



Delivering Secure ArcGIS Solutions

Rand Woolley
Michael Young

Overview



- Introductions
- Enterprise Security & ESRI
- Security Controls
- Current Security Trends
- Emerging Standards
- Example Secure Enterprise Implementation
- Questions

Introductions



- **Rand Woolley**
 - Lead author of the ESRI Security Whitepaper
 - Integrator experience
 - Professional Services Enterprise Consultant
 - Oracle DBA / Geodatabase Administrator
 - Large Telecommunications Company
 - Large Utilities
 - Enterprise Strategy
- **Michael Young**
 - Application Security Officer for Geospatial One-Stop
 - ASP/Datacenter management experience
 - Professional Services Enterprise Architect
 - Local, County, State, and Federal Clients
 - Security Audits with Large Financial and Pharmaceutical Companies
 - FISMA Certification and Accreditation Experience
 - Certified Information System Security Professional (CISSP)

Security

Defined by a Pioneering Developer



Security is a kind of death

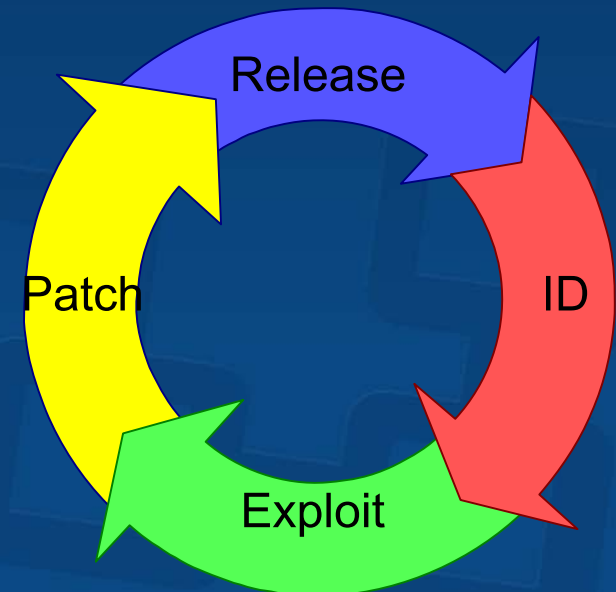
Tennessee Williams (1911-1983)

Enterprise Security

Challenging Environment



- Dynamic
 - ID Vulnerabilities (Users, Software Developers, Hackers, etc)
 - US-CERT (<http://www.us-cert.gov>) Security Bulletins
 - Exploit Vulnerabilities (Hackers)
 - Internet is a Endless Resource
 - Security Patches (Software Providers)
 - Release Schedules
 - Monthly
 - Quarterly
 - As Needed



Enterprise Security

Threats



- Some Common Threats
 - **Spoofing:** Accessing the system using a false identity
 - **Tampering:** Unauthorized modification of data
 - **Information Disclosure:** Unwanted exposure of private data
 - **Elevation of Privilege:** User with limited privileges assumes the identity of a privileged user to gain privileged access to an application.

Enterprise Security

Landscape



- Many Methods of Attack
 - Malicious Code (Trojan Horses, Trap Doors, Logic Bombs)
 - Denial of Service (Render a system unusable)
 - Physical Attacks (Physical Access to system)
 - Buffer Overflows (Extra code placed in Buffer to perform actions)
 - Spamming (Unsolicited E-mail)
 - Brute Force (Attempting all possible password combinations)
 - The list goes on
- Historical View of Enterprise Security -- “The Soft Chewy Inside...”
 - Secure the Perimeter

Enterprise Security

Magnitude



- Enterprise Security Programs
 - Behavioral Controls (policy)
 - Procedural Controls (process)
 - Technological Controls (technology)
- Security Is Part of the Organization Fabric
 - CSO (Chief Security Officer) / CISO (Chief Information Security Officer)

Enterprise Security Strategy



- Identify Risks (Risk Management)
- Identify Vulnerabilities (Vulnerability Management)
- Develop Controls
- Develop Business Continuity Plan (Document)
- Implement Controls
- Perform On-Going Risk Assessment (Verify)
- Document and Take Action

More than one-third (38 percent) of companies do not have comprehensive, integrated disaster recovery and business continuity plans in place.

(Source: Veritas)

Enterprise Security

Structure



- Gartner Enterprise Risk Management (ERM) Framework
 - Definition (formalize risk tolerance into policy)
 - Define Risk Categories (for example: technical, contractual, regulatory)
 - Determine Risk Levels (0-5 scale)
 - Determine Acceptable Risk Level (risk tolerance)
 - Acceptable risk levels for business units
 - Define Risk Levels and Categories as formal policy
 - Planning
 - Analysis
 - Risk Identification
 - Business Impact Analysis
 - Risk Classification
 - Mitigation
 - Avoid / Transfer / Mitigate / Accept
 - Management
 - Control (Measurable / Testable / Auditable / Enforceable)
 - Monitor (Event / Trend / Intelligence / Controls)
 - Report
 - Regulatory Compliance
 - Policy Compliance
 - Risk Dash boarding
 - Risk Benchmarking / Optimization

ESRI & Security

ESRI Role in Enterprise Security



- Ensure ArcGIS software works effectively within enterprise architectures taking full advantage of their inherent security capabilities, either through ArcGIS features and custom extensions or through integration with third-party components.
- *ArcGIS Enterprise Security: Delivering Secure Solutions* – July 2005
 - <http://www.esri.com/library/whitepapers/pdfs/arccgis-security.pdf>
 - esinfo@esri.com

ESRI & Security

Security-In-Depth Approach



- Enterprise-Wide Initiative
- Multiple Layers
 - Bi-directional
 - No single technology or technique
- Beyond Technology Solutions
 - Physical Security
 - Security Policy Guidelines
- Security zone based architecture
 - Further split in segments
 - Compartmentalizing systems

ESRI & Security

Security Solutions are Unique



- Identify **YOUR** Enterprise Risks
- Define **YOUR** Enterprise Control Set
- Implement Reasonable and Appropriate Controls
- Perform On-Going Risk Assessment
- Document, Document, Document and Document



Security Controls

ArcGIS

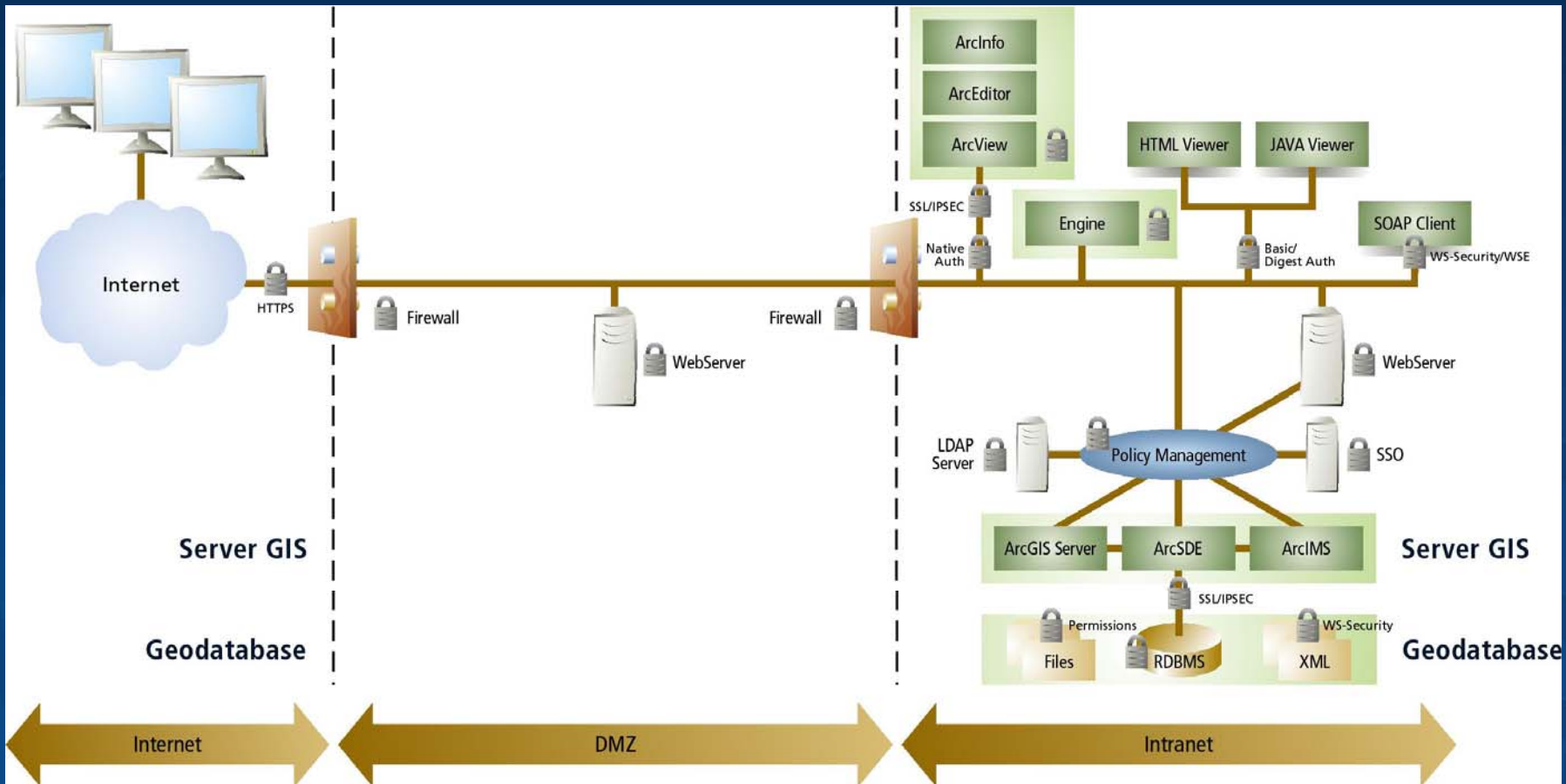
Security Controls



- ArcGIS leverages secure functionality provided by underlying technology and configuration
 - RDBMS / Data Controls
 - Network Controls
 - Operating System Controls
 - Emerging IT Industry Standards (Application Controls)
- ArcObjects Provides Integration Capabilities (Flexible ArcGIS Framework – Interoperability)

