Designing an Enterprise GIS Security Strategy
Michael E. Young
Agenda

- Introduction
- Trends
- Strategy
- Mechanisms
- Server
- Mobile
- Cloud
- Compliance
Introduction

What is a secure GIS?
Introduction
What is “The” Answer?

Risk

Vulnerability

Impact

Threat
Introduction
Where Are the Vulnerabilities?

* SANS Relative Vulnerabilities
Trends
**Trends**

Application Level Vulnerabilities – Really?

* Kaspersky Labs 2012: Why complexity is IT security’s worst enemy
Trends

Game changed

- Understand the security game has changed
  - Risks are continuous and evolving
  - All controls can be circumvented individually

- Initial response by most organizations
  - Add more security controls as quickly as possible
  - Drives complexity
Trends
Complexity Issues

• Complex security control consequences
  - More time to effect change
  - Higher security costs
  - Lower return on security investment

* Kaspersky Labs 2012: Why complexity is IT security’s worst enemy
Trends
Result of complexity / expanding issues

• Claims of basic security models failing
  - Defense-In-Depth (DiD)

• Reality – Either the organization did not
  - Implement DiD
    - Or
  - Add/integrate/consolidate controls strategically
Trends

Most worrisome 3rd party application cyber attacks

* SC – In the crosshairs (2013)
Trends

Pop Quiz

- Question:
  - Of 47,000+ security incidents analyzed in a 2013 report* what % of cases involved data **transit** vs. at rest or while being processed?

- Answer (Choose 1):
  - 67 % - At rest (DB / File Services)
  - 33 % - While being processed
  - 0 % - While data was in transit

- Question – Part 2
  - Which item above does HTTPS / SSL protect?

- Answer
  - Data in transit


Do your security strategy efforts reflect this?
Trends

Mobile

Android threats accelerate

In Australia and the U.S., Sophos is now reporting Android threat exposure rates exceeding those of PCs.

Android Threat Exposure Rate

- Android TER
- PC TER

Threat exposure rate (TER): Measured as the percentage of PCs and Android devices that experienced a malware attack, whether successful or failed, over a three month period.

*Sophos Security Threat Report 2013
## Trends
### Profiling threat actors

<table>
<thead>
<tr>
<th>Victim Industry</th>
<th>Organized Crime</th>
<th>State-Affiliated</th>
<th>Activists</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerospace</td>
<td>Finance</td>
<td>Manufacturing</td>
<td>Information</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Retail</td>
<td>Professional</td>
<td>Public</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Food</td>
<td>Transportation</td>
<td>Other Services</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Eastern Europe</td>
<td>East Asia (China)</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>North America</td>
<td>Western Europe</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td></td>
<td>North America</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Common Actions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Tampering (Physical)</td>
<td>Backdoor (Malware)</td>
<td>SQLi (Hacking)</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Brute force (Hacking)</td>
<td>Phishing (Social)</td>
<td>Stolen creds (Hacking)</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Spyware (Malware)</td>
<td>Command/Control (C2)</td>
<td>Brute force (Hacking)</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Capture stored data (Malware)</td>
<td>Export data (Malware)</td>
<td>RFI (Hacking)</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Adminware (Malware)</td>
<td>Password dumper (Malware)</td>
<td>Backdoor (Malware)</td>
</tr>
<tr>
<td>Aerospace</td>
<td>RAM Scraper (Malware)</td>
<td>Downloader (Malware)</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Targeted Assets</td>
<td>Stolen creds (Hacking)</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>ATM</td>
<td>Web application</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>POS controller</td>
<td>Database</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>POS terminal</td>
<td>Mail server</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Database</td>
<td>Directory server</td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Desktop</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Desired Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aerospace</td>
<td>Payment cards</td>
<td>Credentials</td>
<td>Personal info</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Credentials</td>
<td>Internal organization data</td>
<td>Credentials</td>
</tr>
<tr>
<td>Aerospace</td>
<td>Bank account info</td>
<td>Trade secrets</td>
<td>Internal organization data</td>
</tr>
<tr>
<td>Aerospace</td>
<td></td>
<td>System info</td>
<td></td>
</tr>
</tbody>
</table>
Strategy
Strategy
A better answer

• Identify your Security Needs
  - Assess your environment
    - Datasets, Systems, Users
    - Sensitivity, Categorization
    - Understand attacker motivation

• Understand Security Options
  - ArcGIS for Professionals site
  - Enterprise-wide Security Mechanisms
  - Application Specific Options

• Implement Security as Business Enabler
  - Improve appropriate availability of information
  - Make attackers job more difficult, not your employee’s job
Strategy
Enterprise GIS Security Strategy

