Designing an Enterprise GIS Security Strategy

Michael Young
Randall Williams
Esri Software Security & Privacy Team

SEE WHAT OTHERS CAN'T

Agenda

- Introduction
- Trends
- Strategy
- Mechanisms
- Web GIS
- Mobile
- Cloud
- Compliance

Introduction

Software Security & Privacy Team

- **Who?**
  - **CISO – Products**
  - **Security Architects**
  - **Security Engineers**

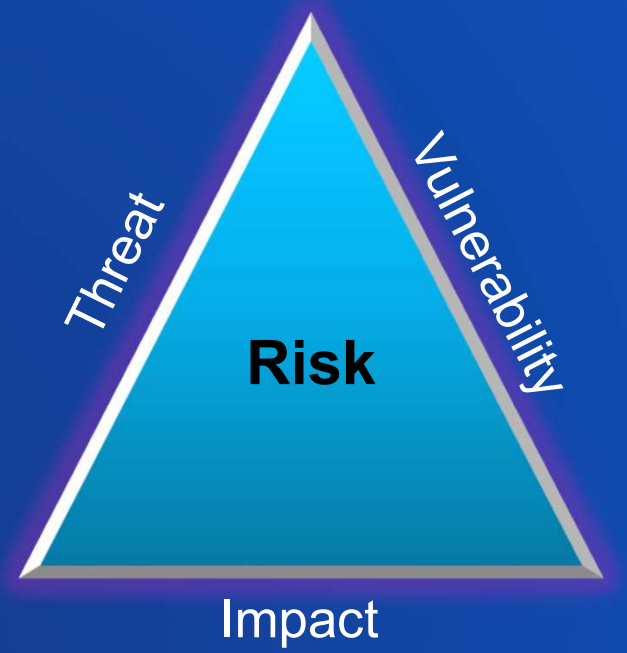
- **Goals**
  - **Coordinate product security incidents / vulnerabilities**
  - **Empower development teams with standardized security/privacy tools and methodologies**
  - **Provide guidance and validation to meet evolving customer compliance requirements**

Introduction

What is a secure GIS?

Introduction

What is “The” Answer?



Trends & Real World Scenarios

Michael Young

Trends

2018 Breach numbers

- 25% - Breaches associated with espionage
- 12x - C-level executives more likely social incident target & 9x more social breach target
- 24% - Ransomware used in case (No. 2 ranked malware type)

- Security game continues to evolve and time to breach expedited
  - Primary breach vehicle was mapping network and gaining access over time
  - Now theft of personal information and credentials is primary vehicle
    - Log-in info, social attacks, and pretexting
  - Target remains the same – Intellectual property (IP) and secrets

Verizon DBIR 2019

Trends

Cloud adoption continues to expand

- **Frequently, cloud providers can and do provide robust security**
- **Largest downfall of cloud security continues to be customer configuration of the services**
  - **2019 Verizon DBIR – Customer admin issues lead to more breaches of cloud storage & web apps**
  - **Repeated exposure of publicly editable mapping services**
- **Importance of administration maintenance & security processes can't be emphasized enough**
  - **Do your admin receive adequate training on the services?**
  - **Do you know about tools available to ensure alignment with best practices?**
  - **What governance do you have in place for publishing data?**

How well are you controlling the publication process to external facing services?

Scenario

Imagine your administrators report unusual accounts on your systems

- Your first reaction is to remove the unusual domain accounts
- Ransomware is immediately triggered on all systems demanding bitcoin payment to unlock
- What would you do?
  - Pay? Sometimes it works, sometimes it does not – It encourages the instigator to do more
  - Rebuild your systems? Are your backups good enough?

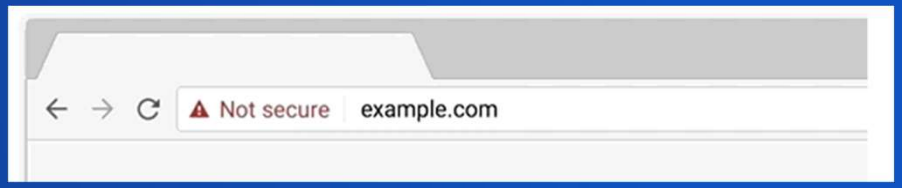
- The organization decided to not pay and has been recovering systems for a little over 1 year now
- Investigators determined nation-state breached environment over a 3 month window
- Once initial breach performed, traversed systems via service accounts

- Lessons learned
  - Ensure your backups are operational
  - For Windows systems utilize Group Managed Service Accounts (gMSA's) for ArcGIS Enterprise
    - New KBA - https://support.esri.com/en/technical-article/000021125

Scenario

ArcGIS Online administrator swamped with user calls stating maps failing to display

- **Widespread disruption of your geospatial services**
- **Users have been complaining about Insecure messages from their browsers when visiting your site for months**

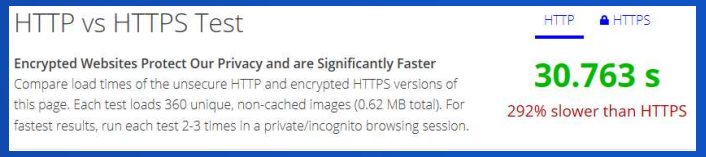


Something changed, but what?

Scenarios

ArcGIS Online Allows Only HTTPS

- In 2020, ArcGIS Online will enforce HTTPS only
- In 2018, browsers like Chrome started flagging sites with HTTP as insecure
  - Nobody will want to consume your maps/apps if you don't correct this
- HTTPS Performance and Cost are Non-issues
  - Let's Encrypt provides free HTTPS certificates
  - Amazon is offering free security certificates to AWS customers
  - Most browsers only support faster HTTP/2 with HTTPS
    - Sites utilizing HTTPS can significantly outperform HTTP sites
    - See for yourself @ http://www.httpvshttps.com/
- Use the new ArcGIS Online Security Advisor HTTP Check tool



The sooner you eliminate HTTP from your systems and the services you consume the better

Trends

Strategic Shifts in Security Priorities for 2019 and Beyond

- HTTP is about to die
  - Migrate away from any HTTP dependences NOW!
- Stronger Privacy regulation driving security demands (GDPR / CCPA)
- Enormous user password dumps now commonplace
  - Use 2-factor auth / enterprise password management solutions
- Mobile security threats increasing quickly
  - Become familiar with vendor mobile app recommendations
- Utilization of named users provides more granular tracking of geospatial information
  - Become familiar with your application logging capabilities
- Customer configuration primary source of cloud breaches
  - Drives importance of admin training & tools/automation for discovery of configuration issues