ArcGIS

Security Controls

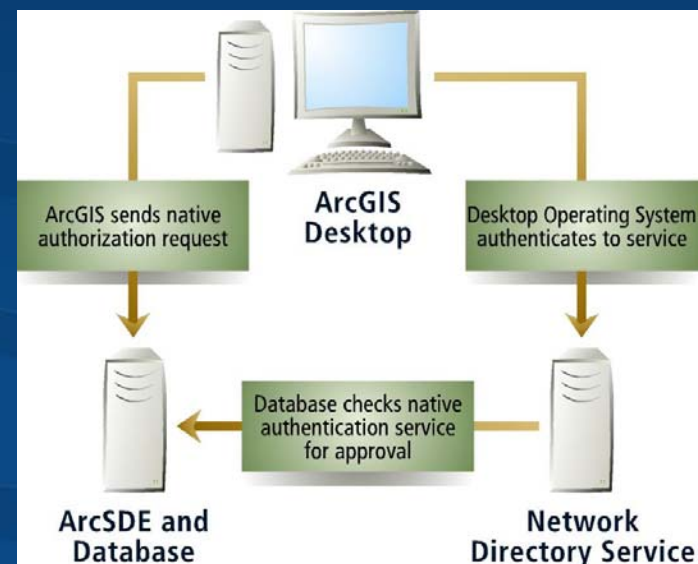


Data Controls

Authentication



- Username and Password
 - Managed by RDBMS
- Integrated Windows Authentication
 - Auditing
 - Password Aging
 - Password Hardening
 - Account Lockout



Data Controls

Authentication



- Central User Repository
 - Application Development (ArcObjects)
 - Active Directory / LDAP Integration
 - Group Policies (Standardized Configurations)
 - » File Permissions
 - » Executable Permissions
 - » Desktop Permissions
 - » Password Complexity
 - » Password Aging
 - » Encrypted File System (EFS)

Data Controls

Access Control



- Role Based Security
 - Traditional RDBMS Roles
 - Permissions are assigned to roles and..... roles are assigned to users
 - ArcGIS assignment of permissions via ArcCatalog
 - Secure Application Roles
 - Associate a package (piece of code) with a defined Geodatabase role
 - Apply security layer in centralized location versus application code → Easy policy updates
 - Role Based Auditing (“Fine Grained Auditing”)
 - Associate auditing events based on DML (Insert, Update, Delete)
 - Audit Trail is stored in the database as a object for easy access

Data Controls

Access Control



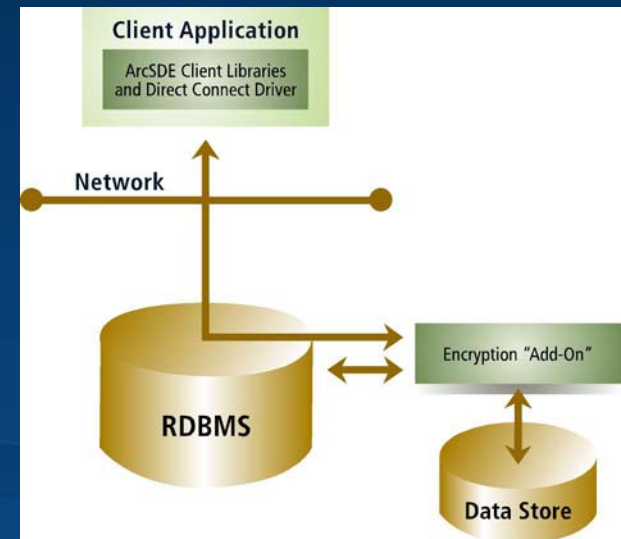
- Label Security (“Row Level Security”)
 - Multi-Level Security
 - Sensitive But Unclassified
 - Classified
 - Secret
 - Top Secret
 - Complexity of Implementation is directly related to “Row Level Security” needs
 - Read-Only “Publish” Geodatabase
 - Versioning

Data Controls

Protecting Data at Rest



- Disk Level Encryption
 - Functionality provided by Underlying RDBMS
 - RDBMS provides the key Management Infrastructure
 - SQL Server 2005
 - Oracle
 - Protegrity
 - Master Key is developed for entire database
 - Encryption of fields designated at table level
 - Protect Sensitive data stored on disk in a manner transparent to the application and user



Network Controls

Firewalls

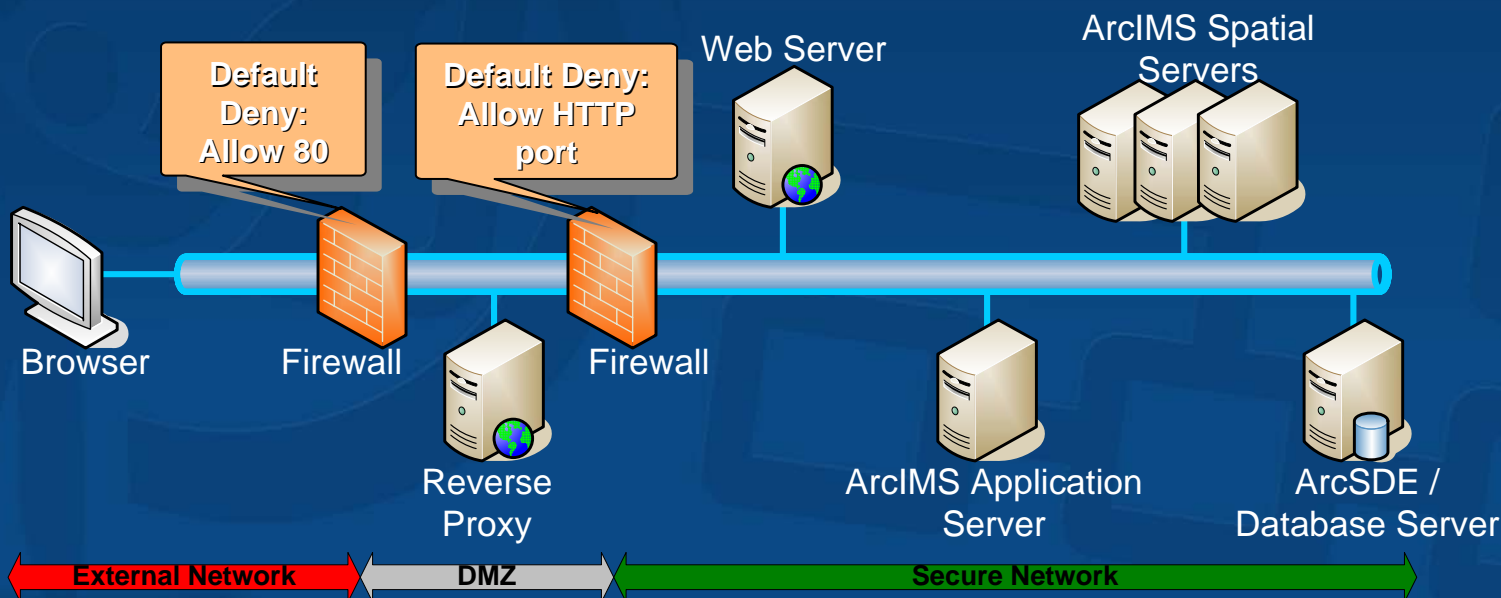


- Enforce security policy by controlling what is allowed to cross a designated point in the network.
- Basic Advantages
 - Can Restrict inbound and outbound traffic
 - Can Filter traffic based on content
 - Can Perform Network Address Translation (NAT)
 - Can Log successful and blocked traffic to Assist Intrusion detection and incident forensics
- Placement of your firewall is a key element of your overall Defense-In-Depth strategy

Network Controls

Firewalls – Reverse Proxy

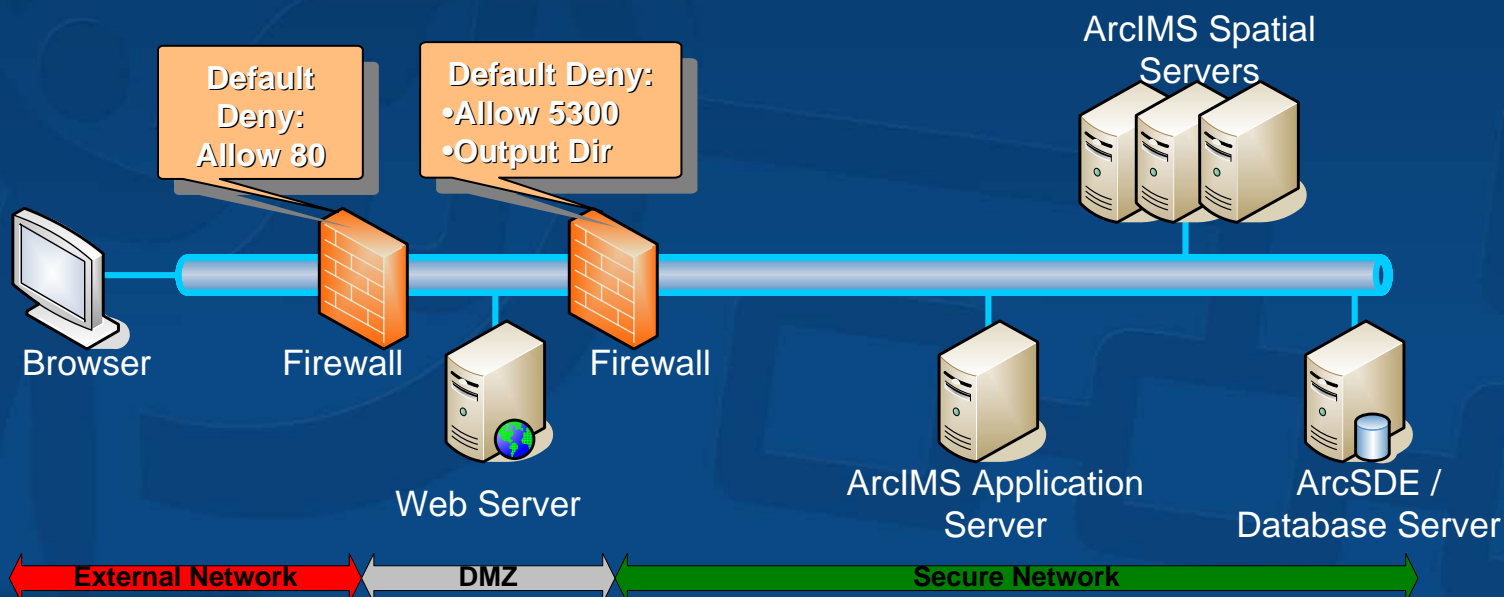
- Reverse Proxy Considerations
 - Performance Impact minimized
 - Minimal Ports allowed through firewall
 - NAT supported
 - Controlled exposure to external network



