The ArcGIS Platform:
Security Practices and Policy

Esri Software Security & Privacy Team
Agenda

- Introduction
- Security Strategy
  - Product Based Security Initiatives
  - Solution Based Security Initiatives
- Deployment Strategy
- ArcGIS Server STIG
- Esri Managed Cloud Services (EMCS) Advanced Plus
- Summary
Introduction
It's all about reducing risk
Introduction

Security Principles – CIA Triad

Confidentiality

Integrity

Availability

CIA Security Triad
Security Strategy
Security Strategy
Evolution of Esri Products & Services

- Desktop GIS
- Server GIS
- Web GIS
- Distributed Web GIS

- 3rd Party Security
- Embedded Security
- Shared Responsibility Security
Security Strategy
Extensive security compliance history

Esri has actively participated in hosting and advancing secure compliant solutions for over a decade.
Security Strategy
Authorization levels across products and services

• Product Based Initiatives
  - ArcGIS Desktop
  - ArcGIS Server
  - ArcGIS Enterprise

• Solution/Service Based Initiatives
  - ArcGIS Online
  - Esri Managed Cloud Services Advanced Plus
Product Based Security Initiatives

Desktop Clients

• Esri performs self-certification of desktop products
  - Ensures smooth product deployments on hardened systems

• FDCC
  - Federal Desktop Core Configuration
  - Versions 9.3-10
  - Deprecated due to Windows XP focus

• USGCB
  - United States Government Configuration Baseline
  - ArcGIS Desktop Version 10.1+
  - ArcGIS Pro 1.4.1 +
Product Based Security Initiatives
ArcGIS Server – DISA STIG

• First Esri product Security Technical Implementation Guide (STIG)
  - Sponsored by government to work with DISA
  - STIG is publically accessible
  - First STIG Windows 2008/2012R2 ArcGIS Server 10.3 (2016)
  - Other STIGs will be performed based on demand

• STIG usage
  - STIG input for providing a more general Server hardening guide
  - Enterprise component integration testing and best practices incorporation
  - Immediately implemented by multiple customers upon release in 2016
Product Based Security Initiatives
DISA STIG Creation Process

Planning
- Project Kickoff
- SME and Government POC Assignment
- FSO provides materials
- Detailed Process explanation

Development
- Requirements Analysis Checkpoint
- Check and Fix Procedure Development Checkpoint
- SME support as needed
- Vendor Submission

Validation
- Compliance Evaluation
- STIG simulation
- Review of Vendor-provided Documents
- Attestation

Review and Approval
- FSO Internal Reviews
- Styleguide Review
- MAE Briefing
- MAE Approval
- Vendor Notification
- STIG publication

STIG Approved by DISA
Product Based Security Initiatives
ArcGIS Server – Awareness of Relative Risk

- Security hardening best practices provide insights into relative risk of different services, and optional mitigation measures to reduce risk

<table>
<thead>
<tr>
<th>Service</th>
<th>Capability</th>
<th>Default when Enabled</th>
<th>Security Hardened</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map</td>
<td>Mapping</td>
<td></td>
<td>Red</td>
</tr>
<tr>
<td>Map</td>
<td>Query</td>
<td></td>
<td>Yellow</td>
</tr>
<tr>
<td>Feature</td>
<td>Read</td>
<td></td>
<td>Green</td>
</tr>
<tr>
<td>Feature</td>
<td>Edit</td>
<td></td>
<td>Red</td>
</tr>
<tr>
<td>Feature</td>
<td>Sync</td>
<td></td>
<td>Yellow</td>
</tr>
<tr>
<td>Geocoding</td>
<td>Geocode</td>
<td></td>
<td>Green</td>
</tr>
<tr>
<td>Geodata</td>
<td>Query</td>
<td></td>
<td>Yellow</td>
</tr>
<tr>
<td>Geodata</td>
<td>Data Extraction</td>
<td></td>
<td>Green</td>
</tr>
<tr>
<td>Geodata</td>
<td>Replica</td>
<td></td>
<td>Green</td>
</tr>
<tr>
<td>Geoprocessing</td>
<td>Geoprocessing</td>
<td></td>
<td>Green</td>
</tr>
<tr>
<td>Image</td>
<td>Imaging</td>
<td></td>
<td>Yellow</td>
</tr>
<tr>
<td>Image</td>
<td>Edit</td>
<td></td>
<td>Red</td>
</tr>
<tr>
<td>Image</td>
<td>Upload</td>
<td></td>
<td>Yellow</td>
</tr>
</tbody>
</table>