Strategy

Michael Young

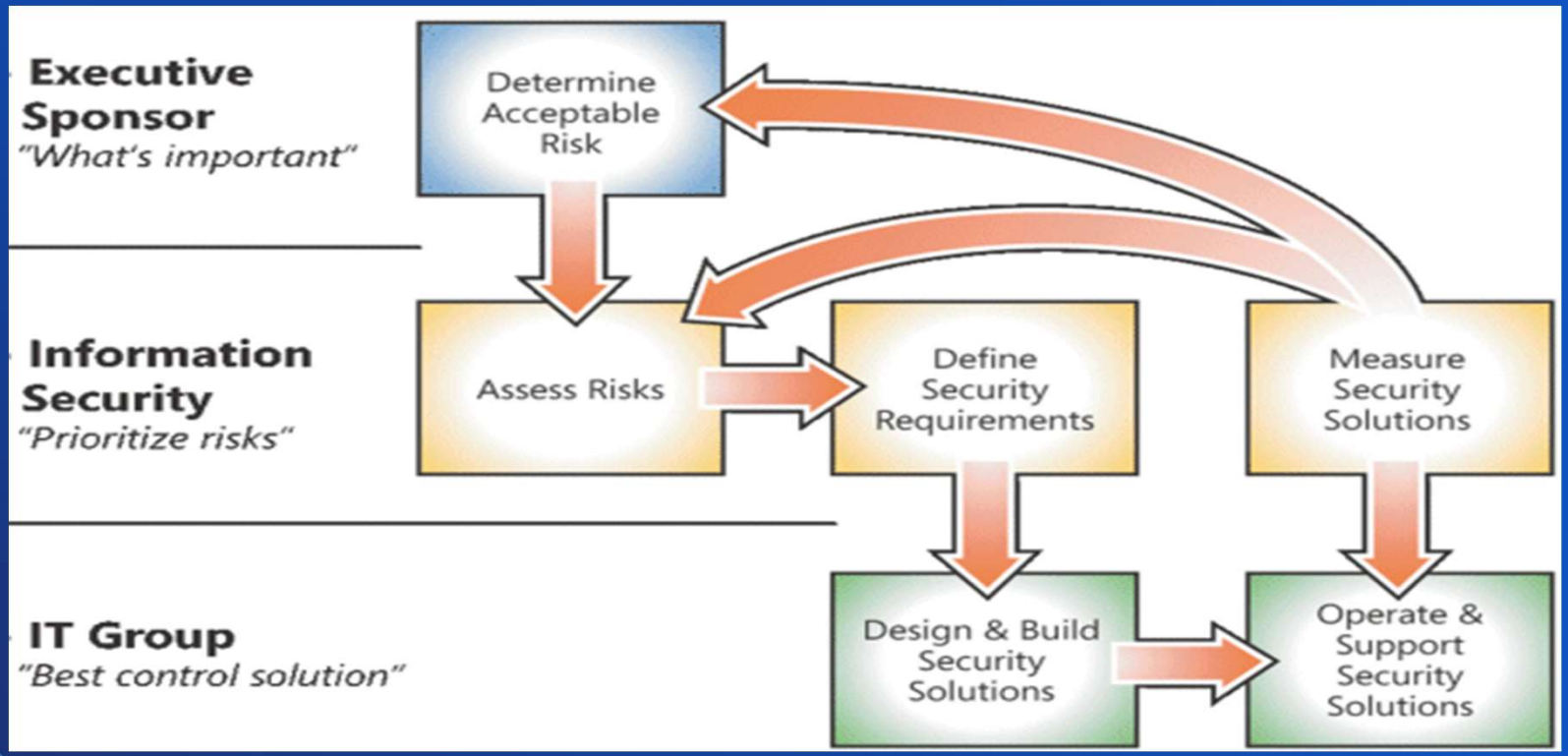
Strategy

A better answer

- Identify your security needs
  - Assess your environment
    - Datasets, systems, users
    - Data categorization and sensitivity
    - Understand your industry attacker motivation
- Understand security options
  - Trust.arcgis.com
  - Enterprise-wide security mechanisms
  - Application specific options
- Implement security as a business enabler
  - Improve appropriate availability of information
  - Safeguards to prevent attackers, not employees

Strategy

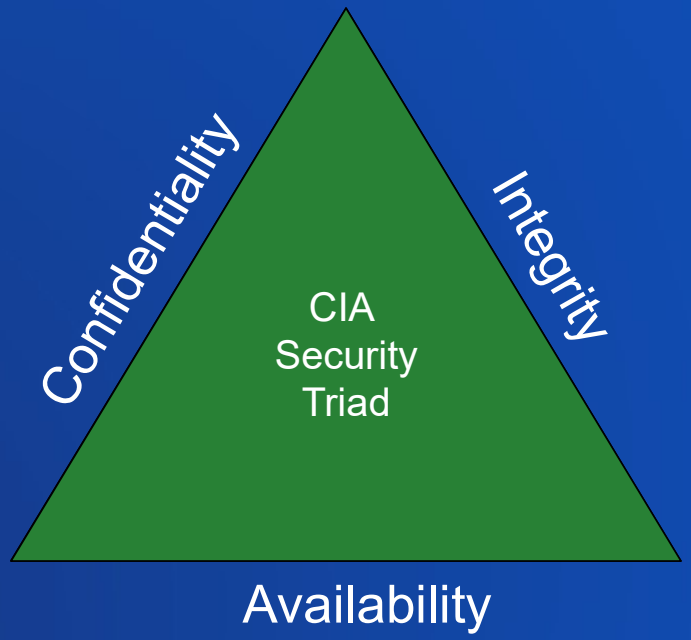
Enterprise GIS Security Strategy



Security Risk Management Process Diagram - Microsoft

Strategy

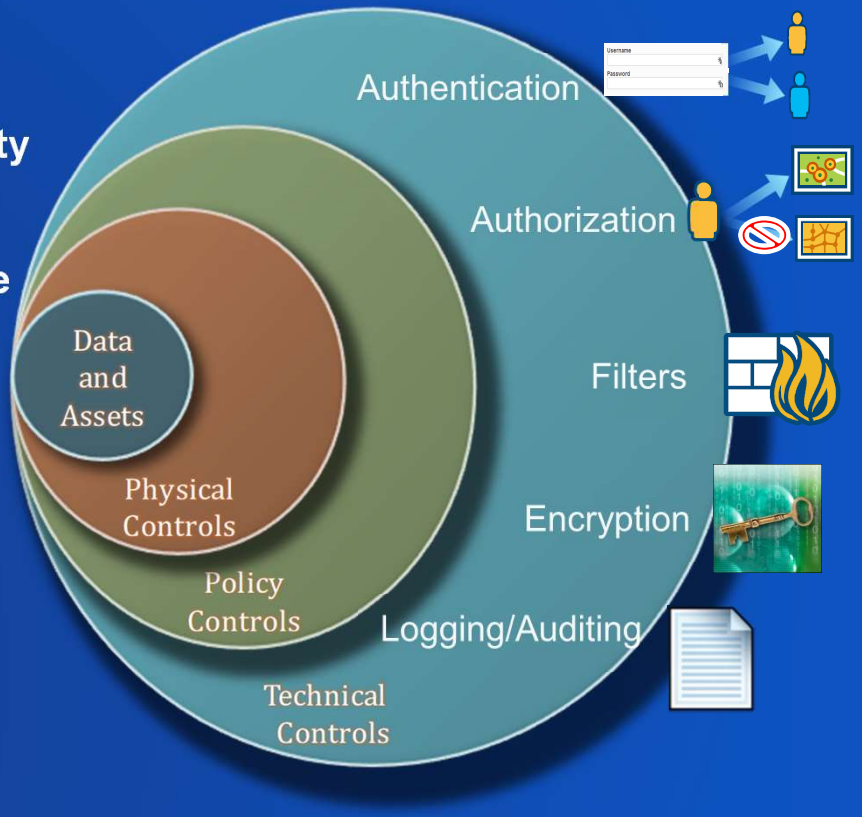
Security Principles



Strategy

Defense in Depth

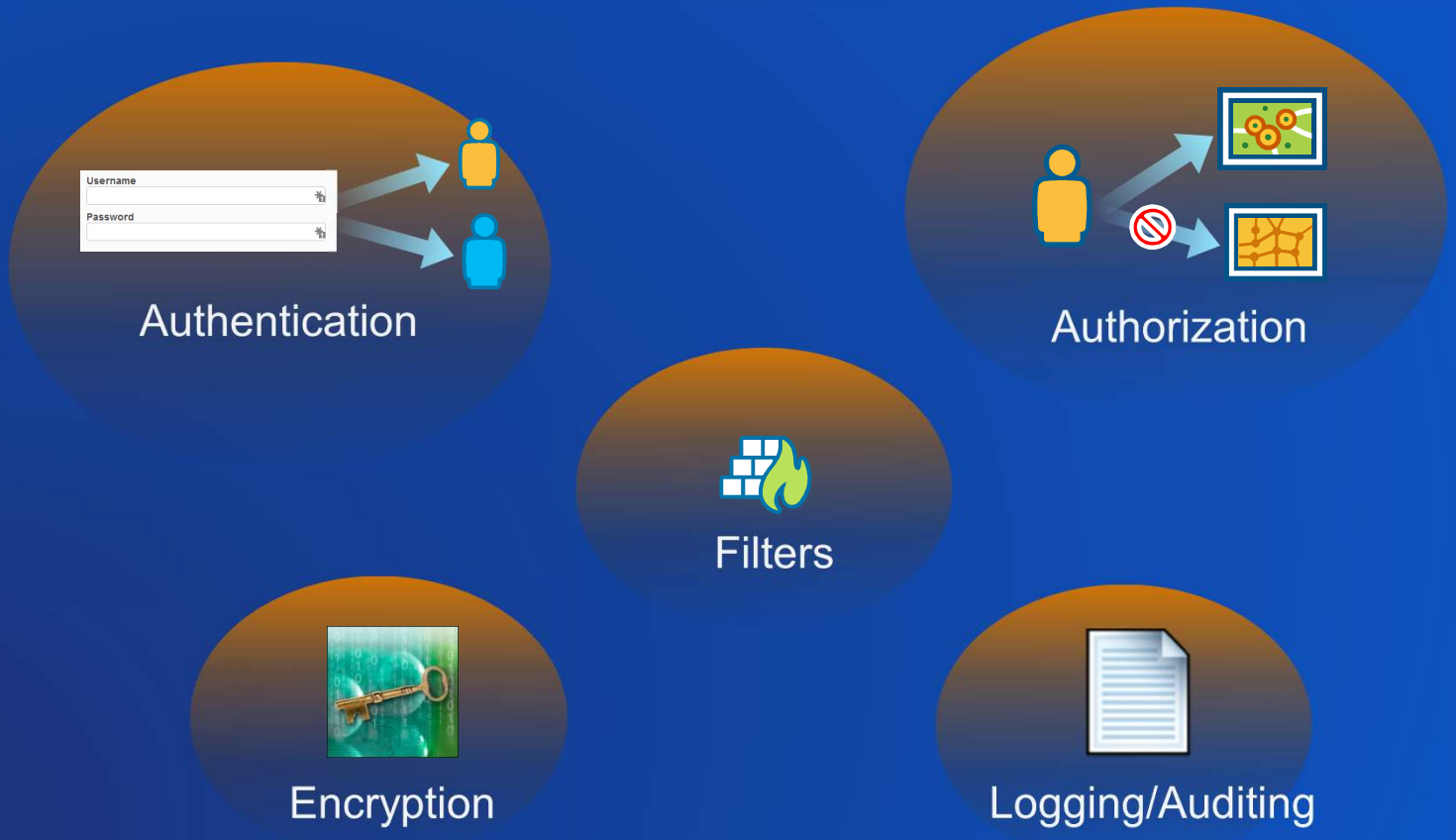
- More layers does NOT guarantee more security
- Understand how layers/technologies integrate
- Simplify
- Balance People, Technology, and Operations
- Holistic approach to security