Network Controls

Firewalls – Web Server in DMZ

- Web Server Considerations
 - ArcGIS Components located on secure network
 - Map output drive through firewall
 - NAT Supported

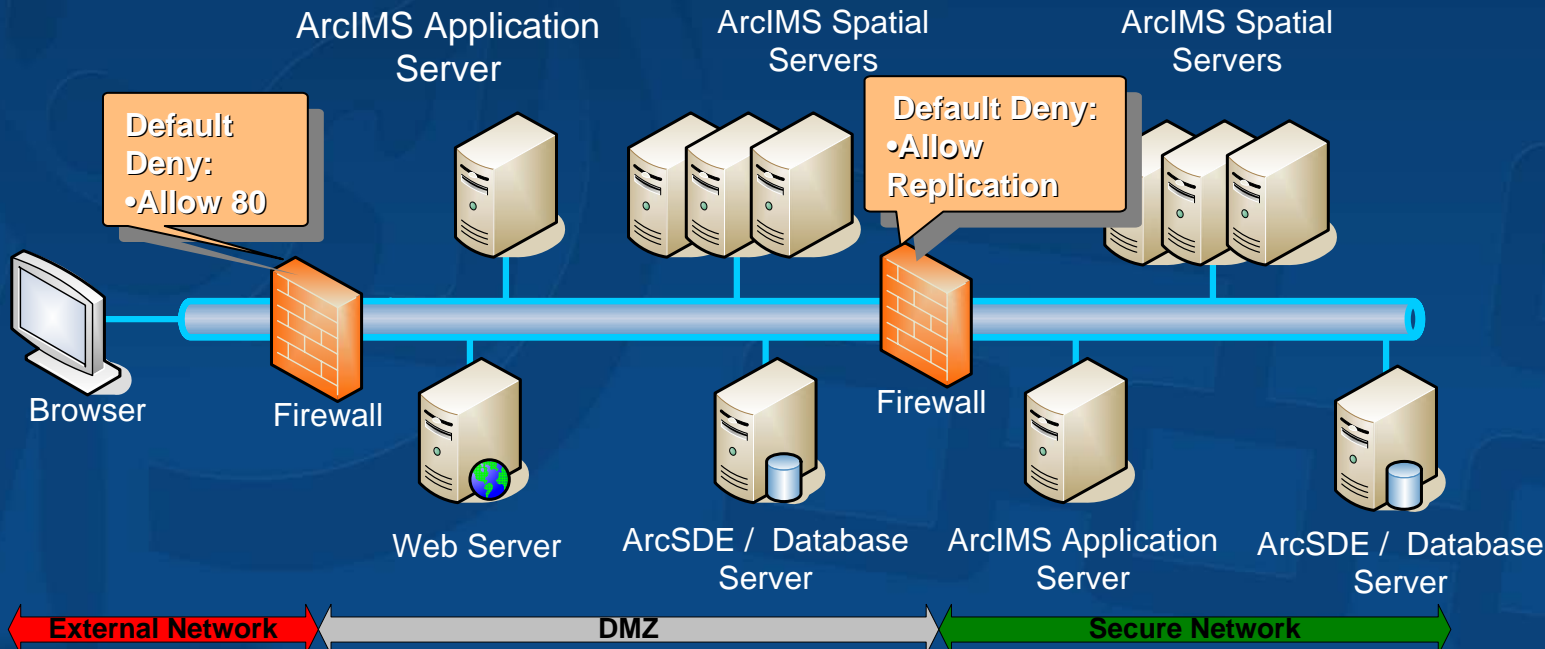


Network Controls

Firewalls – ArcGIS Components in DMZ



- DMZ Considerations
 - Buffer between external and internal systems (Communication only one way between secure and external)
 - Operationally More Complex
 - Additional Costs (Hardware / Software)



Network Controls

Firewalls – Common ArcIMS Ports



- ArcIMS Considerations For Firewall Placement
 - Performance
 - Image/Output Directory
 - Firewall Timeouts

PORT	PROCESS	COMMENT
80	Apache Web Server	Incoming HTTP requests.
8007	Tomcat Servlet Engine	Incoming web server requests.
8080	Tomcat Servlet Engine	Tomcat's built-in web server.
5300	ArcIMS Application Server	Servlet connector for admin requests and client requests.
5353	ArcIMS Application Server	Listens to Tasker, Monitor, Spatial Server, and Virtual Server.
5050	ArcIMS Monitor	Listens to application and spatial servers.
5060	ArcIMS Tasker	Listens to application server.
5151	ArcSDE	Listens to spatial server.

Network Controls

Firewalls – Common ArcGIS Server Ports



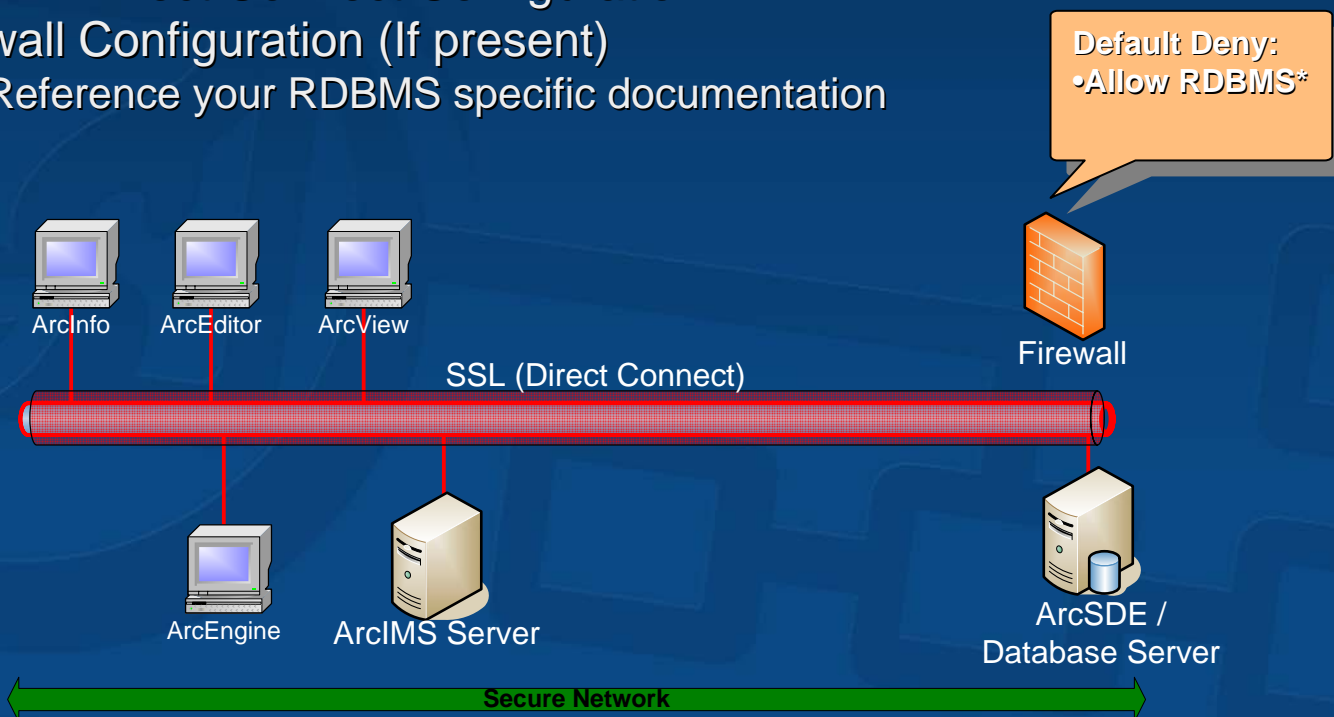
- ArcGIS Server Considerations For Firewall Placement
 - Ports
 - ArcGIS Server Components (SOM/SOC) Utilize the Distributed Component Object Protocol (DCOM)
 - NAT Translation NOT Supported in Some Configurations
 - Performance
 - Firewall Timeouts

PORT	PROCESS	COMMENT
80	Apache Web Server*	Incoming HTTP requests.
8007	Tomcat Servlet Engine*	Incoming web server requests.
8080	Tomcat Servlet Engine*	Tomcat's built-in web server.
135	ArcGIS Server Server Object Manager (SOM)	Listens to Web Server.
135	ArcGIS Server Server Object Container (SOC)	Listens to Web Server.
5000-5nnn	Defined communication between SOM & SOC (DCOM)	Defined communication between SOC & SOM – DCOM Communication
5151	ArcSDE	Listens to SOC.

Network Controls

SSL – Protecting Data in Motion

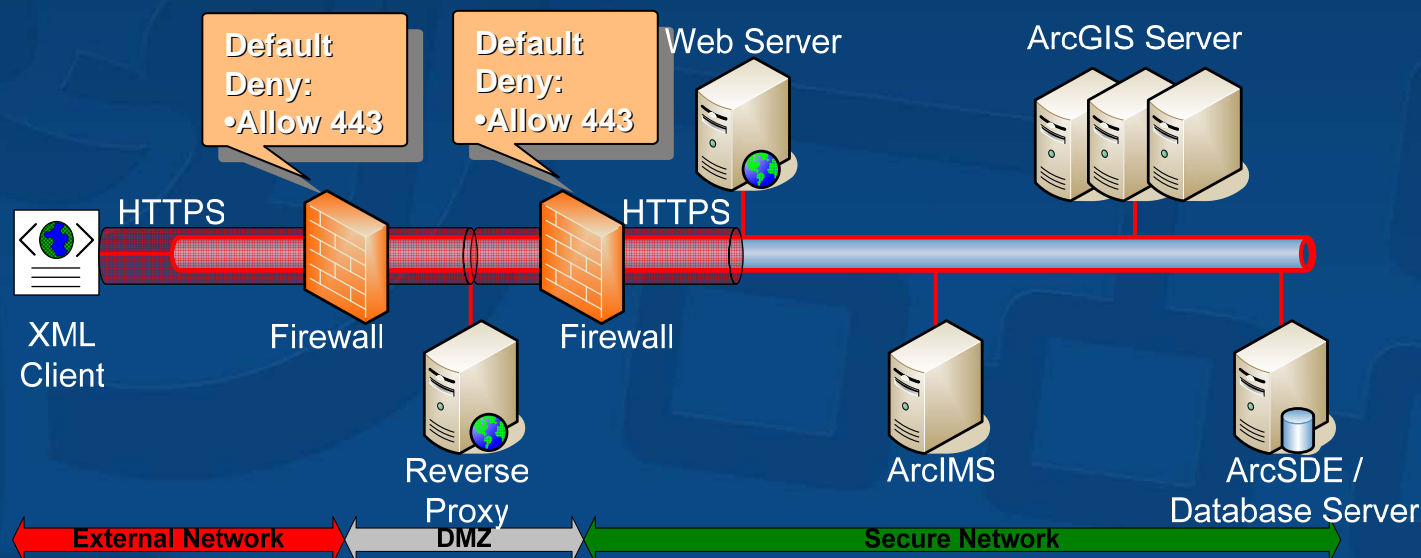
- Secure Session between Client (Desktop, ArcIMS, etc) and Database Server
- Considerations
 - SSL Provided by Underlying RDBMS
 - ArcSDE Direct Connect Configuration
 - Firewall Configuration (If present)
 - Reference your RDBMS specific documentation



