ArcGIS® Enterprise Security: Delivering Secure Solutions

An ESRI® White Paper • July 2005

ESRI 380 New York St., Redlands, CA 92373-8100, USA • TEL 909-793-2853 • FAX 909-793-5953 • E-MAIL info@esri.com • WEB www.esri.com

ArcGIS Enterprise Security: Delivering Secure Solutions

An ESRI White Paper

Contents **Page**

J-9450

Contents **Page**

ArcGIS Enterprise Security: Delivering Secure Solutions

Introduction

Effective enterprise security can be a challenge for the IT architects and security specialists who design, deploy, and support mission-critical solutions. While recent industry advancements, especially in the areas of Web services standards and services-oriented architectures, are helping architects to more effectively meet their security objectives, these new capabilities are also contributing to an already complex set of protocols, tools, and architectures. ESRI, the world leader in enterprise geographic information system (GIS) technology, recognizes the challenges faced by IT security professionals and is committed to providing software and solutions that leverage these advancements. ESRI is also committed to helping our customers determine how best to apply these security alternatives in their GIS solutions.

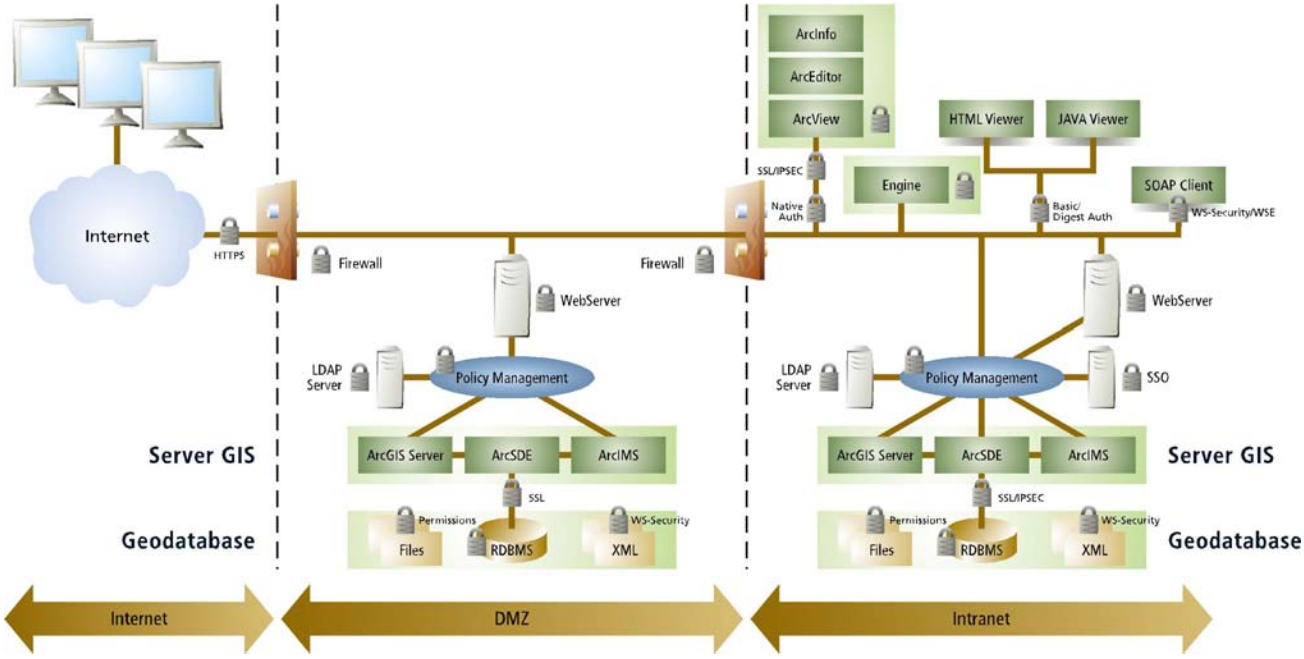
Until the last few years, entire IT systems were frequently designed around a single mission objective and "community of interest." The result was physically isolated systems, each maintaining its own data stores and applications. Integration was accomplished through complicated interfaces that replicated and synchronized data among the various systems. Security was generally enforced at the perimeter; any authorized user, once granted entry to a system, could access all data and applications, including GIS applications, resident in the system. Maintaining such "islands of automation" is expensive and inefficient and does not offer the flexibility or, in many cases, the security that organizations are seeking.

New and emerging standards, coupled with significant improvements in networking, operating systems, and integration technology, are enabling IT architects to design and maintain a single, organization-wide enterprise architecture. Discretionary access to data and applications is managed as a function of an individual's role and privileges in the organization. This flexibility affords tremendous economies and efficiencies as fine-grained access controls can be used to pinpoint information delivery to carefully drawn communities of interest. However, as security moves from the perimeter into core IT infrastructure components, GIS and other enterprise applications must be designed to exploit the new security functionality.

Nearly a decade ago, ESRI undertook a major initiative to rearchitect its GIS product line to leverage these important, emerging IT standards. We have continued to refine our software to work effectively within the new enterprise architectures and take full advantage of their inherent security capabilities, either through ArcGIS® features and custom extensions or through integration with third-party components. ESRI's careful attention to these standards and overall philosophy of providing highly interoperable

products have resulted in a very high level of flexibility for security architects that enables them to establish trust across all ESRI components contained within a solution.

