Building Secure Applications
Dasa Paddock, David Cordes
& Tom Shippee
What’s covered in this session

• Key secured application terms
• Common secured service use cases
• Implementing OAuth-based apps
What’s covered in other security sessions

ArcGIS Online

- Building Secure Applications
- Security and ArcGIS Online

Core ArcGIS Server

- Securing ArcGIS Services Introduction
- Best Practices in Setting Up Secured Services in ArcGIS for Server

ArcGIS Online & Cloud Computing

- Security Best Practices

Enterprise Architecture

- Designing an Enterprise GIS Security Strategy
- ArcGIS Online
- Cloud Computing
Common use cases for secured services

How service URLs authenticate

- **Application (server & portal tokens)**
  - User login
    - AGOL via OAuth
    - Mobile app
    - IdentityMgr
    - In the Code
  - AGS service AGOL item via
    - Web app
    - Impersonated
    - Secured app with tokens stored
    - Mobile app
    - In a Proxy
    - IWA
  - Browser-based Authentication via
    - PKI

Web server (e.g., IIS)
- Single sign on or User login
Key secured application terms

Understanding the concepts…
Understanding authentication

• Key security decision
  - Configured by the GIS admin
  - Specific to a given ArcGIS server site

• Can occur at different levels
  - Web server (e.g., IIS)
  - Application (e.g., GIS Server)

• Verifies credentials against a user store
  - Web server requires Windows Active Directory (AD)
  - Groups and roles can be stored elsewhere
Web Server level authentication

- **Implementation**
  - Configured in the web server (e.g., IIS)
  - Runs in browser before the app is called
  - Web tier authentication in ArcGIS Server

- **Login models**
  - Integrate Windows Authentication (IWA)
    - Pass Windows login credentials
  - Basic or Digest
    - Challenges with a login dialog
Application level authentication

• Implementation
  - Web server MUST be configure for anonymous access
  - Token-based
    - ArcGIS Server uses server tokens
    - ArcGIS Online uses portal tokens
  - Requires server or portal token service
  - GIS server tier authentication in ArcGIS Server

• Login using ArcGIS Identity manager
  - Handles all login and token processing
  - Supported in all Web APIs
What is single sign on?

- **Integrate Windows Authentication (IWA)**
  - Sign in once to Windows
  - Supporting apps automatically passed Windows credentials

- **Same user credentials**
  - Sign in multiple times using the same credentials

- **SaaS Application**
  - AGOL model login once to the application
  - Token stored as an application cookie
What is OAuth?

- Industry standard enterprise authentication system
  - Login redirected to enterprise security server
  - Application NEVER see credentials

- Works with SAML
  - Server based mechanism that handles login requests
  - Supported by AGOL for enterprise authentication
  - More in final section…
Common secured service use cases

Apps to access secured services
Use case: Identity Manager

How service URLs authenticate

Application
(server & portal tokens)

Web server
(e.g., IIS)

User login

Impersonated

Single sign on or User login

AGOL via OAuth

AGS service AGOL item via

Secured app with tokens stored

Browser-based Authentication via

Web app

Mobile app

Identity Mgr

IWA

PKI

In the Code

In a Proxy
Identity Manager

• Why should I use it?
  - Handles all login and token processing
  - Works with default token security model AGS & AGOL
  - Available in all Web API’s & viewer apps

• What should I watch out for?
  - Only works for token secured services
  - Prompts multiple times rather than ignoring services
Use case: Impersonation

How service URLs authenticate

Application
(server & portal tokens)

User login
AGOL via OAuth
AGS service AGOL item via

Impersonated
Secured app with tokens stored
In the Code
In a Proxy

Web server (e.g., IIS)

Single sign on or User login

Browser-based Authentication via
Web app
Mobile app
Identity Mgr

IWA
PKI
Impersonation: Embedded credentials

• To be completed…
  - To be completed…
Use case: Integrated Windows Authentication

How service URLs authenticate

Application
(server & portal tokens)

User login

AGOL via OAuth

AGS service AGOL item via

Impersonated

Secured app with tokens stored

Web server (e.g., IIS)

Single sign on or User login

Browser-based Authentication via

IWA

PKI

Web app

Mobile app

Identity Mgr

In the Code

In a Proxy
Integrated Windows Authentication (IWA)

• To be completed…
  - To be completed…
Use case: PKI

How service URLs authenticate

Application (server & portal tokens)

User login

AGOL via OAuth

AGS service AGOL item via

Impersonated

Secured app with tokens stored

Web server (e.g., IIS)

Browser-based Authentication via

Single sign on or User login

In the Code

In a Proxy

IWA

PKI

Web app

Mobile app

Identity Mgr

Application Level
PKI

• To be completed…
  - To be completed…
Implementing OAuth-based apps

Industry standard enterprise logins
Use case: OAuth

How service URLs authenticate

Application (server & portal tokens)

User login

Web server (e.g., IIS)

Single sign on or User login

Application Level

Impersonated

Web app

Mobile app

Identity Mgr

In the Code

In a Proxy

IWA

PKI

AGOL via OAuth

AGS service

AGOL item via

Secured app with tokens stored

Browser-based Authentication via
OAuth implementation details

• To be completed…
  - To be completed…
Thank you…

Please fill out the session evaluation

First Offering ID: 1421

Online – www.esri.com/ucsessionsurveys

Paper – pick up and put in drop box
Esri UC2013 . Technical Workshop . Building Secure Applications