Network Controls

SSL – Protecting Data In Motion

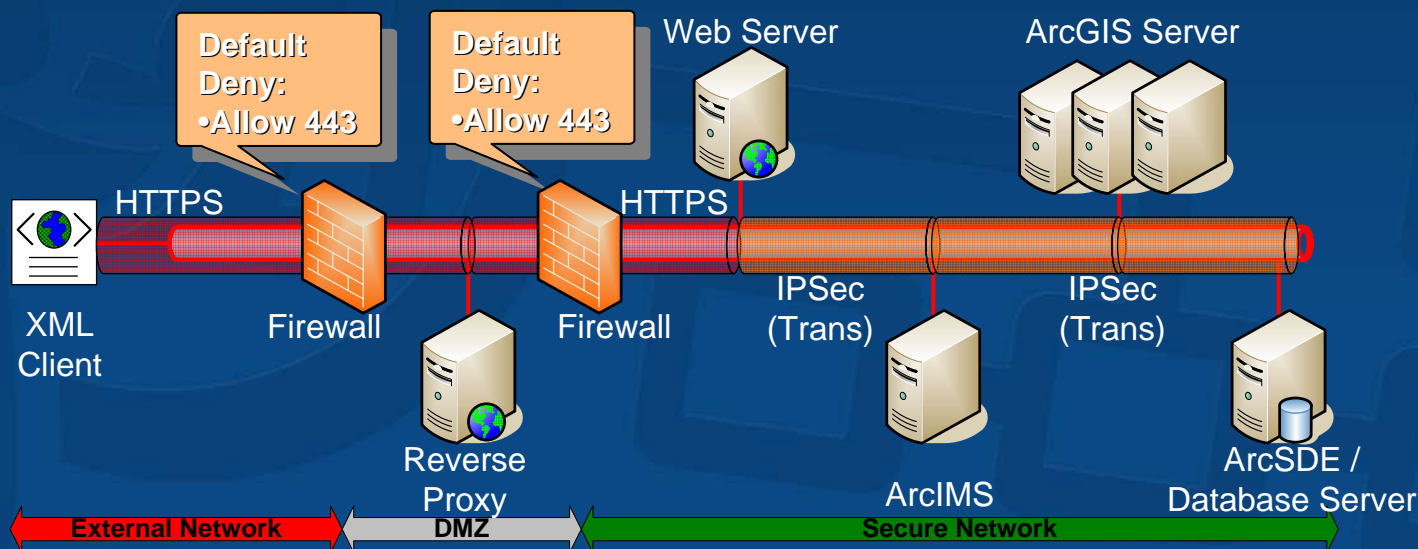
- HTTP over SSL (HTTPS)
- Considerations
 - COTS ArcGIS Clients Can NOT Consume (Custom ArcGIS / SOAP Clients)
 - Future COTS ArcGIS Releases – Requires Adapter
 - Activated at Web Server
 - Encryption Algorithm
 - Valid Server Certificate from CA
 - Firewall Configuration
 - Port 443



Network Controls

IPSEC – Protecting Data in Motion

- IPsec
 - Considerations
 - Configuration
 - Microsoft (<http://support.microsoft.com/?kbid=233256>)
 - SUN (<http://docs.sun.com/app/docs/doc/816-7264/6md9iem15#hic>)
 - Linux (<http://www.ipsec-howto.org/>)
 - Cross Platform Support (See Operating System Documentation)
 - Encryption Algorithm
 - DES / TRIPLE DES / AES



Network Controls

IPSEC



- IPSEC Modes
 - Transport Mode (Host-to-Host)
 - Tunnel Mode (Host-to-network or network-to-network)
- IPSEC Protocols
 - Encapsulation Security Payload (Provides Authentication and Encryption)
 - Authenticating Header (No encryption/minimal overhead)
- Additional Considerations
 - LINUX ipchains is limited to packet filtering
 - Windows provides capabilities to enable encryption between two servers
 - Note that this results in some performance degradation (2-10% performance hit)
- Example:
 - To create a rule on the computer named corpsrv1 for all traffic between the computers named corpsrv1 and corpsrv2, using the combination of both AH and Encapsulating Security Payload (ESP), with pre-shared key authentication, type:

```
ipseccmd \corpsrv1 -f corpsrv2+corpsrv1 -n ah[md5]+esp[des,sha] -a p:"corpauth"
```

- ArcGIS Service Protection
 - Restrict communication between web server and ArcIMS Server

ArcGIS Integrated Controls

LDAP - Desktop



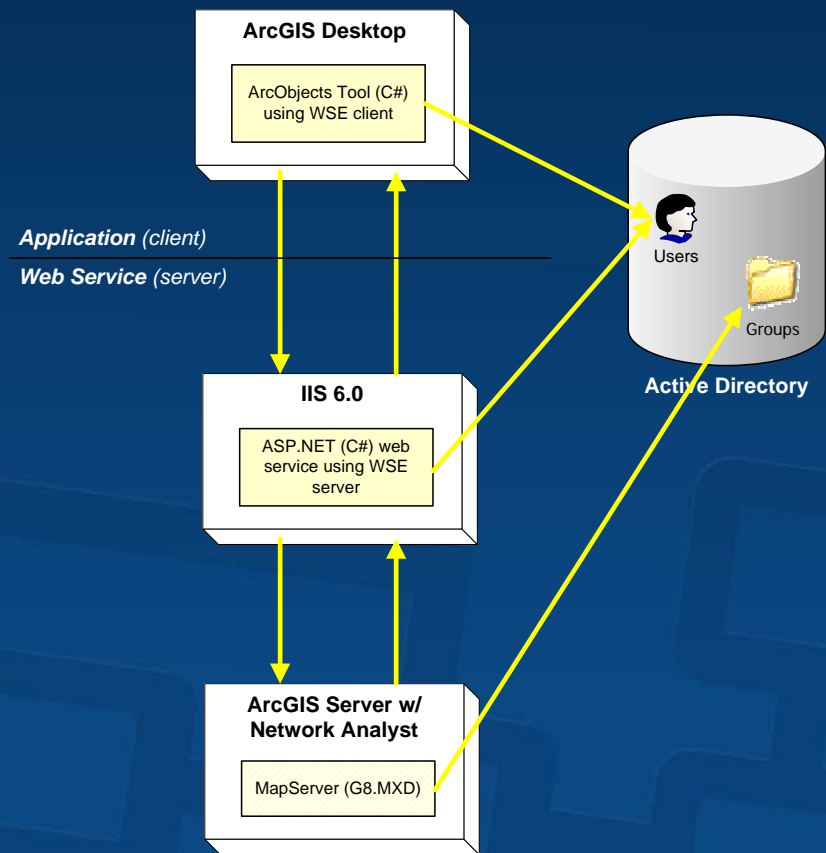
- Log In Desktop / Domain
- ArcMap
- Credentials from Desktop (.Net API for Active Directory)
- Get Connection encrypted connection string from Active Directory
- Through ArcObjects connect to workspace using obtained encrypted string
- Custom Extension for ArcCatalog that created custom objects for managed connections (Stored in Active Directory)
- Disable the ability to add spatial connection

ArcGIS Integrated Controls

LDAP – Web Service



- ArcMap (MXD)
- ArcObjects Tool to Consume Web Service
- Credentials from Desktop
- Active Directory used for authentication and authorization
- HTTPS used to secure transfer of information from application to service
- WSE used to securely pass identity to service (User Token used to encrypt sensitive components of message)
- ASP.NET web service uses impersonation to connect to ArcGIS Server

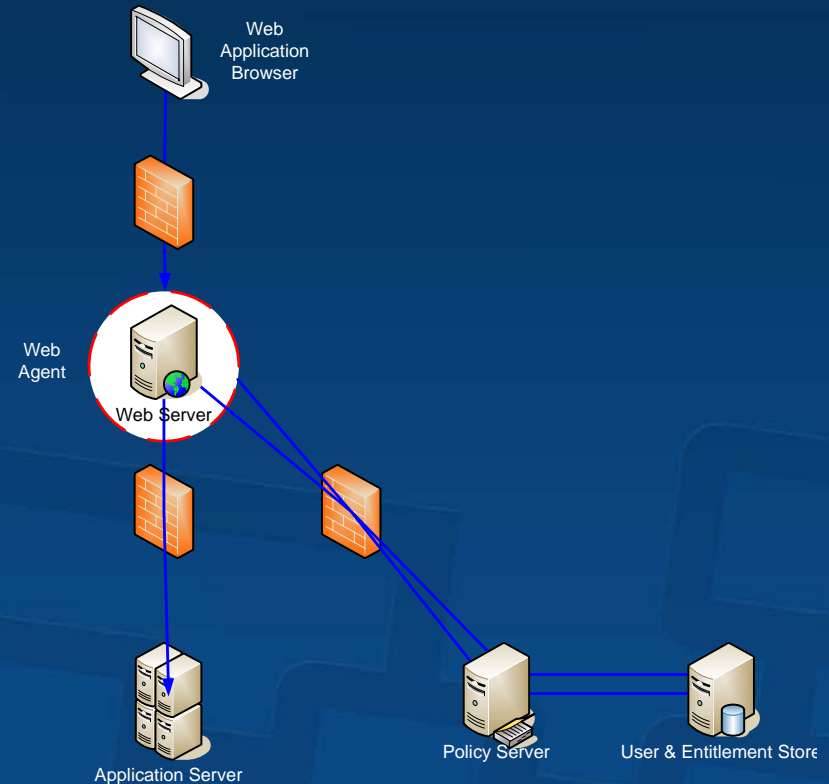


ArcGIS Integrated Controls

SSO



- Centrally Managed Repositories
- Web Deployment descriptor information (redirect web server requests)
- Authentication Methods
 - SAML (Security Assertion Markup Language)
 - X509
 - Two-factor tokens
 - Smart cards
- User-driven security policies used to determine if the user has access to a specific resource

