Schedule

• Security overview & setup
• Securing GIS services
• Working with tokens and proxy pages
• Web apps and security patterns

• We will answer questions at the end on the session

Please complete the session survey!
Security overview and setup
Security overview

- ArcGIS Server security provides access control
  - Users belong to specific roles
  - Roles can access particular services and applications

- Remember other security tasks
  - Security during transmission
  - Operating system – updates, virus protection
  - Code – SQL injection, cross-site scripting, etc.
  - Physical security
  - User education – phishing, etc.
Fundamental concepts

Who are you? What can you do?

Authentication

Authorization

Who are you? What can you do?

Client → Resource
Authenticating users - Windows

- Authentication requires storage location for Principals
  - Windows
  - SQL Server
  - Custom

Client

IIS

ASP.NET

IIS Authentication

ASP.NET Authentication

Windows
Managed by OS

Custom
SQL Server

ASP.NET 2.0 membership
Authenticating users - Java

- Authentication requires storage location for Principals
  - Java EE
  - Derby / External
  - LDAP
  - AD

![Diagram showing the flow of authentication in Java EE and related services.]

Diagram includes:
- Client
- Java EE container
- ArcGIS Server Managed
- Realm
- Custom
- LDAP / AD
- Derby / External DB

Principal Stores are managed by Java EE container.
Configuring security

• Plan the implementation
  - Identify authentication model
  - Install supporting items
    - Database or custom provider
    - SSL Certificate

• Configure the user/role store
  - Create users/roles
  - Assign users to roles

• Assign roles to folders/services

• Enable and test service security

• Secure applications
Demo
Configuring access control
Securing GIS services
Transitioning ArcGIS Server: Open → Secured

- Enabling security for services is set separately from permissions
  - Security-Settings tab

- With no security, everyone has access to everything

- If you enable security before changing permissions, no one will be able to use existing services
Capabilities have same security as service

- **Services**
  - Map, Geodata, Geoprocessing, Geocode, Geometry, Globe, Image, Search

- **Capabilities**
  - KML, WMS, WFS, WCS, Mobile Data, Feature Access, Network Analysis

- **What if I want secure editing with public viewing?**
  - Publish two map services
Securing GIS web services

- Services inherit folder permissions

- Good practice to secure folders

- Permissions changes cascade to all children
  - Set permissions on root first
More details on users and roles

- User and role store usually same place, but can have
  - Windows users + database roles
  - Windows users + roles in custom provider
  - Database users + roles in custom provider

- Built-in roles (Token based security only)
  - Everyone (*): all users logon not required
  - Authenticated Users (@): logon IS required
  - Anonymous (?): must NOT be logged on
Securing ArcGIS Server services

- Two ways to connect to an ArcGIS Server service
  - **Local ("Intranet") connection**
    - Works only on intranets
    - Access to all server functionality
    - User must be a member of the agsusers or agsadmin groups
  - **Web service ("Internet") connections**
    - SOAP, REST, WMS, KML
    - Works on intranets and over Internet
Using secured services

- **ArcGIS Desktop, Explorer**
  - Provide identity via log on dialog
- **SOAP, and REST applications**
  - Use token or Windows authentication
  - More on this shortly
SSL for services

• Require encryption
  - Set ONLY at the folder level
  - Folder property
  - Set in Catalog or Manager

• When is it needed?
  - Using Basic or Digest security
  - Protect token from intercepted in transmission
  - Sensitive geometry is dynamically displayed
  - Queried attributes contain sensitive information
Working with tokens and proxy pages
The Token service

• User authentication web service
  - Token provided to access services
  - Uses HTTPS by default

• Why do we need it?
  - Web service security when using
    - Windows: ASP.NET membership / role provider
    - Java: ArcGIS Server Managed Authentication

• Used only with GIS Web services
  - Not used by default with Windows users
  - Not used to authenticate Web application users
What is in a token?

- Token is a string with encrypted information:
  - User name
  - Expiration time
  - Client ID (optional)
    - IP address or Web URL (HTTP Referrer)
    - If included, expiration can be a longer time period (weeks/months)
      - Used by most clients – Desktop, ADF, Web API/REST applications, etc.
    - If not included, shorter expiration time – needs to be renewed

User name: PetePlanner
Timeout: 90 min
Identifier: srva.esri.com/webApp

- hpWKwqlTkOKiQipeXmyKQEGJzAfZZsVxYVD1%
Working with the token service

• ArcGIS Clients will work with tokens automatically
  - ArcGIS Desktop and ArcGIS Engine
  - ArcGIS Explorer
  - Services Directory

• Other Clients will require explicit token management
  - SOAP-based clients not using ADF
    - Use server-side code to acquire and use token
  - Web API/REST Clients
    - Developer obtains a token from get-token Web page
    - Developer embeds token in application or proxy
Getting a token

Services Directory

- HTTP://myWebAppHost/myApp
  - App must be accessed via HTTP
- myWebAppHost/myApp
  - App can be accessed via HTTP or HTTPS
- Use IP with proxy page (more later)

Copy the following token into your application:

uLjCoVnuUP-lUTnhMtJtm3KYjZ_77efAeDQVCaB3sY.
How developers commonly use the token service

1. Developer uses Token service page
2. Enter required information
3. Client requests token
4. Credentials validated
5. Service returns token
6. Copy/Paste token from token page into web app code
How the Web APIs/REST clients use the token

1. Client requests with token
2. Get user’s roles/authorizes roles
3. Server returns service data

Client Applications

Web server

Web service handler

Token service

Principal Store (Users & Roles)

Permission Store (.SEC files)

GIS Services
Using a token

- Append the token to the URL of the server
  - http://.../arcgis/services/myService/MapServer?token=hpWkqw...