Mechanisms

Randall Williams

Mechanisms


Username
Password
Authentication
Authorization
Filters
Encryption
Logging/Auditing

Mechanisms - Authentication and Authorization

ArcGIS Token Based Authentication

ArcGIS Token-based Authentication

ArcGIS Online Options

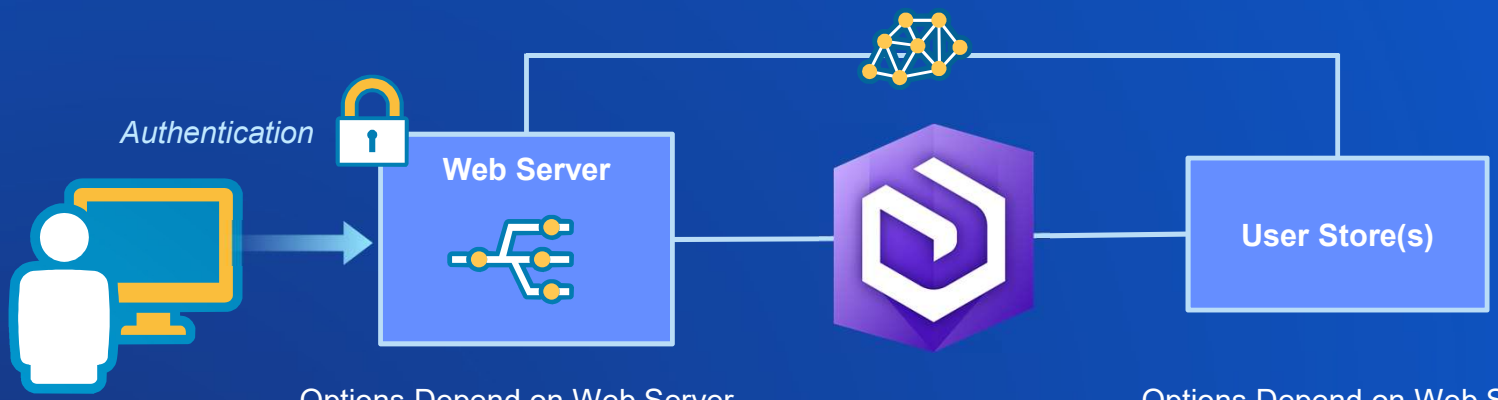
- Built-in User Store

ArcGIS Enterprise Options

- Built-in User Store
- Active Directory
- LDAP

Mechanisms - Authentication and Authorization

Web-Tier Authentication



Options Depend on Web Server…

- Integrated Windows Authentication (IWA)
- Client-Certificate Authentication (PKI)
- HTTP Digest Authentication

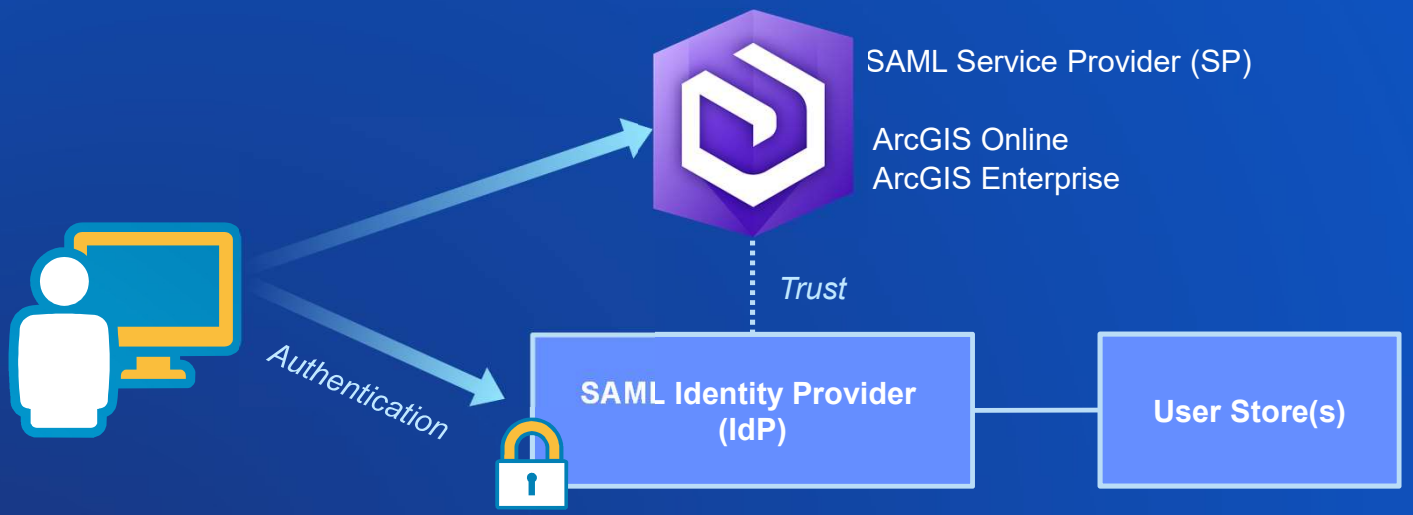
Options Depend on Web Server…

- Active Directory
- LDAP

Only supported using ArcGIS Enterprise…

Mechanisms - Authentication and Authorization

SAML Authentication



Many Options …

- Single or multi-factor authentication
- Client-specific authentication

Many Options …

- Enterprise user store(s)
- One user store or many
- Internal and external users
- …