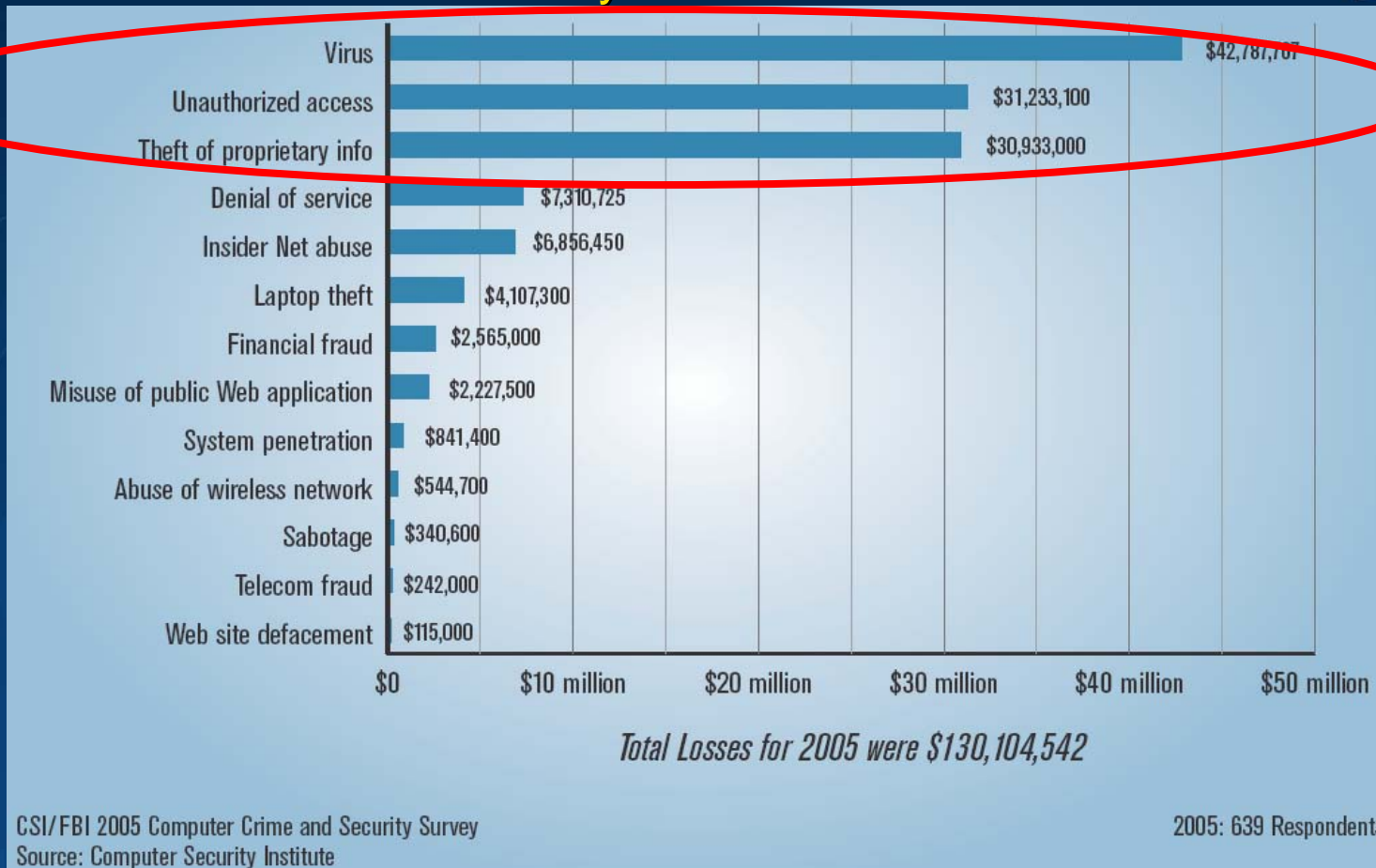




Current Security Trends

Current Security Trends

Dollar Amount Losses by Threat

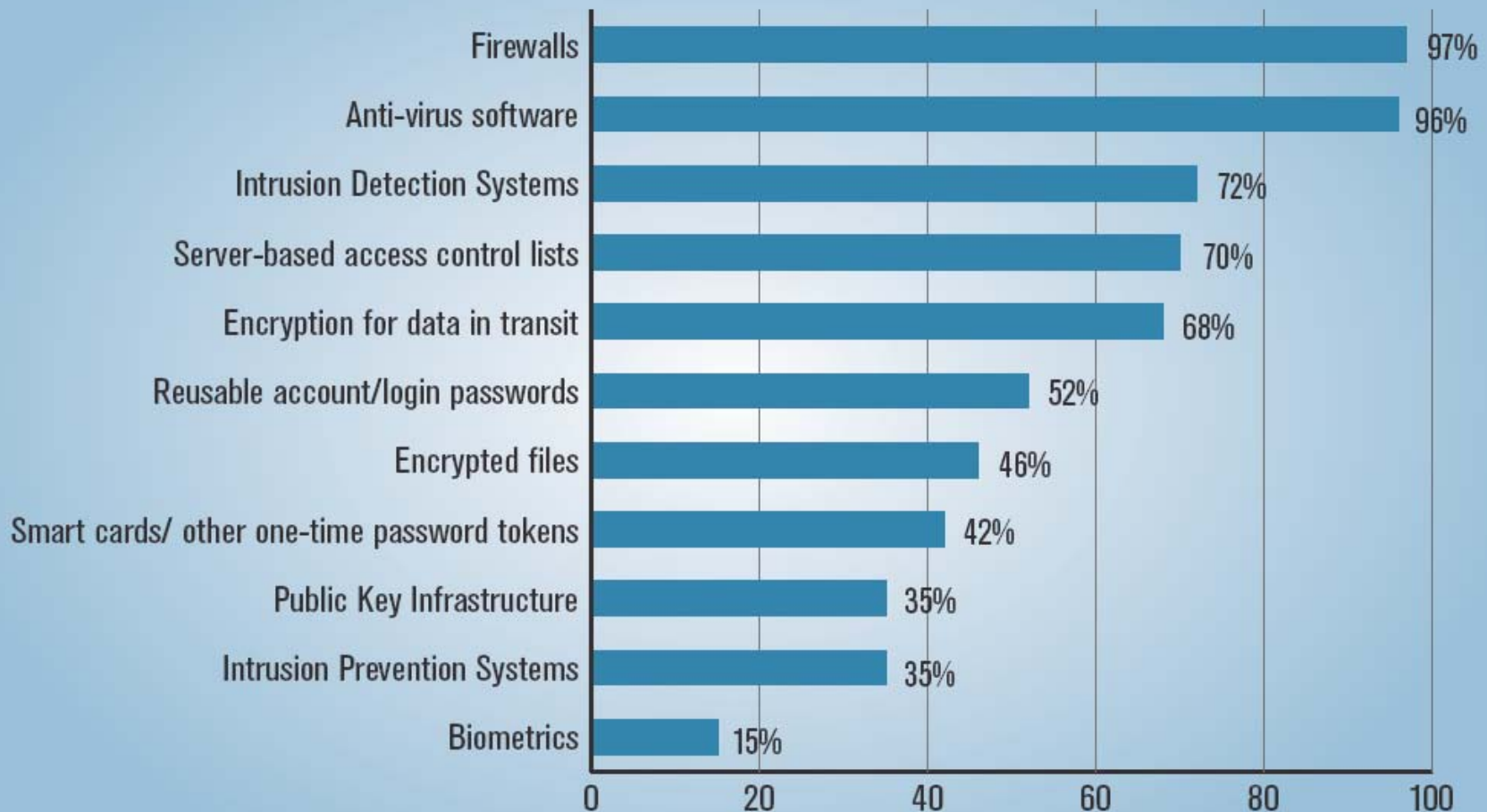


Unauthorized access increased dramatically replacing denial of service as the second most significant contributor to computer crime losses

Theft of proprietary information significantly increased in average loss per respondent, more than double that of last year