- Use HTTPS
  - For maximum security over unsecure networks
  - To guard against token hijacking and replay attacks
Securing Web API applications:
Embed the token directly in code
When the token expires...

- All tokens expire
- HTTP error code of 498
- Refresh embedded tokens periodically
  - Source / config file update

Error 498: Invalid token
Embedding tokens in a proxy page

• Proxy page
  - Embed token using servers IP address as referrer
    - Pro: Token not exposed to client
    - Con: Tokens must still be updated in proxy page
  - Embed user name and password for dynamic token generation
    - Pro: No ongoing maintenance
    - Con: User name and password is unencrypted on the server

• Forum post contains dynamic proxy:
  
Proxy page security

- Proxy page contains no security logic
  - You MUST secure the proxy page
- Include proxy in web application and secure the application
- See [Using the proxy page](#) in JavaScript API help
Securing Web API applications:
Bind the token in a web proxy page
Web apps and security patterns
Application security considerations

- Browser based applications (JavaScript, Flex, Silverlight)
  - Application and web services need to be secured
  - Web services are accessed from the browser
Securing Web API applications

- Can’t secure applications with only client-side code
- Secure using the web server / container
  - IIS / Java EE
- Using ASP.NET
  - IIS 6: Wrap code in .aspx page
  - IIS 7: Application Pool Integrated Pipeline
- Other
Passing identity from Web API to services

- JavaScript, Flex, and Silverlight
  - It just works
- Integrated Windows / Basic automatically pass credentials from application to web services
Passing identity to Secured Services

- Web application requests token from tokens services
  - Tokens service parameters
    - username
    - password
    - clientid (ref.[URL], ip.[IP ADDRESS])
    - Expiration (minutes)
  - E.g.:
    https://host/ArcGIS/tokens/?request=getToken&username=user
    &password=pass&clientid=ref.myAppHost&expiration=10
- Append token to layer
Demo

Securing Web API applications:
Write full logon access to the token service
Token based Web API implementations

- **Embed the token directly in code**
- **Bind token in a web proxy page**
- **Write full logon access to the token service** (e.g., ArcGIS Desktop, custom application)

Diagram:
- IIS
- ArcGIS SOAP/REST
- Proxy page
- Secured container
- Token server
- Token
- User ____
- Password ___
- https://...
## Security patterns

<table>
<thead>
<tr>
<th>Application configuration</th>
<th>Security model</th>
<th>Embed token in proxy page</th>
<th>Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public app with secure services</td>
<td>Token based security</td>
<td>No</td>
<td>Internet / Intranet</td>
</tr>
<tr>
<td>Secure app with secure services</td>
<td>All security models</td>
<td>Yes</td>
<td>Internet / Intranet</td>
</tr>
<tr>
<td>Public app with login for secure services</td>
<td>Token based security</td>
<td>No</td>
<td>Internet / Intranet</td>
</tr>
<tr>
<td>Single sign on</td>
<td>IIS Security using Integrated Windows Authentication</td>
<td>N/A</td>
<td>Intranet</td>
</tr>
</tbody>
</table>
Security resources for ArcGIS Server

- **ArcGIS Server Resource Center**
  - [http://resources.arcgis.com](http://resources.arcgis.com)
  - Accessing secure services: Web APIs

- **Enterprise Resource Center**
  - [http://resources.arcgis.com/content/enterprisegis/10.0/about](http://resources.arcgis.com/content/enterprisegis/10.0/about)

- **Supporting Resources for ArcGIS Server**
  - ArcGIS Server Help
  - Web APIs, REST, SOAP Developer Help
Want to learn more?

ESRI Training and Education Resources

• Instructor-Led (Classroom) Training
  - ArcGIS Server: Web Administration Using the Microsoft .NET Framework

• Self-Study (Virtual Campus) Training
  - ArcGIS Server Setup and Administration
  - Implementing Security for ArcGIS Server .NET Solutions

http://www.esri.com/training
Summary

• ArcGIS Server Manager enables users to
  - Configure user and role stores
  - Secure GIS Web services

• Clients work with security
  - ArcGIS Clients (Desktop, Explorer, Engine) work seamlessly
  - SOAP and REST clients may require working with tokens

• Token management is key to maintaining secure applications
Questions

• Thank you

• Please fill out the survey
Questions ?

Please fill out a session survey…