Web GIS Architecture & Security Best Practices

Witt Mathot - Senior Software Engineer
Jeff DeWeese - Enterprise Solutions Architect

2019 ESRI
FEDERAL GIS CONFERENCE
WASHINGTON, DC
Our World Is Evolving
Architecture Matters Now More Than Ever

Technology
- Virtualization
- Big Data
- IoT
- Faster Computing
- Distributed Processing
- Smart Devices
- Consumerization
- Cloud

Content
- Lidar
- Real-Time
- Field Survey
- Social Media
- Crowdsourcing
- Sensors
- GPS
- Scientific Data
- Remote Sensing
- UAVs

Applications
- Analytics
- Mobile
- Apps
- Visualization
- Collaborative
- Real-Time

Implementation
- Configurable
- Agile
- Open
- Easier
- Ready to Use
Architecture
More Than Just Technology

People
Process
Technology
Architecture

Domains

- Enterprise GIS Deployment
- Business Continuity (*high availability, disaster recovery*)
- Security
- Publication Strategies
- Distributed GIS
- Geodata Management
- Imagery Data Management
- Real-time GIS & Big Data
- Enterprise Integration
- Mobile GIS Deployment
- Desktop GIS Deployment
- Organizational Structure & IT Governance
- Operations & Monitoring
Architecture
Best Practices

1. Capability Delivery
2. Application Implementation
3. Distributed GIS
4. Automation
5. Monitoring
6. Planning for Security
7. Architecting for Security
8. Securing the Deployment
9. Security Tools
10. Adapt to Change
1 Capability Delivery
Through Rapid & Agile Implementation

- Involve stakeholders
- Keep iterations brief (~30 days)
- Stop | restart at any time
- Iterations terminate with the business need

Each iteration results in deliverable you can use
1 Capability Delivery
Using the "Esri Method"

**Understand**
- Mission / Purpose
- Goals & Objectives
- Success Criteria
- Challenges

**Plan**
- Processes & Workflows
- Information & Technology
- Workforce Capabilities
- Roadmap

**Prioritized Activities**

**Act**

1. Prepare
   - Define
   - Design
   - Communicate

2. Implement
   - Build
   - Deploy
   - Enable

3. Operate
   - Monitor
   - Measure
   - Support

4. Review
   - Outcomes
   - Utilization
   - Usability

**Revisit**
Application Implementation
Minimize cost and maximize development resources

- Configure First
- Extend Existing Apps & Templates
- Use the ArcGIS Web APIs and SDKs

Configure first for the lowest cost and least effort

Deviations from “core” increase risk!
2 Application Implementation
Case Study: City of LA's Street Wize

ArcGIS Local Perspective Template

City of LA Street Wize

- Updated styling & symbology
- Tailored workflow to the user
- Tailored application to the data
Distributed GIS
The Next Evolution in GIS Technology
Distributed GIS

An integrated set of GIS’ working together as part of a trusted collaboration

- Model after the organization
- Preserves departmental control
- Supports enterprise needs

*Each node within a distributed GIS can be one or more of the three primary systems of a modern GIS*
Collaboration across organizations

From data sync to data integration

Advancing the “Hybrid” Pattern

Distributed GIS
Powering New Architecture Patterns
Automation
Scripting Defined, Repetitive Workflows

- Efficiency
- Consistency
- Repeatability
- Productivity

New capabilities available through Python, Chef, and more …
… helping to power your DevOps workflows
Monitoring
Web GIS Enables Rapid Growth & Adoption …

... make sure the system scales to meet demand
Planning for Security

Definitions

Built-in Users
Identity Management
Kerberos
Federated Servers
Authorization
Identity Federation
FedRAMP & FISMA

Roles
Windows Authentication
LDAP
Groups

OAuth

Active Directory
Client Certificates

SSO

NTLM

Privileges

Federated Architecture
Enterprise Groups

IWA
Identity
Portal-tier Authentication
Anonymous Access

PKI

Server-tier Authentication

SSL

SAML

Named Users
Planning for Security

Security starts in architecture planning & design
Consider security requirements and constraints
Invoke stakeholders up front
Test with security “on”
Consider Tradeoffs
Goal: Avoid rework!