Current Security Trends

Security Technologies Utilized



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

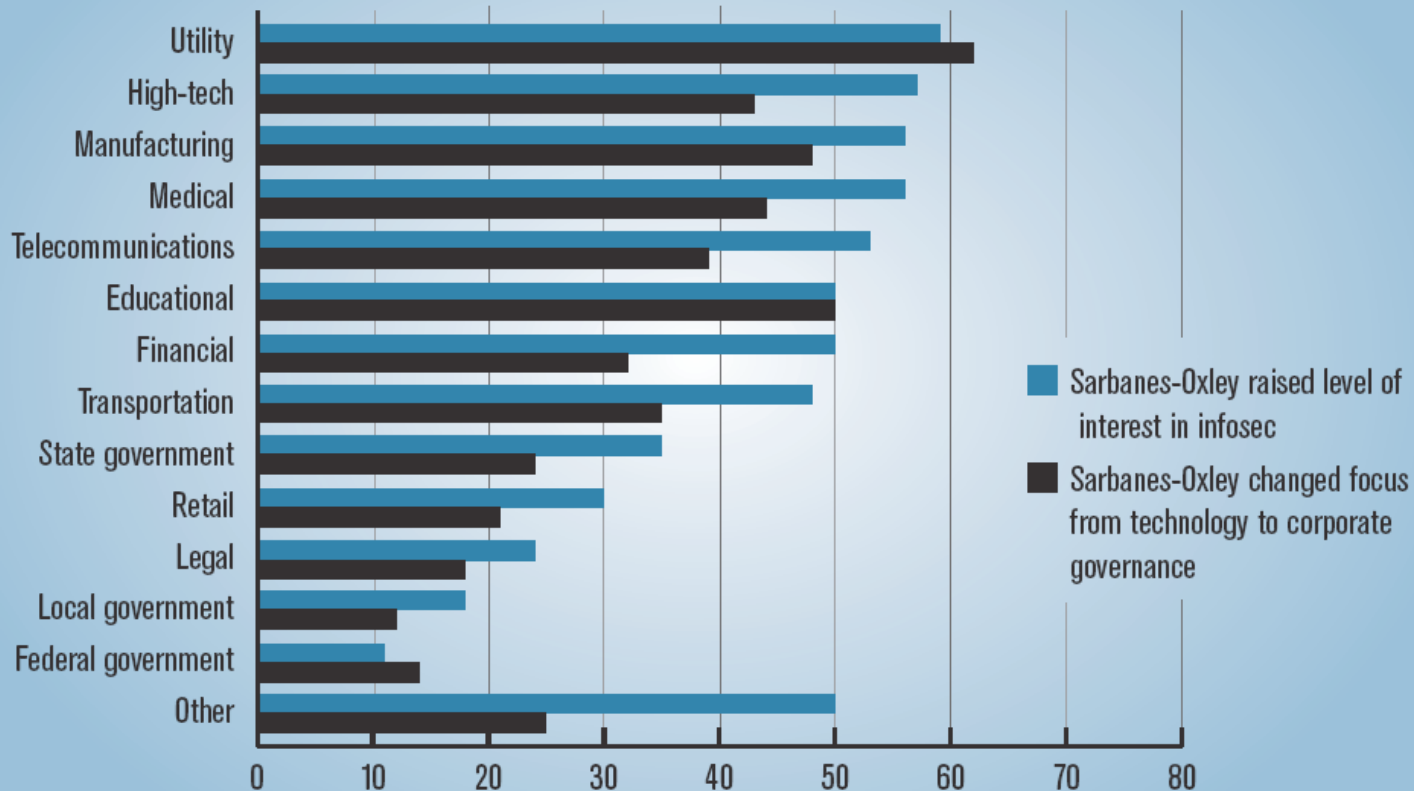
2005: 687 Respondents

Current Security Trends

Impact of SOX Act



Percentage of respondents that agree



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 679 Respondents



Emerging Standards

Emerging Standards



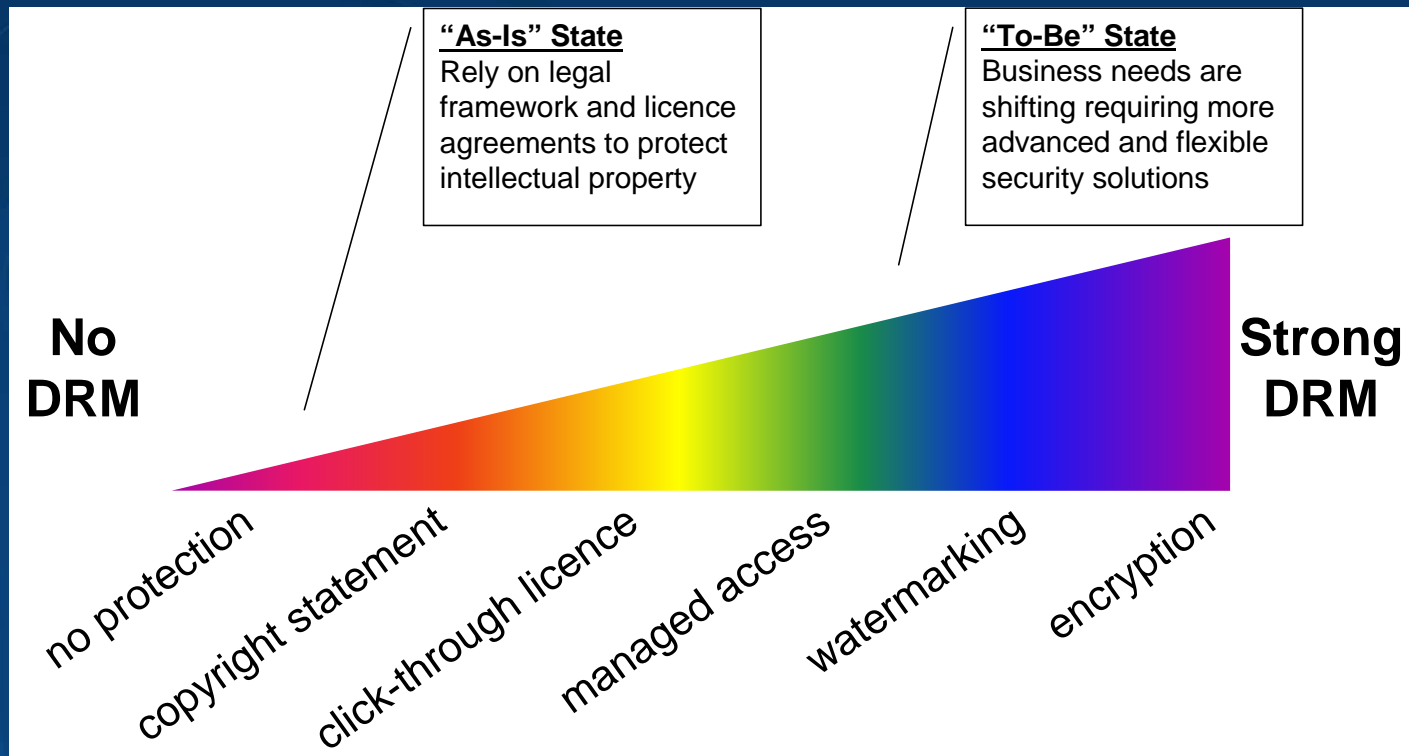
- GeoDRM
- GeoXACML
- WS-Security
- Federated Identity Management

Emerging Standards

GeoDRM



- How can I share data without losing control?
 - Digital Rights Management (DRM)

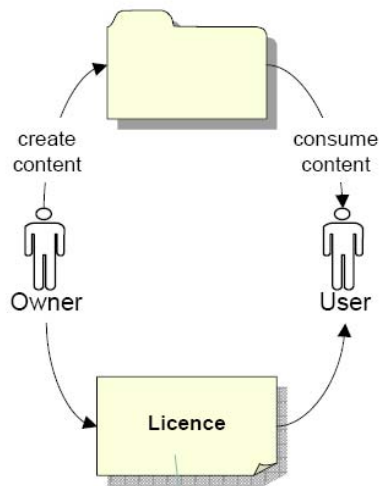


Emerging Standards

GeoDRM

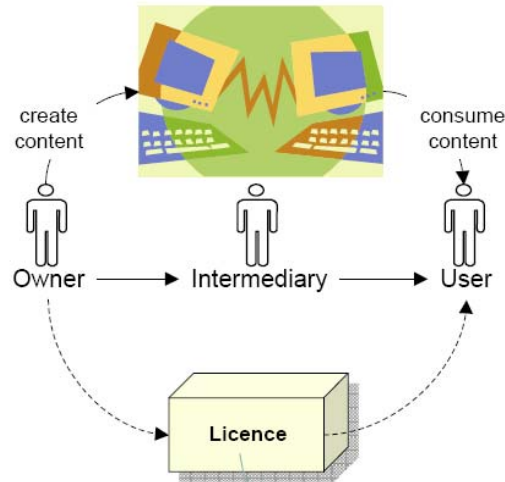


Classic DRM



Extents of licence are "one-dimensional" rights. Display, print, play etc.

GeoDRM Network



Extents of licence are "multi-dimensional" rights and space and time etc.

A multi-dimensional DRM solution would incorporate rights, space and time elements

GeoDRM still being formed

Track now to ensure alignment in the future

Emerging Standards

GeoXACML



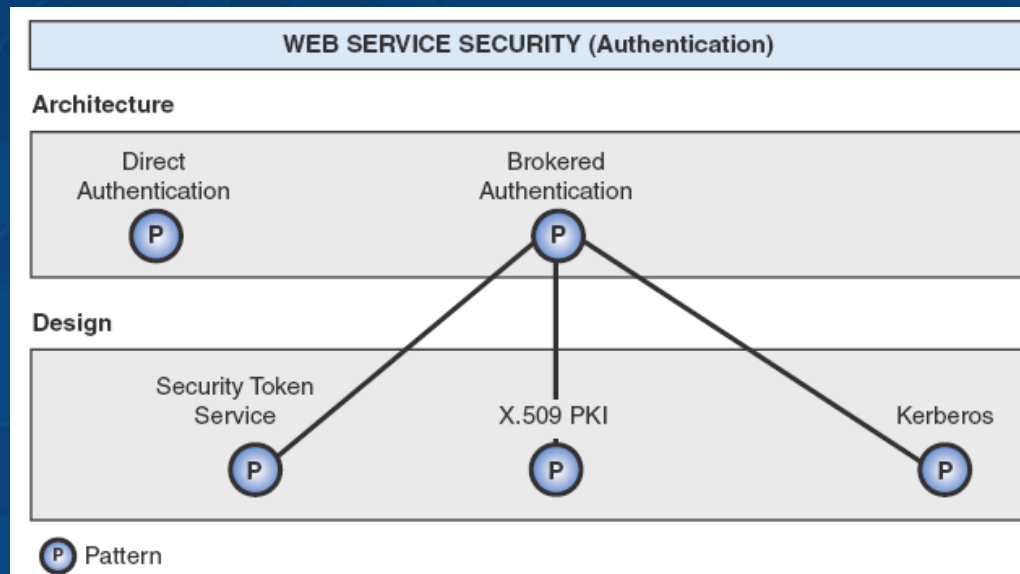
- **eXtensible Access Control Markup Language (XACML)**
 - From OASIS
 - Provides rule-based access control and defines the means for restricting access to XML encoded information
 - No support for spatial restrictions
- **GeoXACML**
 - Adds support for spatial restrictions such as:
 - Class based (e.g. All features of type building)
 - Object based (e.g. All features of type building, painted black)
 - Spatial (e.g. All buildings within an administrative boundary)

Emerging Standards

WS-Security



- Beyond point-to-point security of SSL
 - Enhancements to SOAP messaging to provide message integrity and confidentiality
 - Supports wide variety of security models and encryption technologies