Provides flexibility and security capabilities depending on IdP…

Mechanisms – Firewalls and Filters

3rd Party Options

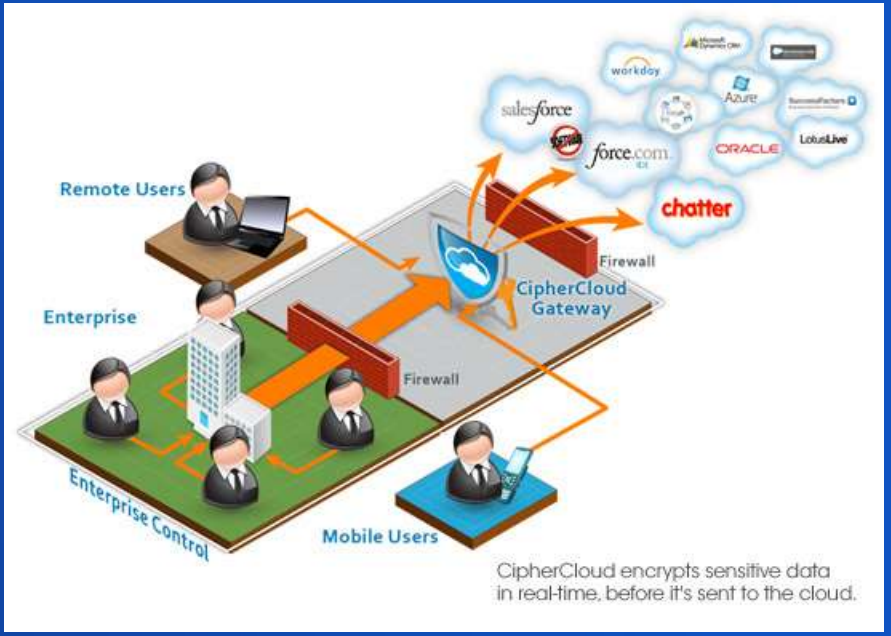
- Firewalls
  - Host-based
  - Network-based
- Reverse Proxy
- Web Application Firewall
  - Open Source option ModSecurity
  - Esri looking into support OWASP WAF Ruleset
- Anti-Virus Software
- Intrusion Detection / Prevention Systems
- Limit applications able to directly access geodatabase

OWASP
ModSecurity
Core Rule Set

Mechanisms - Encryption

3rd Party Options

- **Network**
  - IPSec (VPN, Internal Systems)
  - SSL/TLS (Internal and External System)
  - Cloud Access Security Broker
    - Only encrypted datasets sent to cloud
- **File Based**
  - Operating System – BitLocker
  - GeoSpatially enabled PDF's combined with Certificates
  - Hardware (Disk)
- **RDBMS**
  - Transparent Data Encryption (TDE)



Mechanisms – Logging & Auditing

- **Logging** - Record system events of interest
  - ArcGIS Enterprise Security Log Events summary to be posted to Trust Center
- **Auditing - I**nspect 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

Esri Apps & Capabilities	3rd Party Options
- Geodatabase history	- Web Server & Database
- ArcGIS Workflow Manager	- OS
- ArcGIS Enterprise logging	- Network
- ArcGIS System Monitor	- SIEM (for consolidation)

Web GIS

Randall Williams

Web GIS

ArcGIS Online or Portal?

ArcGIS Online

- SaaS
  - Releases quarterly
  - Upgraded automatically *(by Esri)*
  - Esri controls SLA
- Functionality *(smart mapping, collaboration…)*
- Enterprise Integration
  - Web SSO via SAML
  - Native MFA
- FedRAMP Low Tailored Low Authorized

ArcGIS Enterprise

- Software
  - ArcGIS Server, Portal, Datastore
  - Releases twice per year
  - Upgraded manually *(by organization)*
  - Organization controls SLA
- Functionality *(smart mapping, collaboration…)*
- Enterprise Integration
  - Web SSO via SAML
  - Web-tier Authentication via Web Adaptor
  - Enterprise Groups
  - ArcGIS Server Integration…

Web GIS

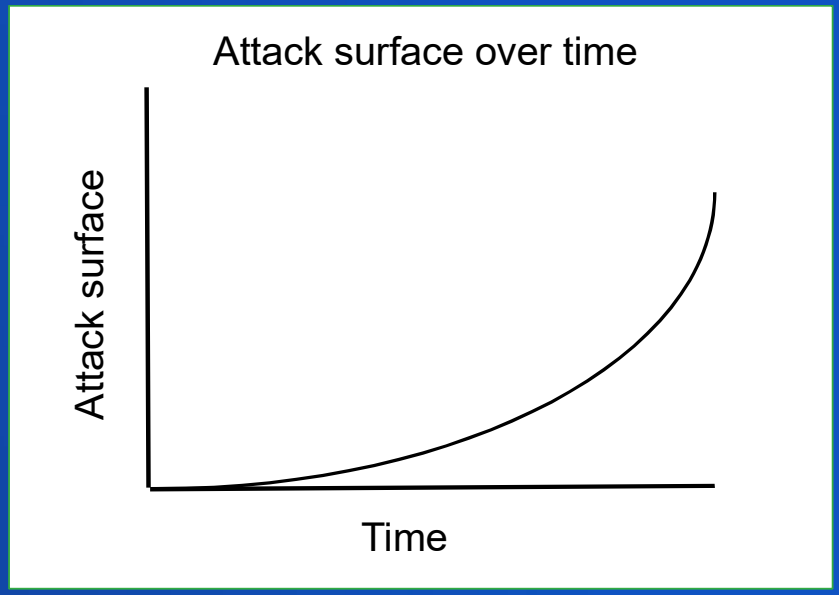
Architecture Options and Security Considerations

- What are the confidentiality and integrity needs of your GIS?
  - Drives extent to which cloud is used
  - Drives potential authentication options used
  - Drives encryption requirements
- What are the availability requirements of your GIS?
  - Redundancy across web tiers, GIS tier, and database tier
- Authentication requirements
  - Leverage centralized authentication (AD/LDAP)
  - For an on premise portal that can be Web-tier authentication or using Enterprise Logins

Web GIS

ArcGIS Enterprise Implementation Guidance

- Don’t expose Server Manager, Server Admin, or Portal Admin interfaces to public
- Disable Services and Sharing Directories
- Disable Service Query Operations (as feasible)
- Limit utilization of commercial databases under website
  - File GeoDatabase can be a useful intermediary
- Require authentication to web services
- Require HTTPS (enabled by default) – enable HSTS
- Restrict cross-domain (CORS) requests
- Restrict Portal Proxy capability
  - Implement a whitelist of trusted domains



Web GIS

ArcGIS Enterprise Recent Enhancements

10.6/10.6.1

- ✓ Distributed collaboration
  - Share content among different Portals and ArcGIS Online
- ✓ Editor tracking for Hosted Feature Services
- ✓ Ownership-based access control for Feature Services records
- ✓ TLS 1.0 disabled OOTB for new installs
- ✓ HSTS support
- ✓ Logging and monitoring improvements
- ✓ Updated JSON content type (helps prevent XSS)
- ✓ Security fixes and enhancements