Security Hardened Settings

- Map Services
  - Disable “Feature Access”
  - Disable “Mobile Data Access”
  - Disable “WFS”
  - Disable “Query”
  - Publish File Geodatabases

- Feature Services
  - Always Secure
  - Use Versioned Data
  - Disable “Sync”
  - Disable “Insert, Update, Delete”

- Geocoding Services
  - Publish File Geodatabases

- Geodata Services
  - Always Secure
  - Use Versioned Data
  - Grant ArcGIS Account Read-Only (RBDMS)

- Geoprocessing Service
  - Risk Varies by Script/Model Design
  - Limit Inputs

- Globe Service
  - Publish File Geodatabases
  - Disable “Query”

- Image Service
  - Disable “Edit”
  - Disable “Upload”

Red = Higher Risk
Yellow = Average Risk
Green = Low Risk

Providing new insights
Product Based Security Initiatives
Security validation and monitoring

- **ArcGIS Server and Portal security scan tool**
  - Validates best practices
  - Server and Portal 10.4 +
  - Python script
Solution Based Security Initiatives

ArcGIS Online

- ArcGIS Online
  - FISMA Low ATO by USDA (2014)
  - FedRAMP Tailored Low by DOI (2018)

- Cloud Infrastructure Providers are ISO 27001 and FedRAMP Moderate compliant
  - Amazon Web Services
  - Microsoft Azure
Solution Based Security Initiatives
ArcGIS Online Assurance Layers

AGOL SaaS
FISMA Low
(USDA)

Cloud Provider
ISO 27001
SSAE16
FedRAMP Mod

Cloud Providers

Customer

Esri

Web App Consumption
ArcGIS Management
Web Server & DB software
Operating system
Instance Security Management
Hypervisor
Physical
Solution Based Security Initiatives
Cloud deployment model responsibility
Deployment Strategy
Deployment Strategy
Real Permutations

Private IaaS

Public IaaS

Database

File

Geodatabase

Filtered Content

Internal AGS

Internal Portal

External AGS

ArcGIS Online

Field Worker

Business Partner 1

Business Partner 2

Enterprise Business

Public

Internal AGS
Deployment Strategy
ArcGIS Online Accreditation Use Cases

• **Use Case 1 – Public Dissemination**
  - Publish tiles for fast, scalable visualizations
  - Share information with the public
  - Can be used for mashing up services with external sites

• **Use Case 2 – USG Internal Operations**
  - Hybrid deployment of ArcGIS Server and ArcGIS Online
  - Share operational data within or between organizations
  - Sensitive data maintained on customer premises or other accredited environment
  - ArcGIS Online operates as a discovery portal
  - Utilize Enterprise Logins
Deployment Strategy
Hybrid – How does it work?