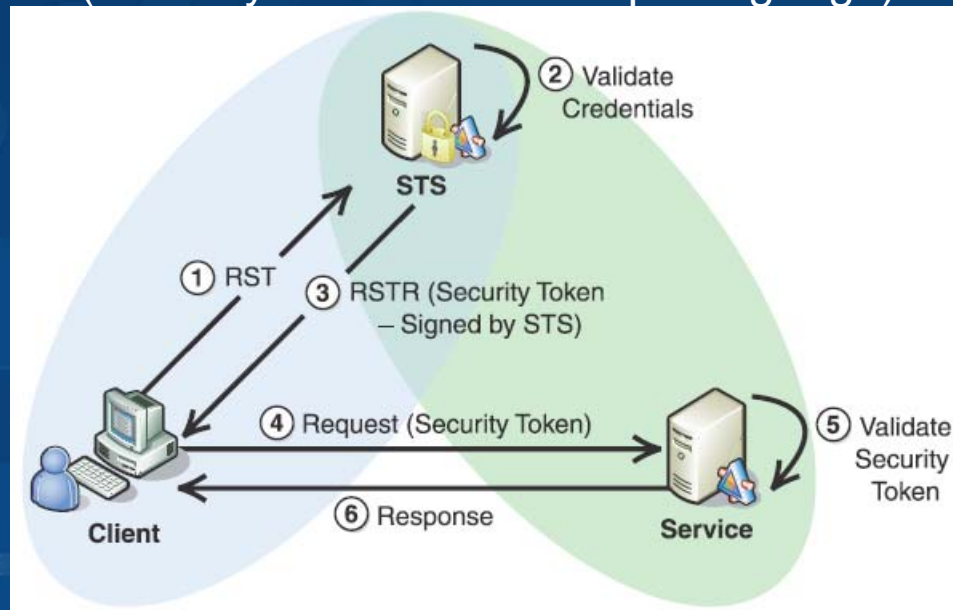


Emerging Standards

Federated Identity Management



- HSPD-12
 - Smart Card Identification
- E-Authentication Initiative
 - SSO between different organizations
 - Private sector and Public
 - GeoSpatial One-Stop will be added
 - Multiple levels of identity verification requirements
 - Follows Brokered Security Token Security Pattern
 - SAML (Security Assertion Markup Language)





Example Secure Enterprise Implementation

Example Secure Enterprise Implementation



- An Actual Customer Solution
 - Functionality Provided
 - Common Operating Picture (COP) Application
 - Open Web Map Services
 - Multi-Organization Spatial Data Repository
 - Heterogeneous Data Loading and Downloading
 - Constraints
 - No Trusted Communication Networks
 - No Centralized Owner
 - Contained Sensitive But Unclassified Data
 - Minimize Costs
 - Minimize Management Requirements
 - Provide high availability
 - Full Synchronization of data between sites

Example Implementation

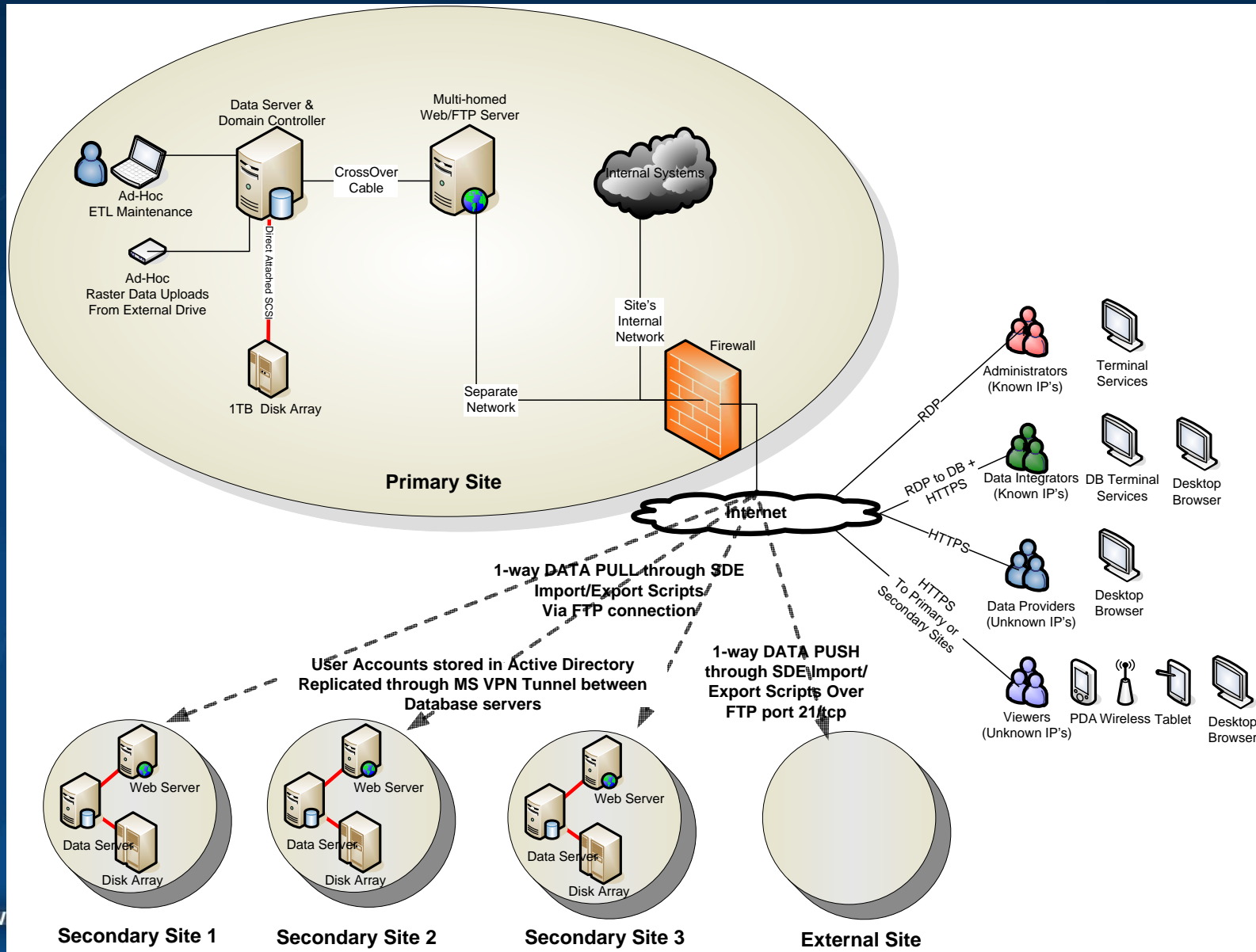
Initial Recommendations



- A homogeneous system:
 - Platform Windows 2003 Server
 - Web IIS 6
 - Database SQL 2000
 - Mapping ArcIMS 9
 - Users Active Directory
 - Replication VPN - Routing and Remote Access

Example Implementation

Architecture Overview



Example Implementation

Fundamental Tradeoff



Secure



You get to pick any two!

Usable

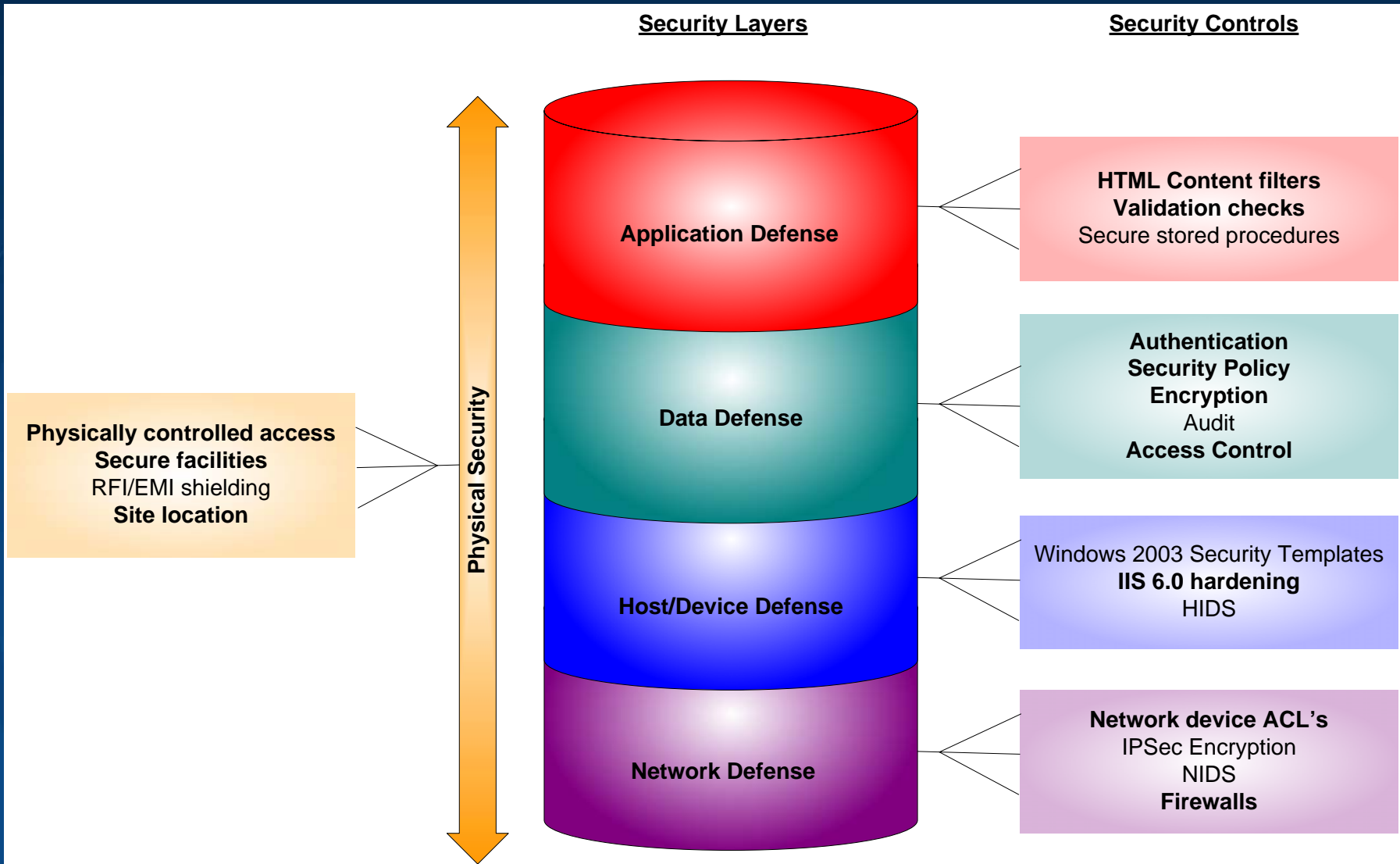


Cheap



Example Implementation

Security Controls Utilized



Example Implementation

Security Controls Utilized



- Anti-Virus
- Multi-homing
 - Allows for separation of traffic types
 - Facilitates TCP/IP port filtering
- Security Lockdowns
 - Utilized SANS 10 Top Issues
 - Microsoft Baseline Security Analyzer
 - Turn off unused services
 - Eg. Tomcat web service on port 8080 disabled by commenting it out of the server.xml file
 - Minimize generally available ports
 - IPSec Filtering utilized to reduce service exposure
- Encryption
 - 128-bit SSL for web traffic
 - Utilized MS SelfSSL for initial testing (Free Cert generation tool)
 - 128-bit AES encryption of files sent via FTP (Meets FIPS 197 SBU handling requirements)
- Authentication
 - Integrated Windows Authentication against MS Active Directory
- Access Control Lists
 - NTFS permissions at role level