Security Risk Management Process Diagram - Microsoft
Strategy
Esri’s Security Strategy Evolution

Product

- Isolated Systems
- 3rd Party Security

Enterprise

- Integrated Systems
- Embedded Security

Platform

- Cloud
- Managed Security
Strategy
Esri Products and Solutions

• Secure Products
  - Trusted geospatial services
  - Individual to organizations
  - 3rd party assessments

• Secure Enterprise Guidance
  - ArcGIS for Professionals site
  - Online Help

• Secure Platform Management
  - SaaS Functions & Controls
  - ArcGIS Online Security Overview
  - Certifications / Accreditations
Strategy

Security Principles

• CIA Security Triad

• Defense in Depth
Strategy
Defense in Depth

- More layers does NOT guarantee more security
- Understand how layers/technologies integrate
- Simplify
- Balance People, Technology, and Operations
Mechanisms
Mechanisms

- Authentication
- Authorization
- Filters
- Encryption
- Logging/Auditing
Mechanisms

Authentication

• GIS Tier (Default)
  - Built-in User store
  - Enterprise (AD / LDAP)
  - ArcGIS Tokens

• Web Tier (Add web adaptor)
  - Enterprise (AD / LDAP)
  - Any authentication supported by web server
    - HTTP Basic / Digest
    - PKI
    - Windows Integrated
Mechanisms
Authorization – Role Based Access Control

• **Esri COTS**
  - Assign access with ArcGIS Manager
  - Service Level Authorization across web interfaces
  - Services grouped in folders utilizing inheritance

• **3rd Party**
  - Web Services – Conterra’s Security Manager (more granular)
  - RDBMS – Row Level or Feature Class Level
    - Versioning with Row Level degrades RDBM performance
    - Alternative - SDE Views

• **Custom - Limit GUI**
  - Rich Clients via ArcObjects
  - Web Applications
    - Sample code Links in ERC
    - Microsoft’s AzMan tool
Mechanisms
Filters – 3rd Party Options

• Firewalls
• Reverse Proxy
• Web Application Firewall
  - Open Source option ModSecurity
• Anti-Virus Software
• Intrusion Detection / Prevention Systems
• Limit applications able to access geodatabase
Mechanisms
Filters – WAF

- High availability ArcGIS infrastructure
- Traffic filtered before accessed by web servers
- Internal users
  - Access GIS servers via port 6080 directly
- If need more encryption
  - Configure SSL across backend systems
- If want no web tier
  - Loadbalancer can hit GIS Servers directly
Mechanisms

Encryption – 3rd Party Options

• Network
  - IPSec (VPN, Internal Systems)
  - SSL (Internal and External System)
  - Cloud Encryption Gateways
    - Only encrypted datasets sent to cloud

• File Based
  - Operating System – BitLocker
  - GeoSpatially enabled PDF’s combined with Certificates
  - Hardware (Disk)

• RDBMS
  - Transparent Data Encryption
  - Low Cost Portable Solution - SQL Express 2012 w/TDE
Mechanisms
Logging/Auditing

• **Esri COTS**
  - Geodatabase history
    - May be utilized for tracking changes
  - ArcGIS Workflow Manager
    - Track Feature based activities
  - ArcGIS Server 10+ Logging
    - “User” tag tracks user requests

• **3rd Party**
  - Web Server, RDBMS, OS, Firewall
  - Consolidate with a SIEM

**Question**: Any geospatial service monitors?
- Vestra’s GeoSystems Monitor
- Geocortex Optimizer
Mechanisms
Logging/Auditing

• Vestra GeoSystems Monitor
  - ArcGIS Platform access and availability awareness
  - New - User consumption metrics
    - SDE Table/Feature class (Who & Frequency)
    - ArcGIS Server Services & Apps (Who & Action)
ArcGIS Server
ArcGIS Server
Public Facing Architecture

HTTP(s)
WEB
Reverse Proxy

HTTP(s)
WEB
WAF
Web Adaptor

HTTP(s)
DCOM
SOM
SOC
DBclient

HTTP(s)
SQL
SvrDir
DBMS

HTTP(s)
SQL
SvrDir
DBMS

Public
DMZ
Private

10
10.1 & 10.2

ArcGIS Server
Enterprise Deployment

Supporting Infrastructure
- AD/ LDAP
- Clustered HA DB1
- Clustered HA DB2
- SQL

ArcGIS Site
- GIS Server A
  - Port: 6080
  - GIS Services
  - Web Adaptor
  - ArcGIS for Server
- GIS Server B
  - Port: 6080
  - GIS Services
  - Web Adaptor
  - ArcGIS for Server

ArcGIS Site
WAF, SSL Accel
Load Balancer
- Port: 80
- IIS/Java Web Server
- Web Adaptor
- Web Apps