Align with the CIA triad
- C: "Do we need to consider data classification?"
- I: "Does the system require an identify for data changes?"
- A: "What SLA requirements need to be met?"
Planning for Security Compliance (Products and Services Security)

- FISMA / NIST
- FedRAMP
  - ArcGIS Online
    - FedRAMP Tailored Low
    - SaaS multi-tenant
  - Esri Managed Cloud Services - Advanced Plus
    - FedRAMP Moderate
    - SaaS single tenant
- USGCB
  - Federal Agency Requirement for Desktop based products (self-certified)
- Section 508
  - Federal Agency Software Accessibility Requirements for People with Disabilities

https://trust.arcgis.com
Architecting for Security
Tiered Architectures

- Enables network segmentation and access control (confidentiality)
- Supports separation of duties (integrity)
- Isolates issues to respective tier (availability)
Architecting for Security
System Availability

• What level of system availability is required?
  - 95%: No redundancy
  - 99%: Redundancy
  - 99.9%: Redundancy + Disaster Recovery

• Highly-Available System Architecture
  - Increased complexity/cost
  - Load balancers
  - Redundant servers
  - HA file storage
  - Additional administration
## Architecting for Security

### Business Continuity

<table>
<thead>
<tr>
<th>Tier</th>
<th>Criticality</th>
<th>Recovery Time (RTO)</th>
<th>Recovery Point (RPO)</th>
<th>Others… (test frequency, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tier 1</td>
<td>Mission Critical</td>
<td>&lt; 4 hours</td>
<td>&lt; 1 hour</td>
<td>…</td>
</tr>
<tr>
<td>Tier 2</td>
<td>Business Critical</td>
<td>&lt; 24 hours</td>
<td>&lt; 1 hour</td>
<td>…</td>
</tr>
<tr>
<td>Tier 3</td>
<td>Significant</td>
<td>&lt; 72 hours</td>
<td>&lt; 48 hours</td>
<td>…</td>
</tr>
<tr>
<td>Tier 4</td>
<td>No Impact</td>
<td>&lt; 1 week</td>
<td>&lt; 1 week</td>
<td>…</td>
</tr>
</tbody>
</table>

**NOTE:** GIS deployments are becoming more prevalent within Tiers 1-2
Architecting for Security
Workload Separation

- Start with a base ArcGIS Enterprise, primarily focused on hosted services and enabling GIS functionality (e.g., Vector Tiles)

- Deploy additional separate sites as needed
  - Highly used dynamic map services
  - Heavyweight geoprocessing services
  - CPU-intensive routing services
  - Mission-critical services that have different SLAs
  - Geoevent processing
  - Image and Raster Analytics services
Architecting for Security
ArcGIS Enterprise Federation

- **Benefits**
  - Security
    - Shared identity, SSO
    - Enables GIS Server w/ SAML
    - Portal groups for authorization
    - Shared roles w/ restricted publishing
    - Portal item management
    - Required for Pro Publishing/Admin
    - More capabilities in future

- **Considerations**
  - Highly distributed environments
  - Version consistency (upgrades)
  - HA and DR complexities
Securing the Deployment

Key Security Mechanisms

- Authentication
- Authorization
- Encryption
- Filtering
- Logging & Auditing
Securing the Deployment
Identity and Authorization

**User Stores**
- Built-In
- Enterprise
  - Active Directory
  - LDAP
  - More (SAML)

**Authentication**
- ArcGIS Token-Based
- Web-Tier
- SAML (Enterprise Logins)

**Authorization**
- Roles
- Groups
- Enterprise Groups
- Server GIS Model
- Advanced Options
- Encryption is the process of encoding a message so that it can be read only by the sender and the intended recipient.

- **Data-In-Transit:**
  - Protocol: HTTPS, Transport Layer Security (TLS), etc.

- **Data-At-Rest:**
  - File System: BitLocker, Self-encrypting drives (SEDs)
  - RDBMS: Transparent Data Encryption

- **Algorithms:**
  - Advanced Encryption Standard (AES), Secure Hash Algorithms (SHA), etc.
  - Cryptography is constantly changing (monitor NIST)
Filtering involves the screening of undesirable content or malicious requests typically through rules or detection through signatures or anomalies.

- Firewalls
- Reverse Proxy
- Web Application Firewall
- Anti-Virus software
- Intrusion Detection Systems (IDS)
Securing the Deployment
Web Application Firewall (WAF)

- More sophisticated than a traditional port-based firewall
- Operates at Layer 7 and can inspect the contents of the HTTP conversation
- Protects your web application from web vulnerabilities and attacks
- A WAF is becoming standard for secured architectures, particularly in the cloud
- Often coupled with a Layer 7 Load balancer to create an Application or Security Gateway
Securing the Deployment

Logging & Auditing

- **Logging** involves recording events of interest from a system.
- **Auditing** is the practice of inspecting those logs to ensure system is functioning desirably or to answer a specific question about a particular transaction that occurred.