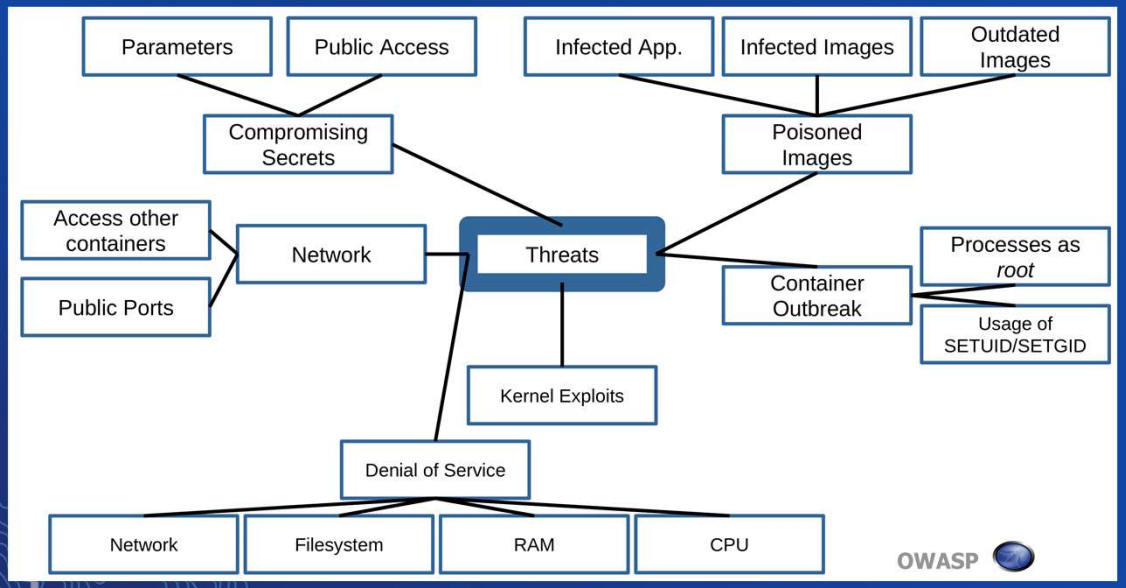
10.7/10.7.1

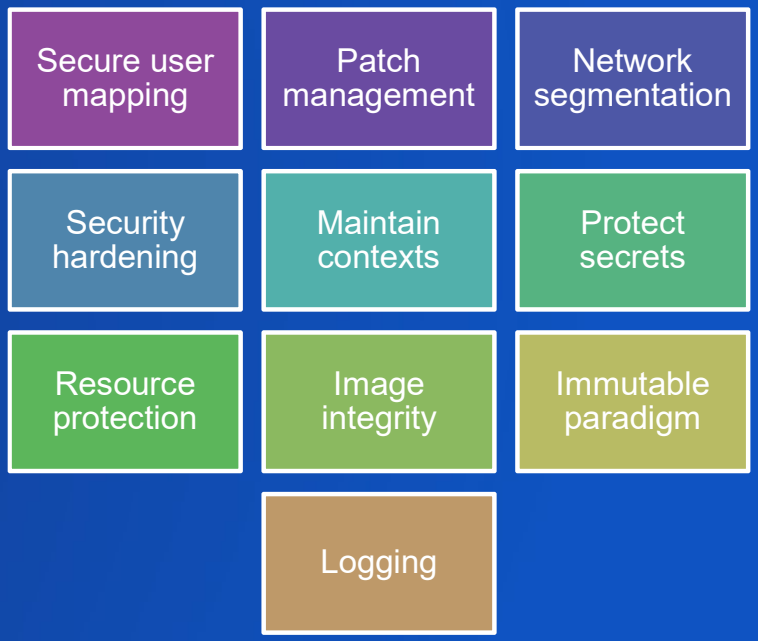
- ✓ Notebook Server
  - Hosted Jupyter Notebooks (containers)
- ✓ Hosted feature layer views
- ✓ Webhooks for administration
- ✓ Shared Instances for Server
- ✓ New Apps
- ✓ HTTPS/TLS1.2 ONLY default
- ✓ Fine Grained admin functions
- ✓ Bulk Publishing
- ✓ Security fixes and enhancements

Web GIS

Containers

- **ArcGIS Notebook Server uses Docker container allocation software**
  - **Container security is mostly about secure system, network and architecture design**
  - **Plan your environment security *before* you start using containerization**
  - **See Docker OWASP Top 10 for further guidance**



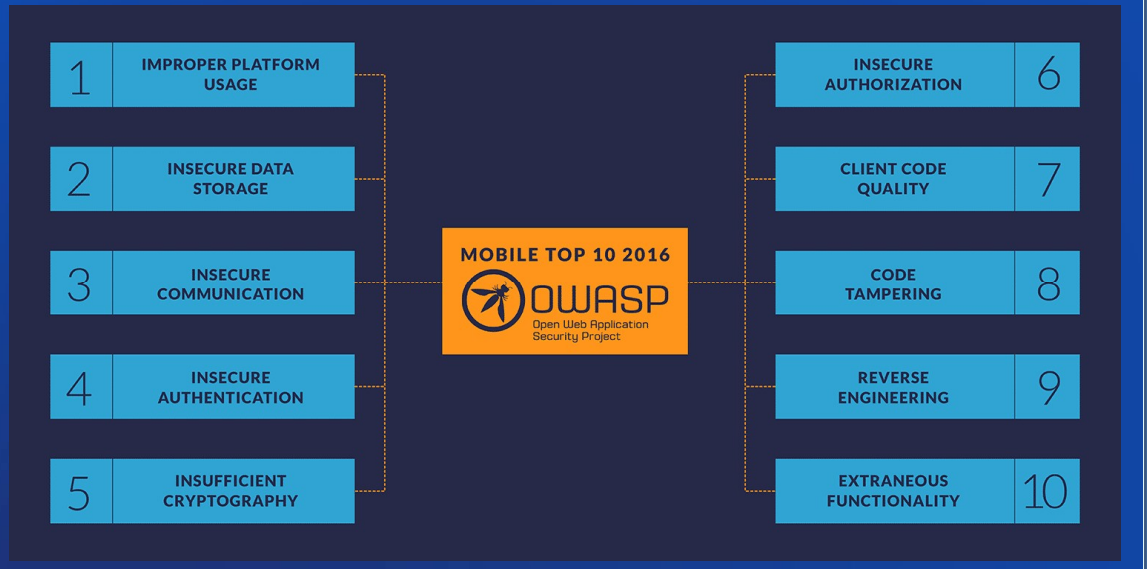


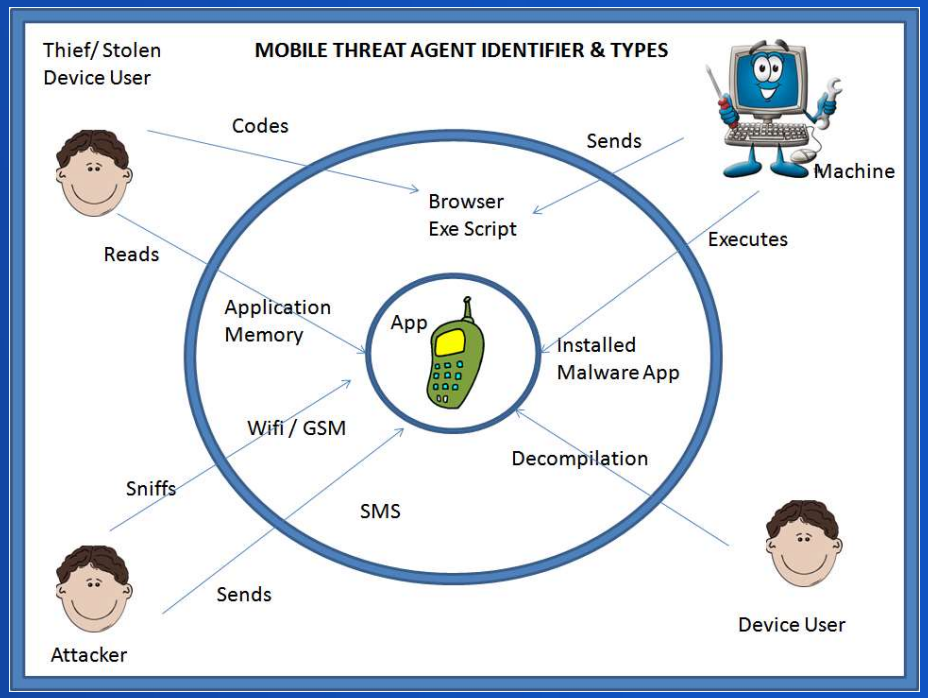
Mobile

Randall Williams

Mobile

What are the mobile concerns?