• Where are internal and cloud datasets combined?
  - At the browser
  - The browser makes separate requests for information to multiple sources and does a “mash-up”
  - Token security with HTTPS (TLS) or even a VPN connection could be used between the device browser and on-premises system

On-Premises Operational Layer Service

Cloud Basemap Service ArcGIS Online

Browser Combines Layers

https://YourServer.com/arcgis/rest...  +  https://services.arcgisonline.com...
Deployment Strategy
Hybrid Deployments

• Common for large enterprises

• Data Segmentation

• Meet more stringent security and compliance requirements such as CJIS by storing sensitive datasets on-premises

• ArcGIS Online or EMCS can operate as discovery portal in the cloud
Deployment Strategy
Hybrid Cloud Deployment Models

On-Premises
- Ready in months/years
- Behind your firewall
- Your security infrastructure
- You manage & certify

Esri Managed Cloud Services
- Ready in days/weeks
- All ArcGIS capabilities at your disposal in the cloud
- Dedicated services
- FedRAMP Moderate

ArcGIS Online
- Ready in minutes
- Centralized geo discovery
- Segment anonymous access from your systems
- FISMA Low

Anonymous Access
- Ready in months/years
- Behind your firewall
- Your security infrastructure
- You manage & certify

...All models can be combined or separate
Deployment Strategy

Key security areas to address

- Authentication
- Authorization
- Encryption
- Filters
- Logging/Auditing
Deployment Strategy

Security Best Practices

• Authentication – 2 Factor Authentication (2FA)
  - ArcGIS Online: SAML 2.0 or built-in accounts
  - ArcGIS for Server: Web-tier Authentication
  - Portal for ArcGIS: Web-Authentication or SAML 2.0

• Authorization – Principle of Least Privilege
  - Role Based Access Control – Administrator, Publisher, and User
    - Custom Roles in Portal and ArcGIS Online
  - ArcGIS for Server – Service level authorization set by publisher/admin roles
  - ArcGIS Online and Portal – Item level authorization set by item owner
  - Can be extended by third party components
    - Database level: Row or Feature Class Level, SDE Views
    - Web Server level: URL filtering
    - Service level: Layer / Attribute level authorization
Deployment Strategy
Security Best Practices

• Filters – Security Infrastructure
  - Web Application Firewall (WAF), Anti-virus, firewalls, reverse proxies, …
  - Intrusion Detection Systems (IDS)

• Encryption
  - In-transit – supported across products
    - Use strong protocols (TLS) and ciphers
    - IPSec with corporate VPN
  - At-rest
    - Database level: Transparent Data Encryption (TDE)
    - File based: Operation System Level (such as Bitlocker), Disk-level

• Logging and Auditing
  - Logging should be done and reviewed across application, OS, database, firewall, and other layers
  - Consolidate with a SIEM
STIG Highlights
STIG Implementation Approach
ArcGIS Server STIG

- + Windows 2012 R2 Member Server STIG
- + IIS 7.0 STIG Concepts (Applied to 8.x)
- + ArcGIS Server 10.3x STIG

Contact SoftwareSecurity@esri.com for Assistance/Guidance
Inherited Controls
ArcGIS Server STIG

• Windows Server 2012 / 2012 R2 Member Server STIG
  - Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
  - Implement Organization Approved Certificates (PKI)
  - Integrate with Central Authentication (Active Directory/LDAP)
  - Multifactor Authentication (Smartcards)

• IIS 7.0 STIG Concepts (Applied to IIS 8.5)
  - Web Tier Authentication (HTTP/PKI)

Contact SoftwareSecurity@esri.com for Assistance/Guidance
AC (Access Control)
ArcGIS Server STIG

- Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
- Implement Organization Approved Certificates (PKI)
- Integrate with Central Authentication (Active Directory/LDAP)
AC (Access Control)
ArcGIS Server STIG

- Enforce DoD Approved Encryption Algorithms (FIPS 140-2)
- Implement Organization Approved Certificates (PKI)
- Integrate with Central Authentication (Active Directory/LDAP)
Configure VERBOSE Logging with ArcGIS Server

Contact SoftwareSecurity@esri.com for Assistance/Guidance
CM (Configuration Management)
ArcGIS Server STIG

- Disable HTTP Listener
- Disable REST Services Directory
IA (Information Assurance)
ArcGIS Server STIG

- Require Certificate Authentication (MFA/Smartcards)
- Utilize Centralized Authorization (Active Directory Groups)
IA (Information Assurance)
ArcGIS Server STIG