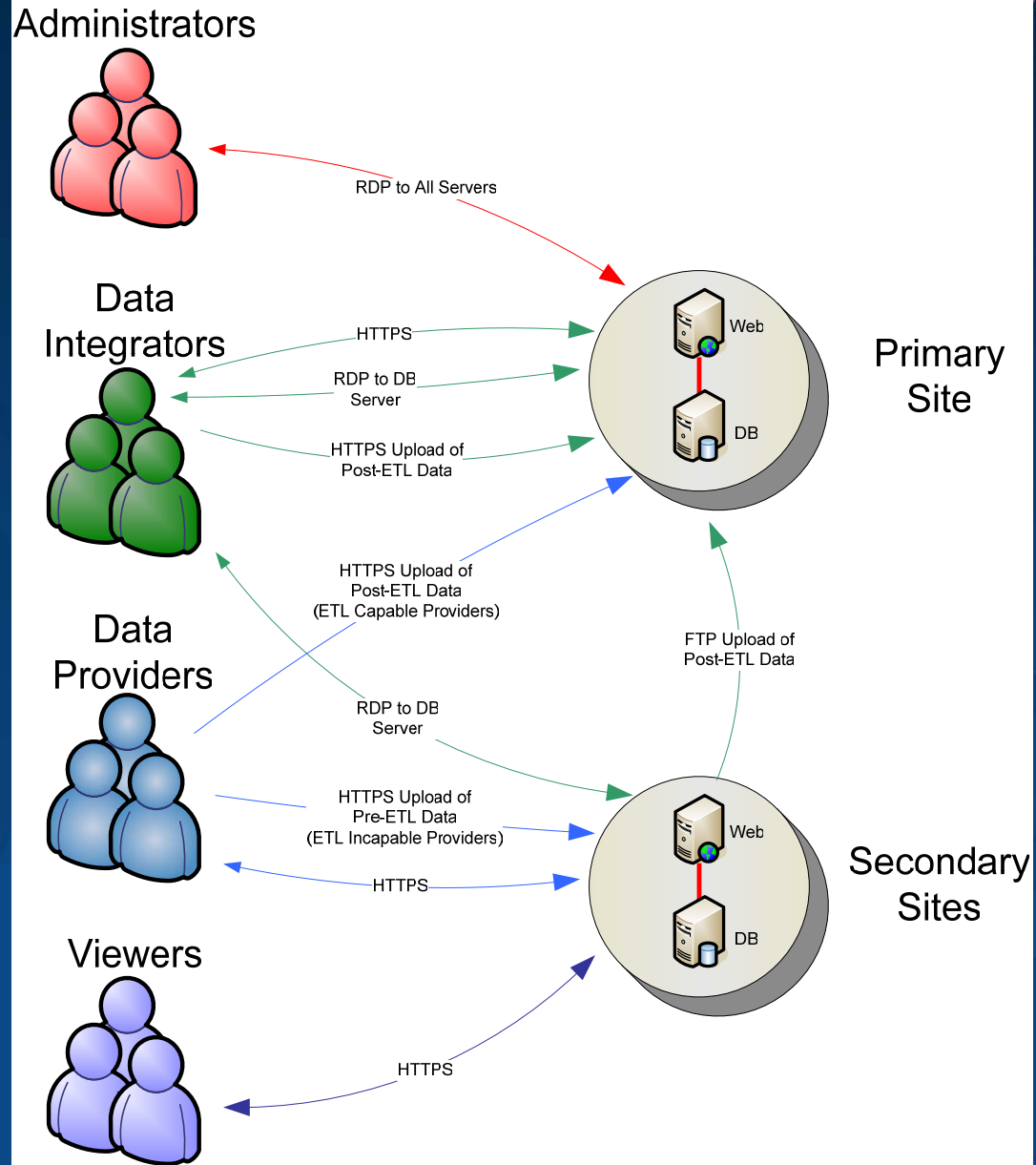
Example Implementation

User Roles

Users rights are managed at the role level

Single authentication mechanism for:

- Database
- Web Application
- OS Administration



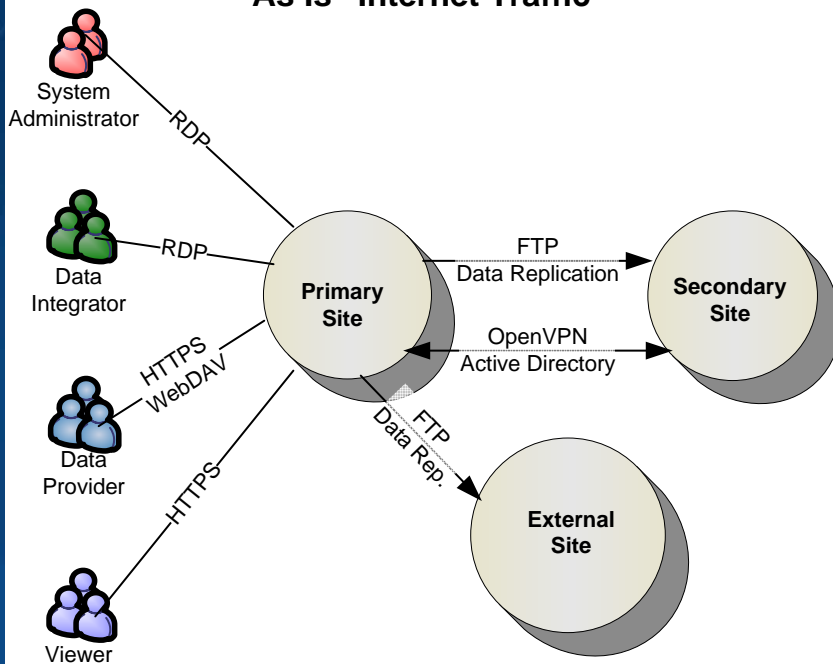
Example Implementation

Propose Improvements

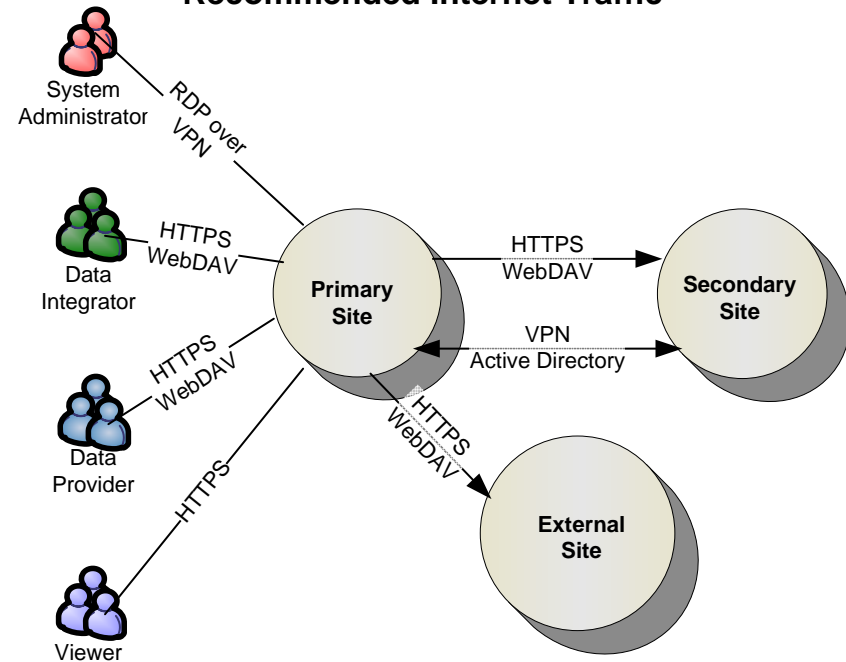


- Project constraints may led to sub-optimal solutions
- Provide a summary of improvements that can be made over time

“As Is” Internet Traffic



Recommended Internet Traffic





Summary

Summary



- Discussed Security Basics
- Described how to use specific security mechanisms
- Discussed Emerging Standards
- Reviewed a Secure Enterprise Example

Summary

ESRI Security & You



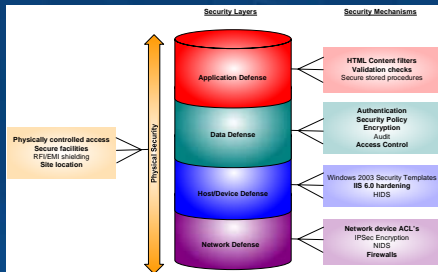
- Today's discussion was limited to specific security solutions
 - Tell us your strongest security needs concerning ESRI products
 - We will address the highest priorities in future security Presentations / Whitepapers
 - Email suggestions to:
 - esinfo@esri.com

Summary

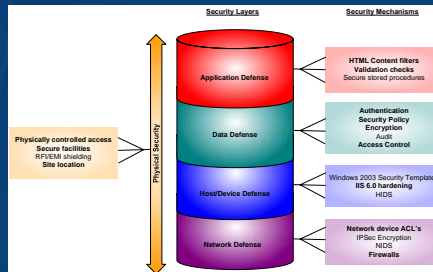
What do YOU think?



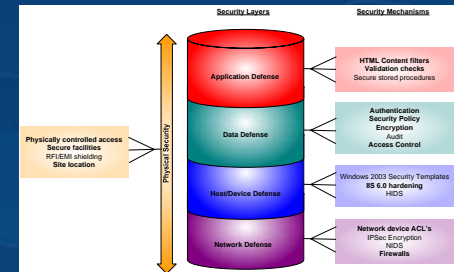
- Security Lab Suggestions
 - SOA Security...
- Tailored Controls
 - ESRI providing Low, Medium, and High recommendations for Enterprise GIS Systems



Low Risk
Environment



Med Risk
Environment



High Risk
Environment

Session Evaluations Reminder



Session Attendees:
Please turn in your session evaluations.

... Thank you

References



- 2005 CSI/FBI Computer Crime and Security Survey
 - http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
- Scenarios, Patterns, and Implementation Guidance for Web Services Enhancements 3.0, Dec 2005
 - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpag2/html/wss_ch1_intro.asp
- “NMCA’s and the Internet II” Workshop, G. Vowles, 2/23/05
- Gartner’s Simple Enterprise Risk Management Framework”, Rich Mogul, December 2004