Esri International User Conference | San Diego, CA
Technical Workshops | July 14, 2011

Protecting Your Maps and Data when using ArcGIS Server

David Cordes

Agenda

- Stopping Data Theft
- Stopping Unauthorized Use
- Q&A

Stopping Data Theft

What is Data Theft?

Data Theft

- Either a violation of law (personal information)
- A violation of a license

- Can be *your* data or someone else's
  - Need to protect vendor data

What types of data theft occur?

Violation of re-distribution clause for

- Features
- Cache tiles

What can you do about it?

- Prevention
  - Communicate your policy and license
  - Service security
  - Cache security
  - Throw in subtle errors for theft identification
  - Keep query limit
  - Monitor web server requests
    - Look for excessive hits from a user, domain, or ip

- Responding
  - Communicate – many apparent thefts are just mistakes
  - Block ip or domains at router or web server level
  - Remove account access to secured services

Stopping Unauthorized Use

What is unauthorized use?

- Unauthorized use is any violation of law or license
- Most common examples:
  - Deleting data
  - Service being accessed by unauthorized client
  - Manager exposed to Internet
  - Opening up “services directory” to cross-site scripting attack
  - People can “sniff” my data

What can I do about data deletion?

- Every feature service with the edit capability should be secured.

Unauthorized client

- Use long-term token combined with monitoring
- Monitor and change

Manager Exposed to Internet

- Normally administration actions through DCOM, blocked by firewalls
- Manager secured by username/password
    - Could be subject to brute force attack
    - Java Manager on port 8399, usually safe
        - Can be turned off
    - .Net Manager, usually installed on port 80 (same as services)
        - Instead don’t install Manager on default instance
        - Run AddInstance.exe to add Manager to second instance
        - http://bit.ly/nj69gP

Services Directory Cross-Site Scripting

- Upgrade to 10 SP2
- Turn off services directory when exposed to Internet.
- Help for Java and .Net here: http://bit.ly/ngX0BD

Data Sniffing

- Make your folders encrypted in Manager
- Will require https and won’t allow http requests
- If you don’t check encrypted people can accidentally use http
- Doc: http://bit.ly/pzflyc

Evaluations

- **http://www.esri.com/sessionevals**

Q&A