- Require Certificate Authentication (MFA/Smarcards)
- Utilize Centralized Authorization (Active Directory Groups)
- Require Encrypted Web Access
- Disable Anonymous Web Access
SC (System & Communication Protection)
ArcGIS Server STIG

- Disable “Primary Site Administrator”

Contact SoftwareSecurity@esri.com for Assistance/Guidance
Mitigating Controls
ArcGIS Server STIG

• Access Control (AC): Endpoint Protection
  - Web Application Firewalls (eg. Barracuda, Sonicwall)

• Audit & Accountability (AU): Log Aggregation & Correlation
  - 3\textsuperscript{rd} Party SIEM (eg. Splunk, Alienvault)

Contact SoftwareSecurity@esri.com for Assistance/Guidance
Mitigating Controls
ArcGIS Server STIG

- **System & Communication Protection (SC): Mobile Code Execution**
  - Client Browser Management ("Trusted Sites")
- **System & Communication Protection (SC): DoS Protection**
  - DoS Protection (Automated IP Blacklist)

Contact SoftwareSecurity@esri.com for Assistance/Guidance
<table>
<thead>
<tr>
<th>Containment Strategy</th>
<th>Volumetric (Effectiveness)</th>
<th>Protocol (Effectiveness)</th>
<th>Application (Effectiveness)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network firewalls, subnets, segmentation</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Scaling</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Report to your ISP</td>
<td>Varies</td>
<td>Varies</td>
<td>Low</td>
</tr>
<tr>
<td>Throttling</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Low</td>
</tr>
<tr>
<td>Secure endpoints</td>
<td>Low</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Filtering (WAF)</td>
<td>Low</td>
<td>Low</td>
<td>Moderate-High</td>
</tr>
</tbody>
</table>
Mitigating Controls
ArcGIS Server STIG

- **System & Communication Protection (SC): Data Protection at Rest**
  - Whole Disk Encryption on Data Drives (Bitlocker, checkpoint, ...)
- **SI (System & Information Integrity): Automated Response to Anomalies**
  - System Center Operations Manager (SCOM, Solarwinds, ...)

Summary
ArcGIS Server STIG

• Inherited Controls
  - Windows 2012 / 2012 R2 STIG
  - IIS 7.x STIG Concepts

• Configurable Controls (ArcGIS Server)
  - Integrated Security (Active Directory & PKI)
  - Disable HTTP
  - Disable Services Directory
  - Enable Verbose Logging
  - Disable Primary Site Administrator

• Mitigating Controls
  - Whole Disk Encryption
  - Mobile Code Execution Management
  - Automated DoS Protection
  - Log Management (SIEM)
  - Automated Monitoring (SCOM)

Contact SoftwareSecurity@esri.com for Assistance/Guidance
Real World Deployments
Lessons Learned

• Distributed File Services
  - High Availability File Services
  - ArcGIS Server Config Store
  - ArcGIS Server Directories
  - File Data

• Group Managed Service Accounts
  - ArcGIS Server Service Account
  - Automated Password Management

• Encryption at Rest (Easy Win)
  - Whole Disk Encryption
  - Transparent Data Encryption

• Web Application Firewalls
  - High Effort / Maintenance
  - Automated Learning / Scoping

Contact SoftwareSecurity@esri.com for Assistance/Guidance
Esri Managed Cloud Services Advanced Plus
Esri Managed Cloud Services Advanced Plus

What is Esri Managed Cloud Services?