Internet
- 443
- Firewall

Network Load Balancing
- Port: 80
- Port: 6080
- Web Adaptor
- Round-Robin

Server Request Load Balancing
- GIS Server A
- GIS Server B

Supporting Infrastructure
- HA NAS
  - Config Store
  - Directories
  - FGDB

Clustering
- HA NAS
ArcGIS Server
Minimize Attack Surface

- Don’t expose Server Manager to public
- Disable Services Directory
- Disable Service Query Operation (as feasible)
- Enable Web Service Request Filtering
  - Windows 2008 R2+ Request Filtering
  - XML Security Gateway
  - Does not intercept POST requests
  - REST API only requires GET and HEAD verbs
    - Exception – Utilize POST for token requests
- Limit utilization of commercial databases under website
  - File GeoDatabase can be a useful intermediary
- Require authentication to services
ArcGIS Server
10.2 Enhancements

• Single-Sign-On (SSO) for Windows Integrated Authentication
  - Works across ArcGIS for Server, Portal, and Desktop

• Stronger PKI validation
  - Leverage multi-factor authentication when accessing applications, computers, and devices
  - Web adaptor deployed to web server forwards to AGS the request and username

• Integrated account management and publishing capabilities
  - Across ArcGIS for Server and Portal in a federated configuration

• Key SQL Injection vulnerabilities addressed
  - Changes made in 10.2 may affect some advanced users that were using database-specific SQL statements in their custom applications

• Add support for
  - Active Directory nested groups & domain forests
  - Configuring Private and Public services within the same ArcGIS Server site
Mobile
Mobile
What are the mobile concerns?

- M1 - Insecure Data Storage
- M2 - Weak Server Side Controls
- M3 - Insufficient Transport Layer Protection
- M4 - Client Side Injection
- M5 - Poor Authorization and Authentication
- M6 - Improper Session Handling
- M7 - Security Decisions Via Untrusted Inputs
- M8 - Side Channel Data Leakage
- M9 - Broken Cryptography
- M10 - Sensitive Information Disclosure
Mobile
Security Touch Points

- SDE permissions
- Server authentication
- Service authorization

Communication

- Device access
- Storage
- Project access
- Data access

Designing an Enterprise GIS Security Strategy
Mobile

Authenticating to ArcGIS Services

- **GIS Tier Auth - ArcGIS Tokens**
  - Pass credentials through UserCredentials / AGSCredential object
  - Hardcode long-term token into layout XML (Ideally avoid)

- **Web Tier Auth – HTTP Basic/Digest**
  - Pass credentials through UserCredentials object
  - PKI Support 10.1.1
    - Android OS version dependent
    - Not available on Windows phone yet

- **SSL Support**
  - Certificates issued by trusted cert authority
  - Self-signed certificates (Dev environment)
Mobile

Enterprise Mobile Security

• Built-in device capabilities
  - Can store features iOS5 encrypted with Flex 3.0 API

• Enterprise device solutions (InTune, AirWatch, Good, MaaS360)
  - Benefits: Secure email, browser, remote wipe, app distribution

• Application specific solutions
  - Benefits: Secure connections and offline device data
  - Esri iOS SDK + Security SDK
Cloud
Cloud
Service Models

• Non-Cloud
  - Traditional systems infrastructure deployment
  - Portal for ArcGIS & ArcGIS Server

• IaaS
  - Portal for ArcGIS & ArcGIS Server
  - Some Citrix / Desktop

• SaaS
  - ArcGIS Online
  - Business Analyst Online
Cloud Deployment Models

- Public
- Hybrid 1
- Hybrid 2
- On-Premises
- On-Premises +

Cloud On-premise

Public

Intranet

Online

Server

Portal

Read-only Basemaps

Intranet

On-premise

Designing an Enterprise GIS Security Strategy
Cloud
Management Models

• **Self-Managed**
  - Your responsibility for managing IaaS deployment security
  - Security measures discussed later

• **Esri Managed**
  - Managed Services
  - Starting work on FedRAMP compliant environment capabilities
Cloud
Model relationships

Service Model
- Non-Cloud
  - AGS Your Location

Deployment Model
- On-Premises
  - Your location

Management Model
- Self Managed
  - You

Cloud
- AGS in AWS
  - Community
    - Your Loc+AWS
  - Hybrid
    - Managed
      - Esri
  - Public
    - AWS/Azure

AWS is a placeholder on this slide for any cloud provider such as Azure, CGI, or Terremark.
Cloud
Real Permutations