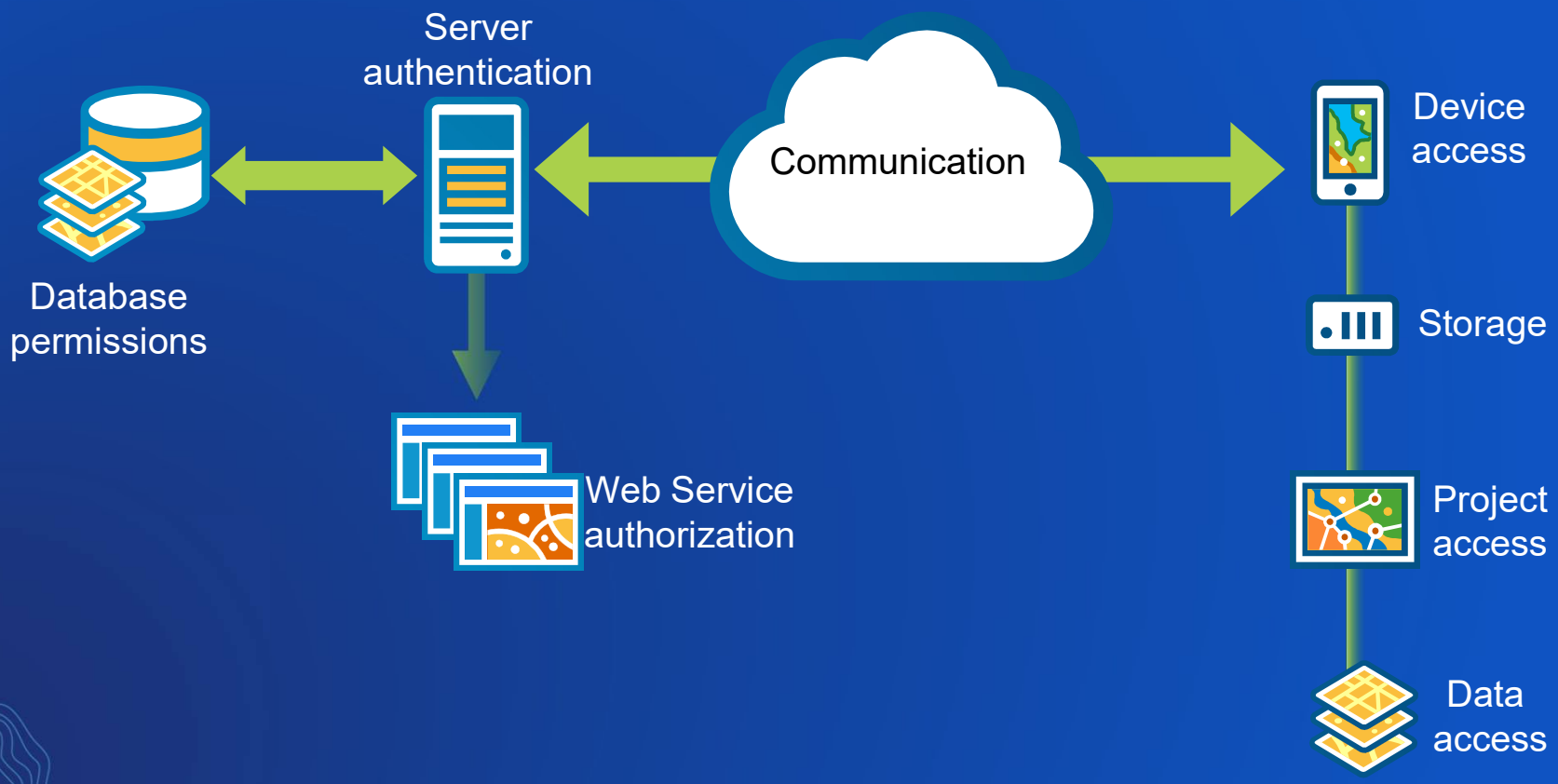




OWASP Top Ten Mobile: https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

Mobile

Security Touch Points



Mobile

Challenges

- Users are beyond corporate firewall
  - To VPN or not to VPN?
- Authentication/Authorization challenges
- Disconnected editing
  - Local copies of data stored on device
- Management of mobile devices
  - Enterprise Mobility Management is the answer!
    - Mobile Device Management
    - Mobile Application Management
    - Security Gateways
    - Examples: MobileIron, MaaS360, Airwatch, and many more…

Mobile

Implementation Guidance

- Encrypt data-in-transit (HTTPS) via TLS 1.2
- Encrypt data-at-rest
- Segmentation
  - Use ArcGIS Online, Cloud, or DMZ systems to disseminate public-level data
- Perform Authentication/Authorization
- Use an Enterprise Mobility Management (EMM) solution
  - Secure e-mail
  - Enforce encryption
  - App distribution
  - Remote wipe
  - Control 3rd party apps & jailbreak detection
  - Distribute Certificates

Mobile

Need More Granularity?

White Paper: ArcGIS Secure Mobile Implementation Patterns

- Replacing redundant inefficient field processes
- Reducing costs and overhead
- Improving collection speed, accuracy, and currency of data
- Modernizing workflows and replacing paper-based workflows
- Helping management make timely and informed decisions

There are two additional mobile apps in the ArcGIS Platform that do not support field data collection workflows, but support other business use cases, (see Figure 5). These apps are mentioned in this document for completeness and are available for both iOS and Android devices. They will follow the same mobile implementation patterns described in later sections of this document. The apps are:

- **ArcGIS Business Analyst**[14]: Enables demographic and socio-economic data in the field
- **AppStudio Player for ArcGIS**: Displays custom apps built with *AppStudio for ArcGIS*[15]

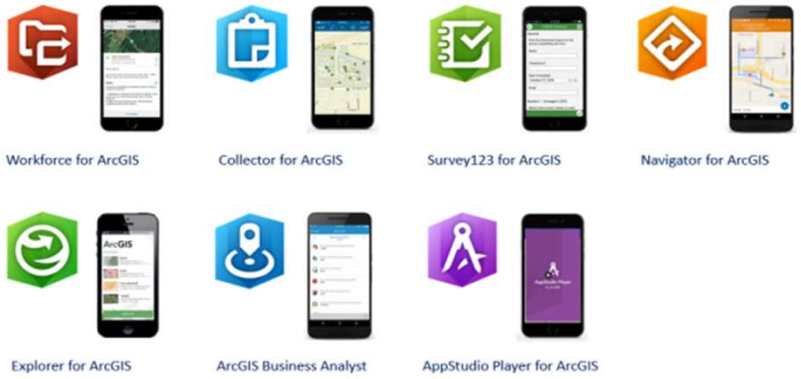


Figure 5: ArcGIS Mobile Apps

All these apps are designed to work with the ArcGIS Platform and support all WAN GIS deployment

