross-Domain Requests

- **For JavaScript**, a common method used to make cross domain requests is called a CORS request (cross origin resource sharing).
- These can be restricted in the Server Administrator Directory:
  - system > handlers > rest > servicesdirectory > edit
  - AllowOrigins field: specify a comma-separated list of domain names that are allowed to make CORS requests to access your web services.

### ArcGIS Server Administrator Directory

<table>
<thead>
<tr>
<th>Service Directory</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Javascript API URL</td>
<td><a href="http://js.arcgis.com/3.18/init.js">http://js.arcgis.com/3.18/init.js</a></td>
</tr>
<tr>
<td>Javascript API CSS URL</td>
<td><a href="http://js.arcgis.com/3.18/dijit/themes/tundra/tundra.css">http://js.arcgis.com/3.18/dijit/themes/tundra/tundra.css</a></td>
</tr>
</tbody>
</table>
Demo

Restrict Cross-Domain Requests
Restrict File Permissions

- Recommend restrict file and folder permissions on
  - ArcGIS Server installation directory
  - Configuration store
  - Server directories
  to the ArcGIS Server account

- Your organization may require that additional accounts have access
  - Warning: Any account with write access to the configuration store can change ArcGIS Server settings
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 - 07/03/17

`loanr13238.esri.com (10.5.1)`

<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>
<tr>
<td>SS09</td>
<td>Important</td>
<td>Dynamic workspace</td>
<td>Map service: SampleWorldCities Dynamic workspace is enabled for this map service. To prevent a malicious party from obtaining the workspace ID and potentially gaining access, this should be disabled. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS07</td>
<td>Important</td>
<td>Rest services directory</td>
<td>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. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS12</td>
<td>Recommended</td>
<td>Feature service operations</td>
<td>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. <a href="#">More information</a></td>
</tr>
<tr>
<td>SS11</td>
<td>Recommended</td>
<td>PSA account status</td>
<td>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. <a href="#">More information</a></td>
</tr>
</tbody>
</table>
Demo

Run serverScan.py
Security Check
Agenda

- **GIS Server**
- **Portal for ArcGIS**
  - Enforce HTTPS Communication only
  - Disable ArcGIS Portal Directory
  - Restrict proxies
  - Disable the ‘Create Account’
  - 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
How to Disable ArcGIS Portal Directory

- Access the Portal Administrator Directory
  - Security > Config > Update Security Configuration
  - Set property = ‘true’
Restrict Proxy Hosts

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

- Portal ships with a built-in proxy server that is used in some scenarios to access resources on a different machine.
- 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
Disable ‘Create Account’ on Login Page

- Recommend disable ability to create a new Portal account
- Access Portal Administrator Directory
  - System > Properties

![Sign In Page](image1)

![Portal Administrator Directory](image2)

System Properties

- Properties: 
  
  ```
  {
  "disableSignup": "true"
  }
  ```

- Resources: Update Properties
- Supported Interfaces: REST
Trusted Servers List in Portal

- Configure list of trusted servers that work with Portal for ArcGIS
- My Organization > Edit settings > Security
Trusted Servers in Portal

- A list of servers to where credentials will be passed when making a CORS request to access secured resources.
Trusted Servers in Portal for ArcGIS
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 - 03/02/17

loanerr12306.esri.com (10.5.0)

<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>
</tbody>
</table>
Demo

Run *portalScan.py*

Security Check
Agenda

• GIS Server
• Portal for ArcGIS
• Advanced Topics
Password settings for Portal (long passwords, complex, etc)

- Portal > My Organization > Edit Settings > Security > Update Password Policy
SSL Property Configurations
https://www.ssllabs.com/ssltest/clients.html

- 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.

Client App

TLS 1.0

TLS 1.2

Port: 6443

Port: 7443

Portal for ArcGIS

Ports:
- 6443
- 7443
How to Specify Cipher Suites

- Access the Portal Administrator Directory
  - Security > SSLCertificates > Update
  - For the SSL Protocols text box, specify the protocols to be used
SAML Access to any ArcGIS Enterprise
Bring secured services together from anywhere!

- Feature: “Allow Portal Access”
  - Portal > My Organization > Edit Settings > Security
Demo

Allow Portal Access
Collaboration

Security Considerations
What is it?
Collaboration
As a Developer what do I need to know?

- Collaborating Apps
  - Oauth?
  - App ID?
  - Access Token?
Collaboration
As an Administrator what do I need to know?

- Collaborating…Service by Reference
  - Low Risk
Collaboration
As an Administrator what do I need to know?

- Collaborating…Feature Layer by Copy
  - Moderate Risk
Collaboration
As an Administrator what do I need to know?

• Collaborating…Data Items
  - Moderate Risk
Collaboration
As an Administrator what do I need to know?

- Transitive Trust
  - High Risk

ArcGIS Enterprise

ArcGIS Enterprise

ArcGIS Enterprise

Data

Data

Data
Collaboration
As an Administrator what do I need to know?

• **Recommended Practices**
  - Limit Collaborations to Trusted Partners
  - Collaborate Layers by Reference
  - Establish New Groups for Collaboration
## Other Related Sessions

<table>
<thead>
<tr>
<th>Session</th>
<th>Date and Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArcGIS Enterprise Security: An Introduction</td>
<td>Tuesday, July 11, 10:15 AM</td>
<td>SDCC - Room 16 B</td>
</tr>
<tr>
<td>ArcGIS Enterprise Security: Advanced Topics</td>
<td>Tuesday, July 11, 1:30 PM</td>
<td>SDCC - Room 16 B</td>
</tr>
<tr>
<td>Designing a Web GIS Security Strategy</td>
<td>Tuesday, July 11, 3:15 PM</td>
<td>SDCC - Room 31 B</td>
</tr>
<tr>
<td>Building Security into Your System</td>
<td>Tuesday, July 11, 4:30 PM</td>
<td>SDCC - Esri Services (Showcase)</td>
</tr>
<tr>
<td>ArcGIS Enterprise: Introducing Portal for ArcGIS</td>
<td>Wednesday, July 12, 10:15 AM</td>
<td>SDCC - Room 09</td>
</tr>
<tr>
<td>ArcGIS Enterprise Security: An Introduction</td>
<td>Thursday, July 13, 8:30 AM</td>
<td>SDCC - Room 14 A</td>
</tr>
<tr>
<td>ArcGIS Enterprise Security: Advanced Topics</td>
<td>Thursday, July 13, 10:15 AM</td>
<td>SDCC - Room 14 A</td>
</tr>
<tr>
<td>Best Practices for Configuring Secured Services</td>
<td>Thursday, July 13, 12:30 PM</td>
<td>SDCC - Demo Theater 09</td>
</tr>
<tr>
<td>Designing a Web GIS Security Strategy</td>
<td>Thursday, July 13, 3:15 PM</td>
<td>SDCC - Room 32 A</td>
</tr>
<tr>
<td>ArcGIS Enterprise: Introducing Portal for ArcGIS</td>
<td>Friday, July 14, 9:00 AM</td>
<td>SDCC - Room 04</td>
</tr>
</tbody>
</table>
Key Takeaways

Summary

- Use Server Scan Script to Validate ArcGIS Server Security
- Use Portal Scan Script to Validate Portal for ArcGIS Security
- Developers: Collaborating Apps = No code changes required
- Admins: Collaborate Carefully, *particularly when sharing Data Items*
Please Take Our Survey on the **Esri Events App**!

**Download the Esri Events app and find your event**

**Select the session you attended**

**Scroll down to find the survey**

**Complete Answers and Select “Submit”**