- Ensure logging across the system: applications, operating system and network

- Logging Capabilities
  - Geodatabase history
  - Web Server logs
  - Portal logs
  - ArcGIS Server logs
  - ArcGIS Monitor

```
<Msg time='2009-10-31T14:36:05'
type='INFO3'
code='4004'
target='Yellowstone.MapServer'
machine='padisha'
user='Fred'
thread='2936'
elapsed='2.443'>
Server Object instance is success
</MSG>
```
ArcGIS Server Security Tools

- ArcGIS Server Best Practices
  - Requesting and configuring your own server certificate
  - Restricting file permissions
  - Disabling the primary site administrator account
  - Defining the shared key used to generate an ArcGIS token
  - Securely transmitting ArcGIS tokens
  - Using standardized queries
  - Disabling the Services Directory
  - Restricting cross-domain requests

- ArcGIS Server - ServerScan.py
  - ArcGIS Server comes with a Python script tool that scans for some common security issues.
  - Based on documented ArcGIS Server Best Practices (above)
  - Analyzes twelve criteria or configuration properties and divides them into three severity levels

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS01</td>
<td>Critical</td>
<td>Web communication</td>
<td>Determines if HTTPS is enabled for ArcGIS Server. To prevent the interception of any communication, it is recommended that you configure ArcGIS Server and ArcGIS Web Adaptor (if installed) to enforce SSL encryption.</td>
</tr>
<tr>
<td>SS02</td>
<td>Critical</td>
<td>Standardized queries</td>
<td>Determines if standardized queries are enforced. To provide protection against SQL injection attacks, it is critical that this option be enabled.</td>
</tr>
<tr>
<td>SS03</td>
<td>Critical</td>
<td>Token requests</td>
<td>Determines if generate token requests via GET are supported. When generating tokens via GET, a user’s credentials are sent as part of the URL and can be captured and exposed through browser history or network logs. This should be disabled unless required by other applications.</td>
</tr>
<tr>
<td>SS04</td>
<td>Critical</td>
<td>Token requests</td>
<td>Determines if generate token requests via POST with credentials in the query parameter are supported. When generating tokens, a user’s credentials could be provided as part of the URL and may be exposed through browser history or network logs. This should be disabled unless required by other applications.</td>
</tr>
</tbody>
</table>
Security Tools
Portal for ArcGIS Security Tools

- Portal for ArcGIS Best Practices
  - Restrict the portal's proxy capability
  - Disable anonymous access
  - Configure CA-signed server certificates
  - Configure HTTPS
  - Disable the ArcGIS Portal Directory
  - Configure your firewall to work with the portal
  - Specify the default token expiration time
  - Restrict file permissions

- Portal for ArcGIS - PortalScan.py
  - Portal for ArcGIS comes with a Python script tool that scans for some common security issues.
  - Based on documented Portal for ArcGIS Best Practices (above)
  - Analyzes six criteria or configuration properties and divides them into three severity levels

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PS01</td>
<td>Critical</td>
<td>Proxy restrictions</td>
<td>Determines if the portal's proxy capability is restricted. By default, the portal proxy server is open to any URL. To mitigate against potential Denial of Service (DoS) or Server Side Request Forgery (SSRF) attacks, it's strongly recommended that you restrict the portal's proxy capability to approved web addresses.</td>
</tr>
<tr>
<td>PS02</td>
<td>Critical</td>
<td>Token requests</td>
<td>Determines if generate token requests with credentials in the query parameter are supported. If supported, when generating tokens, a user’s credentials could be provided as part of the URL and may be exposed through browser history or in network logs. This should be disabled unless required by other applications.</td>
</tr>
<tr>
<td>PS03</td>
<td>Important</td>
<td>Portal services directory</td>
<td>Determines if 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.</td>
</tr>
<tr>
<td>PS04</td>
<td>Important</td>
<td>Secure communication</td>
<td>Determines if the portal communicates through HTTPS only. To prevent the interception of any communication within the portal, it’s recommended that you configure your portal and the web server hosting the Web Adapter to enforce SSL.</td>
</tr>
</tbody>
</table>
Security Tools
Security Tools - Links