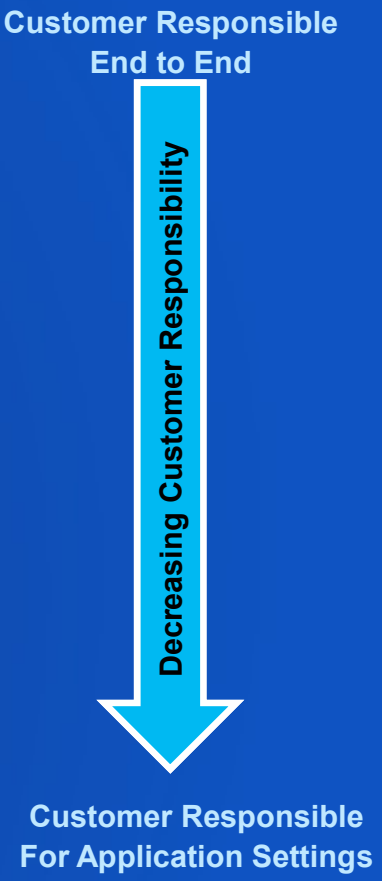
Cloud

Randall Williams

Cloud

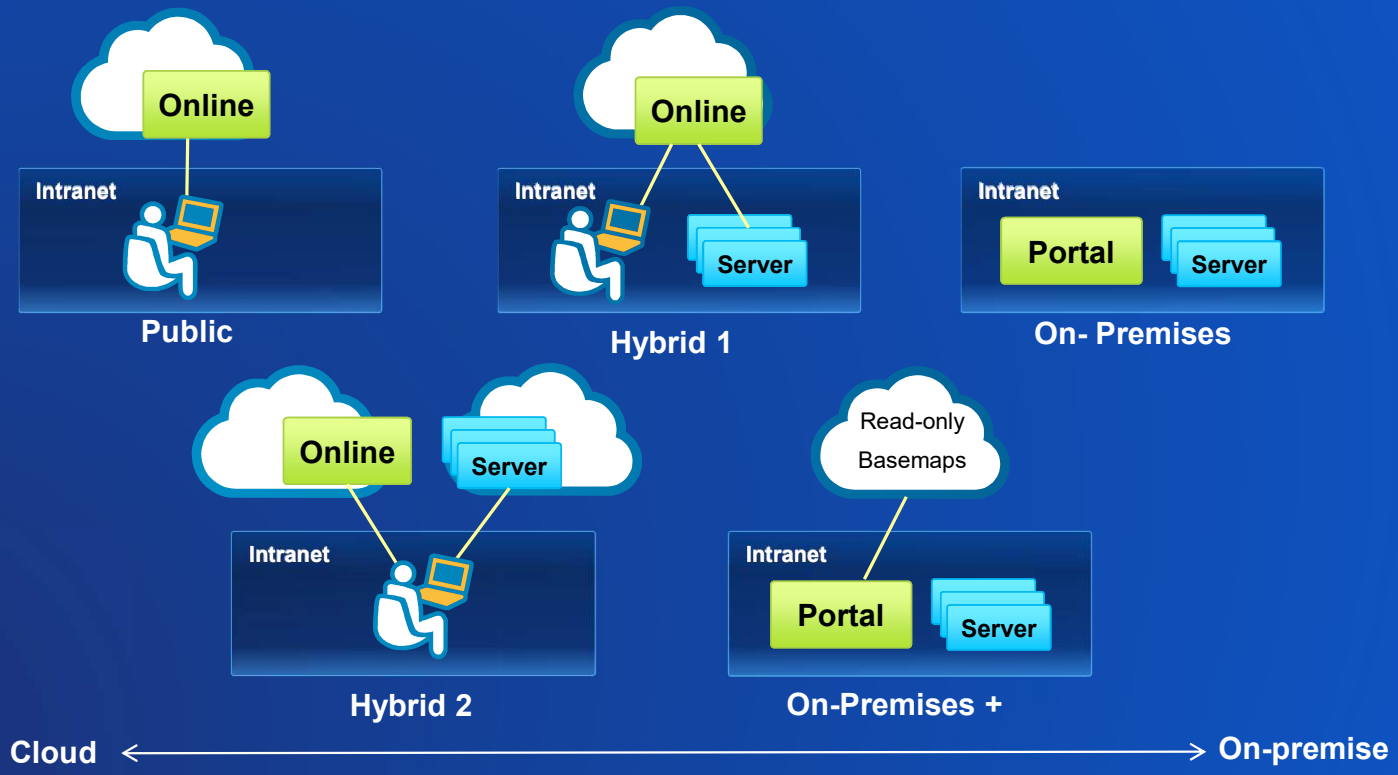
Service Models

- **Non-Cloud: On Premises**
  - Traditional systems infrastructure deployment
  - ArcGIS Enterprise
- **IaaS: Infrastructure as a Service**
  - ArcGIS Enterprise
  - Some Citrix / Desktop
- **SaaS: Software as a Service**
  - ArcGIS Online
  - Business Analyst Online



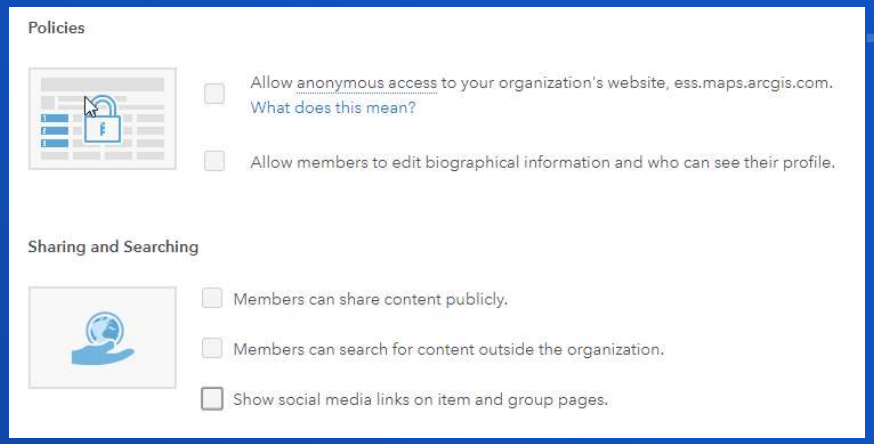
Cloud

Deployment Models



Cloud

ArcGIS Online – Implementation Guidance

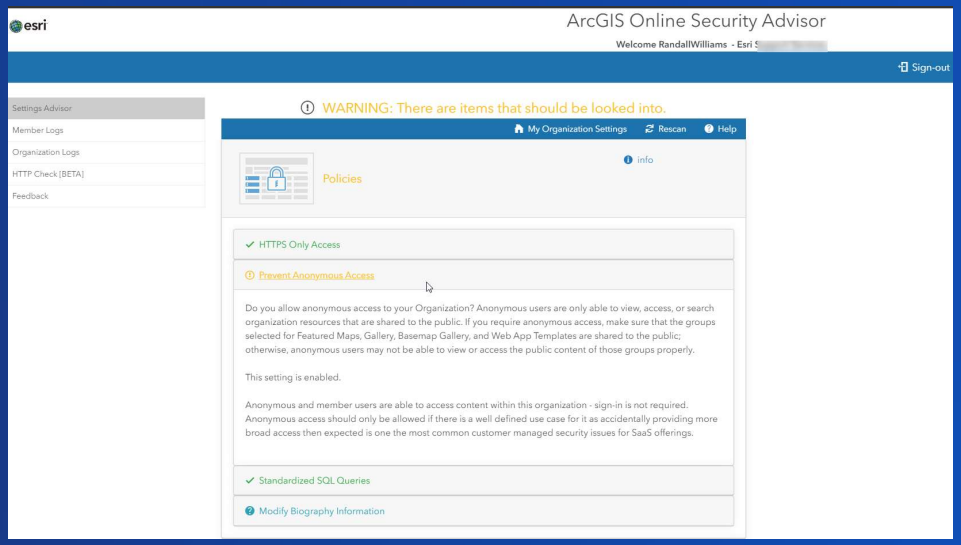


- Require HTTPS
- Do not allow anonymous access
- Restrict members from sharing outside of organization (as feasible)
- Use enterprise logins with SAML 2.0 with existing Identity Provider (IdP)
  - If unable, use a strong password policy (configurable) in ArcGIS Online
  - Enable multi-factor authentication for users
- Always use multi-factor authentication for admin accounts
- Use a least-privilege model for roles and permissions
  - Custom roles

Cloud

ArcGIS Online – Implementation Guidance

- How can you validate your configuration options?
- ArcGIS Online Security Advisor
  - Launch button on ArcGIS Trust Center home page
  - Updated this week with new HTTP Checker in preparation for HTTPS only enforcement



Compliance

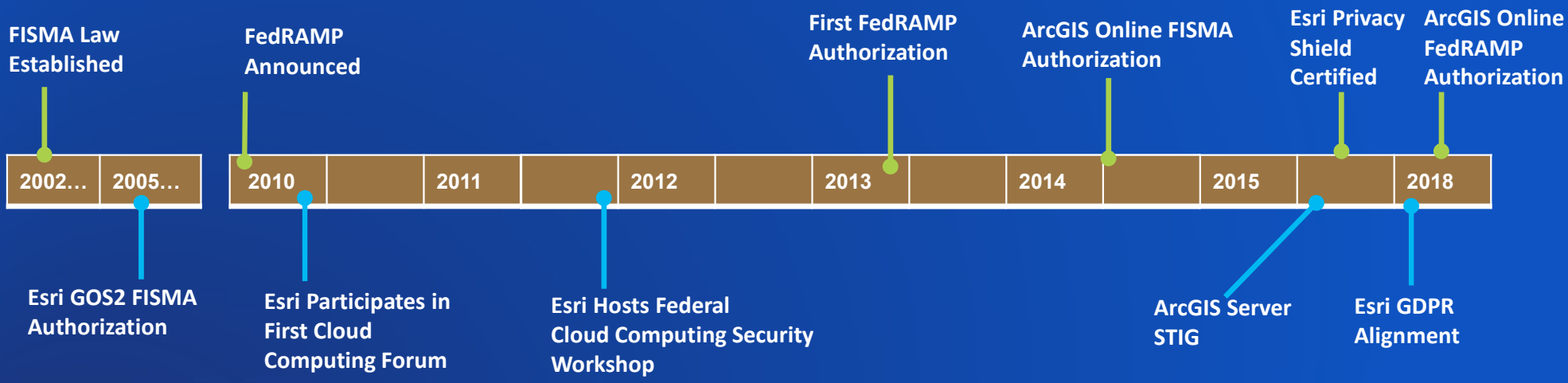
Michael Young

Compliance

- Milestones
- Cloud Infrastructure Providers
- Products and Services
- Privacy Assurance / GDPR
- Security Assurance / FedRAMP

Compliance

Milestones



Esri has actively participated in hosting and advancing secure compliant solutions for over a decade

Compliance

Cloud Infrastructure Providers

- **ArcGIS Online Utilizes World-Class Cloud Infrastructure Providers**
  - **Microsoft Azure**
  - **Amazon Web Services**