Private IaaS

Internal AGS
Internal Portal
Filtered Content
External AGS

Database
File Geodatabase

Enterprise Business

ArcGIS Online
Public

Field Worker

Business Partner 1

Business Partner 2
Designing an Enterprise GIS Security Strategy

1. Register Services
2. Enterprise Login (SAML 2.0)
3. Request to View
4. Access Service

On-Premises ArcGIS Server
User Repository
AD / LDAP

AGOL Org
Group “TeamGreen”

Hosted Services, Content
Public Dataset Storage
ArcGIS Org Accounts
External Accounts

Users

Segment sensitive data internally and public data in cloud
Cloud
Hybrid – Data sources

- 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 SSL 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
Cloud
On-premises

• Why?
  - Additional security demands
  - Federated account management needs between ArcGIS Server and Portal
    - Registered services *(managed and secured via Server)*
    - Federated services *(managed via Server, secured via Portal)*
    - Hosted services *(managed and secured via Portal)*

• Requires
  - Infrastructure
  - Portal & System Administration
Cloud
Data Locations

On-premises
ArcGIS Server
Typically utilized for sensitive data & services

Cloud Provider
ArcGIS Server
Commonly utilized to reduce management costs

ArcGIS Online
Feature Services
Commonly utilized for mildly sensitive information and public data/services
Cloud
ArcGIS Online – Standards

• New Enterprise Logins
  - SAML 2.0
  - Provides federated identity management
  - Integrate with your enterprise LDAP / AD

• New API’s to Manage users & app logins
  - Developers can utilize OAuth 2-based API’s
Cloud
ArcGIS Online - Settings

- Organization administrator options
  - Require SSL encryption
  - Allow anonymous access to org site

- Consume Token secured ArcGIS Server services
  - 10 SP1 and later
  - User name and password prompts upon adding the service to a map, and viewing

- Transparency
  - Status.ArcGIS.com
Cloud

IaaS

• Common ArcGIS IaaS Deployments
  - ArcGIS Server Windows AMI to AWS
  - ArcGIS Server via Cloud Builder to AWS

• ArcGIS AWS Security Best Practices
  - 8 main areas
  - 5 minute minimum
Cloud
IaaS – AWS

- 8 Security Areas to Address
  - Virtual Private Cloud (VPC)
  - Identity & Access Management (IAM)
  - Administrator gateway instance(s) (Bastion)
  - Reduce attack surface (Hardening)
  - Security Information Event Management (SIEM)
  - Patch management (SCCM)
  - Centralized authentication/authorization
  - Web application firewall (WAF)
Cloud
IaaS - AWS

• Question
  - What is the most common mechanism utilized to compromise AWS instances running Windows?

• Answer
  - Remote Desktop Protocol (RDP)

• Question – Part 2
  - Is the problem typically with the RDP protocol or configuration?

• Answer
  - Configuration.
  - Specifically entering 0.0.0.0 for RDP security group allowing all Internet users to attempt access
Cloud
IaaS – AWS – 5 minute minimum

1. Minimize RDP surface
   - Update OS patches
   - Many AMI’s disable automatic updates
   - Enable NLA for RDP
   - Set AWS Firewall to Limit RDP access to specific IP’s

2. Minimize Application Surface
   - Disable ArcGIS Services Discovery
   - Don’t expose ArcGIS Manager web app to Internet

These steps can be completed within 5 minutes – Do them!
Compliance
Compliance
ArcGIS Online

• In-Place Now
  - Safe Harbor Self-Certification
  - TRUSTed Cloud Certified

• Expected in 2013
  - FISMA Low Accreditation

• Future
  - FedRAMP Moderate
Compliance
Beyond ArcGIS Online

- **FDCC**
  - Desktop products 9.3-10

- **USGCB**
  - Desktop products 10.1

- **SSAE 16 Type 1 – Previously SAS 70**
  - Esri Data Center Operations
  - Expanded to Managed Services in 2012
Summary
Summary

• Security is NOT about just a technology
  - Understand your organizations GIS risk level
  - Realize the game has changed and prioritize efforts accordingly
  - Don’t just add components, simplify!

• Secure Best Practice Guidance is Available
  - Check out the ArcGIS for Professionals site!
  - Drill into details by mechanism or application
  - Look for ArcGIS Online Cloud Security Alliance security control documentation soon
Summary
UC 2013 Security Sessions

ArcGIS Online
- Security and ArcGIS Online
- Building Secure Applications

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

ArcGIS Platform
- Designing an Enterprise GIS Security Strategy
Thank you…

Please fill out the session evaluation

**Offering ID:** 1379

**Online** – www.esri.com/ucsessionsurveys

**Paper** – pick up and put in drop box
Questions?

Trends
Strategy
Mechanisms
Server
Mobile
Cloud
Compliance

Offering ID: 1379