- **ArcGIS Server**
  - Best Practices
  - ArcGIS Server - ServerScan.py
    - `<ArcGIS Server installation location>/tools/security>`

- **Portal for ArcGIS**
  - Best Practices
  - Portal for ArcGIS - PortalScan.py
    - `<Portal for ArcGIS installation location>/tools/security>`
• Esri is committed to using the latest industry standards and best practices for security protocols
• On April 16, 2019, we are updating ArcGIS Online to enforce the use of TLS (Transport Layer Security) version 1.2
• What Does This Mean For You?
  - Users of most ArcGIS software or custom solutions using Esri technology may be affected by this planned update - If you have not updated and validated your system's support for TLS v1.2 only, you may lose your ability to connect to ArcGIS Online.
• What Do You Need to Do?
  - Go to the Esri TLS Support page for information, patches, and instructions for updating software:

  https://support.esri.com/en/tls
Architecture
Top 10 Best Practices

1. Capability Delivery
2. Application Implementation
3. Distributed GIS
4. Automation
5. Monitoring
6. Planning for Security
7. Architecting for Security
8. Securing the Deployment
9. Security Tools
10. Adapt to Change
Architecture
More Than Just Technology

People

Process

Technology
<table>
<thead>
<tr>
<th>WORKSHOP</th>
<th>LOCATION</th>
<th>TIME FRAME</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tuesday</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ArcGIS Monitor: An Introduction</td>
<td>102 A</td>
<td>3:00 – 4:00pm</td>
</tr>
<tr>
<td>• ArcGIS Enterprise Security: An Introduction</td>
<td>102 A</td>
<td>4:15 – 5:15pm</td>
</tr>
<tr>
<td>• Architecture Best Practices</td>
<td>102 B</td>
<td>4:15 – 4:45pm</td>
</tr>
<tr>
<td>• Distributed Collaboration with ArcGIS Enterprise</td>
<td>Implementing ArcGIS</td>
<td>4:15 – 5:15pm</td>
</tr>
<tr>
<td>• Esri Managed Cloud Services: An Introduction</td>
<td>204 B</td>
<td>4:15 – 5:15pm</td>
</tr>
<tr>
<td><strong>Wednesday</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• ArcGIS Online: A Security, Privacy, and Compliance Overview</td>
<td>209 C</td>
<td>8:30 – 9:30 am</td>
</tr>
<tr>
<td>• Distributed Collaboration with ArcGIS Enterprise</td>
<td>102 B</td>
<td>8:30 – 9:30 am</td>
</tr>
<tr>
<td>• ArcGIS Enterprise: High Availability and Disaster Recovery</td>
<td>Demo Theater 3</td>
<td>11:00am - Noon</td>
</tr>
<tr>
<td>• Driving GIS Adoption through Organizational Change Mgmt.</td>
<td>209 A</td>
<td>11:00am - Noon</td>
</tr>
<tr>
<td>• ArcGIS Enterprise: Best Practices for Layers and Service Types</td>
<td>102 A</td>
<td>1:30 – 2:30pm</td>
</tr>
<tr>
<td>• Esri Best Practices: App Configuration, Customization or Dev?</td>
<td>204 B</td>
<td>1:30 – 2:30pm</td>
</tr>
</tbody>
</table>
# GIS Solutions Expo

**Print Your Certificate of Attendance**

Print Stations Located at L Street Bridge

<table>
<thead>
<tr>
<th>Tuesday</th>
<th>Wednesday</th>
</tr>
</thead>
<tbody>
<tr>
<td>12:30 pm – 6:30 pm</td>
<td>10:45 am – 5:15 pm</td>
</tr>
<tr>
<td><strong>GIS Solutions Expo</strong></td>
<td><strong>GIS Solutions Expo</strong></td>
</tr>
<tr>
<td>Hall D</td>
<td>Hall D</td>
</tr>
<tr>
<td>5:15 pm – 6:30 pm</td>
<td>6:30 pm – 9:00 pm</td>
</tr>
<tr>
<td><strong>GIS Solutions Expo Social</strong></td>
<td><strong>Networking Reception</strong></td>
</tr>
<tr>
<td>Hall D</td>
<td>National Museum of Natural History</td>
</tr>
</tbody>
</table>

- **GIS Solutions Expo**
- **Networking Reception**
Please Take Our Survey on the App

Download the Esri Events app and find your event

Select the session you attended

Scroll down to find the feedback section

Complete answers and select “Submit”