Cloud Infrastructure Security Compliance

Compliance

Products & Services

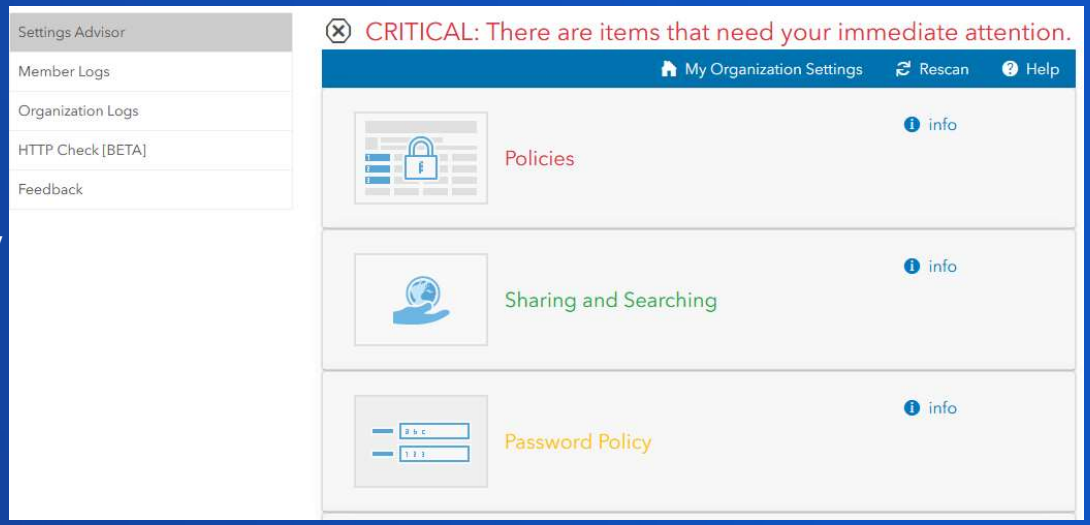
- **Service Based Initiatives**
  - EMCS Advanced Plus (Single-tenant) – FedRAMP Moderate
  - ArcGIS Online (Multi-tenant) – FedRAMP Tailored Low

- **Product Based Initiatives**
  - ArcGIS Server DISA STIG
    - ArcGIS Server 10.3 (ArcGIS Enterprise next)
    - Confirmed compatibility through all current product versions
  - ArcGIS Desktop (10.1 and above) and ArcGIS Pro (1.4.1 and above)
    - USGCB Self-Certified

Compliance

Security Validation Tools

- **ArcGIS Server**
  - Python script located in Admin tools directory
- **Portal for ArcGIS**
  - Python script located in Security tools directory
- **ArcGIS Online Security Advisor**
  - Checklist validates your org settings/usage against secure best practice recommendations
  - *NEW* – HTTP Checker added this week!
- **Python HTTP Checker for Enterprise & Online**
  - To be released later this month



Find latest information for ArcGIS security tools within the ArcGIS Trust Center Security tab

Compliance

Privacy Assurance

- EU-U.S. Privacy Shield self-certified
  - General Esri Privacy Statement
  - Products & Services Privacy Statement Supplement
- TRUSTe
  - Provides privacy certification and dispute resolution
- General Data Protection Regulation (GDPR)
  - Stronger privacy assurance for EU citizens
- California Consumer Privacy Act (CCPA)
  - Alignment expected by enforcement of 1/1/2020

Compliance

GDPR - Protect By Design

- Esri established a formal Security Development Lifecyle in 2017
- Addresses governance structure (CISO – Products, CISO – Corporate)
- Guidelines practices based on BSIMM, OWASP, CWE/SANS
- Most rigorous security measures starting with ArcGIS Enterprise & Online
- Static, Dynamic, and Component Analysis + 3rd party testing
- Product Security Incident Response Team (PSIRT) established
- FedRAMP Tailored Low Authorization drives continuous monitoring
- Customer datasets are encrypted at rest

Compliance

FedRAMP

- **ArcGIS Online Agency FedRAMP Tailored Low authorization-to-operate (ATO)**
  - **Referred to as a Low-Impact Software as a Service (Li-SaaS)**
  - **Standardizes US government security authorization process for cloud products and services**

- **Value to All Organizations**
  - **Recognized by many organizations around the globe as a gold standard for security**
  - **Mapping of ISO 27001 & 15408 controls available via Trust Center**
  - **Ensures annual 3rd party assessments**

Compliance

FedRAMP Alignment

- Customer Responsibility Matrix (CRM) provides guidelines for FedRAMP alignment
  - Enable the HTTPS Only Security Policy
  - Enable Allow only Standard SQL Queries
  - Disable Security Policy allowing members to edit biographical information
  - Enable SAML v2.0 Enterprise Logins
  - Disable Social logins (w/exception for Google business accounts)
  - Add relevant domains for Allow CORS Origins
  - Enable using Esri vector basemaps under Settings/Map/Basemap Gallery

Compliance

Summary

Summary

Michael Young

Summary

- Security demands are rapidly evolving
  - Prioritize efforts accord to your industry and needs
  - Don’t just add components, simplified Defense In Depth approach
- Esri continues to advance their privacy and security
  - FedRAMP Tailored Low authorization and GDPR alignment
  - Prepare for 2020 ArcGIS Online HTTPS only enforcement now
- Secure Best Practice Guidance is Available
  - Check out the Trust.ArcGIS.com Site!
  - New customer only documents section
  - Security validation tool capabilities updated available - use them now!
  - Feel free to contact us:
    - SoftwareSecurity@esri.com

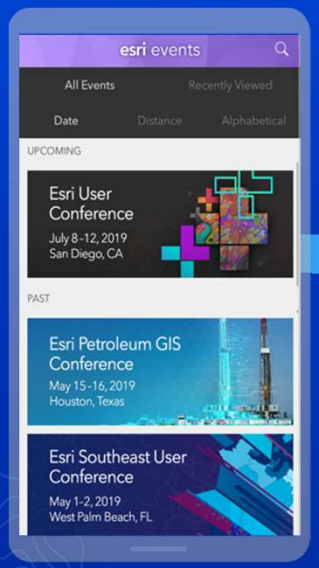
Summary

Useful Security Links

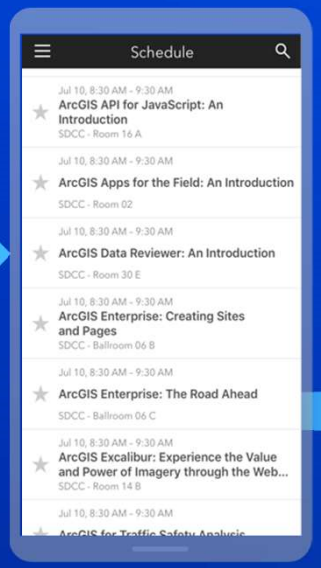
- ArcGIS Trust Center & Latest Security Tools
  - https://trust.arcgis.com
- Overview OWASP Docker Top 10
  - https://github.com/OWASP/Docker-Security/blob/master/D00%20-%20Overview.md
- OWASP Mobile Security Project
  - https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- ArcGIS FedRAMP Authorization Status
  - https://marketplace.fedramp.gov/#/products?sort=productName&productNameSearch=esri
- New Group Managed Service Account (gMSA) KBA for ArcGIS Enterprise
  - https://support.esri.com/en/technical-article/000021125

Please Share Your Feedback in the App

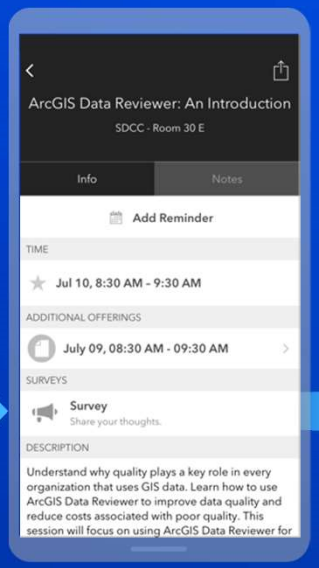
Download the Esri Events app and find your event



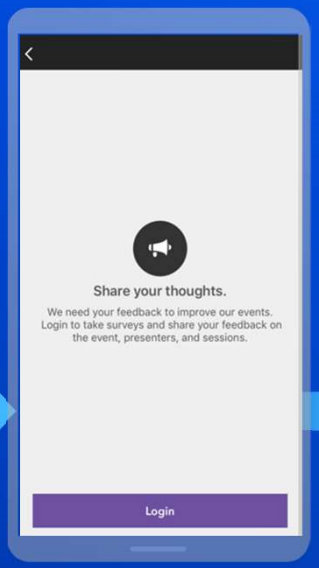
Select the session you attended



Scroll down to "Survey"



Log in to access the survey



Complete the survey and select "Submit"