- Cloud-based GIS infrastructure support, including:
  - Enterprise system design
  - Infrastructure management
  - Software (Esri & 3rd Party) installation, updates, and patching
  - Application deployment
  - Database management
  - 24/7 support and monitoring

- Advanced plus offering
  - FedRAMP Moderate ATO by US Census Bureau
  - Security infrastructure & 24x7 SOC
  - Security controls and processes that align with FedRAMP moderate level
  - Initial offering based in AWS, looking at expanding into Azure based on demand
Esri Managed Cloud Services Advanced Plus
Continuous Monitoring

FedRAMP Reporting Workflow

Monitoring Workflow

Ensures maintenance of acceptable risk posture
Esri Managed Cloud Services Advanced Plus
Rigorous Third Party Security Assessment

- Must occur annually

- Third Party Assessment Organization (3PAO) accredited by FedRAMP

- Documentation
  - A security review of all FedRAMP controls and implementation details

- Technical Assessment
  - System level scans
  - Web Interface scans
  - Database scans
  - Penetration testing

Great advisors and skilled assessors keep the effort focused
Esri Managed Cloud Services Advanced Plus

Design goals

• Most government systems
  - Require moderate security baseline controls

• Most geospatial information sets
  - Only require low baseline controls
  - ArcGIS Online FedRAMP Tailored Low is adequate for many customer use cases

• EMCS FedRAMP Infrastructure Design Goals
  - Consumable by the widest range of customers
    - Amazon East-West Regions – Not limited to GovCloud
  - Drive down customer expenses for secure, compliant geospatial services
    - Customer’s can choose level of multi-tenancy vs dedicated services they are comfortable with
  - Meet and exceed current rigorous FedRAMP requirements for cloud services
    - First geospatial platform to be compliant with FedRAMP Rev 4 requirements

A balance of robust security and business requirements drove infrastructure choices
EMCS Security Infrastructure

Customer Infrastructure

End Users

Security Ops Center (SOC)

Esri Administrators

Active/Active Redundant across two Cloud Data Centers

Web Application Firewall
  WAF

ArcGIS for Portal

ArcGIS Server

Relational Database

File Servers

Intrusion Detection
  IDS / SIEM

Centralized Management
  Backup, CM, AV, Patch, Monitor

Bastion Gateway
  MFA

Authentication/Authorization
  LDAP, DNS, PKI

Cloud Infrastructure

Hypervisor, TCP/IP, Network ACLs, Routing, Storage, Hardware

Legend

Agency

Application

Cloud Provider

Security
Summary
Resources Available for Agency Review

• Cloud infrastructure provider
  - SSAE16 and ISO 27001
  - Report available from cloud providers under NDA

• FedRAMP Repository
  - ArcGIS Online Compliance Package (See FedRAMP.gov Marketplace)
  - Cloud Service Provider FedRAMP Moderate Packages

• Esri
  - Reports available from Esri under NDA
  - Cloud Security Alliance (CSA) Answers Publically Available
    - ArcGIS Online answers have been updated to newest version
Summary
Solution/Services Accreditation Roadmap

- **ArcGIS Online FedRAMP Tailored Low Authorization**
  - Agency authorization 2018

- **Esri Managed Cloud Services (EMCS) FedRAMP Moderate Authorization**
  - Agency Authorization 2015
  - Establishes validated secure clouds deployment patterns

- Documentation and assessment materials enable FISMA or FedRAMP authorization
Summary

• Esri is working with security leaders to create standardized security hardened deployment guidance for our customers
• ArcGIS Online is FedRAMP Tailored Low authorized and we can work with you to support your Agency’s authorization
• Esri Managed Cloud Services FedRAMP moderate compliant option ready for your agency to review and authorize
• Information readily available on Trust.ArcGIS.com

We welcome your feedback concerning any authorization needs or gaps not addressed in this presentation
Summary
We are here for you

• Esri’s Software Security & Privacy Team
  - Led by Esri’s Chief Product Security Officer consisting of Security Engineers and Architects
  - Leads Security Certification efforts across the ArcGIS Platform
  - Created and maintain Trust.ArcGIS.com as a one-stop shop for security and privacy
  - Performs security validation / testing of products and deployments
  - Utilizes all of the above as inputs for providing customer guidance such as this presentation

• Contact our team at: SoftwareSecurity@Esri.com
Questions?

Contact SoftwareSecurity@esri.com for Assistance/Guidance