ArcGIS is an open, integrated collection of software products that have been widely deployed in secure environments. Built on a single set of interoperable components, the ArcGIS framework enables you to deploy GIS functionality and logic wherever it is needed—in desktops, servers, and mobile devices and as Web services. For more specialized tasks, ArcGIS may be extended and customized using industry-standard tools. When combined with the geodatabase and, as appropriate, third-party products, ArcGIS provides the flexibility and capabilities necessary to assemble robust, secure enterprise geographic information systems.



ArcGIS technology is widely used today in secure enterprise solutions in both commercial and classified environments. Applying security controls to ArcGIS solutions is no different from securing any other IT solution. Security principles and controls can be applied at all levels of the architecture. Based on the security policies and requirements of the organization, ArcGIS security can be applied at the application, network, operating system, and RDBMS levels.

The application level provides the greatest level of flexibility of implementing security controls. Through the use of ArcObjects™, desktop applications, Web applications, and Web services can integrate with standard technologies to provide enhanced controls that authenticate, authorize, and provide access control. ArcGIS functionality can be restricted and geographic transactions can be logged for ArcGIS users with assigned privileges. ArcGIS Web applications and services can also be customized to use standard authentication methods (basic, digest, form, client certificate) over a secure channel (HTTPS). If additional security controls are required, ArcGIS applications can be

customized to integrate with policy management systems for authorization to specific content based on assigned roles. As with any other secure IT solution, application security controls are designed to integrate and enhance the secure solution.

The network level additionally provides many industry-standard network configurations that can be utilized to secure the flow of data and communication between ArcGIS components. Firewalls provide a first line of defense in that they restrict unauthorized access to ArcGIS Server components (ArcIMS®, ArcSDE®, and the RDBMS) by providing a restrictive gateway between ArcGIS clients and the ArcGIS Server components. Secure Sockets Layer (SSL) can enhance security controls by providing encrypted point-to-point security between the ArcGIS client and the ArcGIS Server components. IP security protocol (IPsec) can further enhance network layer security by providing secure exchange of packets at the Internet protocol (IP) layer. Both the header and data portions of each packet can be encrypted and decrypted between ArcGIS components that implement a common public key infrastructure (PKI).

The operating system layer of ArcGIS is additionally leveraged to provide operating system controls for authorization into ArcGIS. Operating system controls available to ArcGIS are dependent on the underlying RDBMSs support of operating system integration. ArcGIS can be configured to leverage, for example, Windows® client native authentication methods supported by the RDBMS client. On the server, data file encryption can be utilized as a security control to ensure that data on the file system is not compromised.

The RDBMS layer enhances the secure solution by providing additional confidentiality and integrity controls between the ArcGIS components and database server. RDBMS privilege assignments can be implemented to restrict access to feature datasets by allowing access to certain groups of users. Basic row-level security controls can also be implemented to restrict access, allowing only certain information to be presented to a user based on that user's assigned organizational role.

The ability of the security architect to integrate standard security practices and technology with the ArcGIS technologies determines the level of security being provided. Organizations must identify the level of control required to provide a secure solution that meets the requirements of their enterprise. ESRI continues to configure and test our products so they can be readily integrated in secure enterprise solutions.

Paper Objective and Organization

The objective of this paper is to provide the security architect with information and concepts concerning how ArcGIS software can be deployed in the enterprise as a secure component. Enterprise solutions are unique to the organizations they serve, and the security architect should use the concepts presented in this paper for planning secure solutions that meet the unique requirements of their specific GIS implementation. There is no one security tool that will meet all needs, nor is there one security design that is appropriate for all situations. As is the case with system architectures and application systems, the delivery of secure solutions is a design process, fraught with tradeoffs and demanding countless decisions. As such, the successful delivery of secure enterprise solutions requires a holistic approach to systems architecture and security design as well as a "layered" defense against those who, either accidentally or maliciously, would threaten a system's confidentiality, integrity, or availability.

As a provider of secure enterprise GIS solutions, ESRI ensures that its products integrate with other hardware and software controls to meet the basic security requirements of confidentiality, integrity, and availability. The multidimensional challenge that confronts security architects matches these basic requirements against a host of architectural alternatives and security mechanisms. This paper focuses on how architects can mitigate the threats to confidentiality, integrity, and availability of ArcGIS deployed in the most common GIS deployment architectures: client/server, Web application, and Web services. For each of these architectures, the paper outlines various security mechanisms that may be applied to mitigate these threats.

Secure ArcGIS software configurations and solutions are presented in a "pattern" format to address the threats of ArcGIS in enterprise architectures. Threats are categorized based on the goals and purposes of the attack using the Microsoft®-conceived acronym STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege). Microsoft defines the components of STRIDE as follows:

- **Spoofing:** Spoofing is attempting to gain access to a system by using a false identity.
- **Tampering:** Tampering is the unauthorized modification of data.
- **Repudiation:** Repudiation is the ability of users (legitimate or otherwise) to deny that they performed specific actions or transactions.
- **Information Disclosure:** Information disclosure is the unwanted exposure of private data.
- **Denial of Service:** Denial of service is the process of making a system or application unavailable.
- **Elevation of Privilege:** Elevation of privilege occurs when a user with limited privileges assumes the identity of a privileged user to gain privileged access to an application.

J-9450

Each solution pattern will present the ArcGIS threat, solution description, and ArcGIS mitigation of the threat.

	Threats				
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑	☑	☑

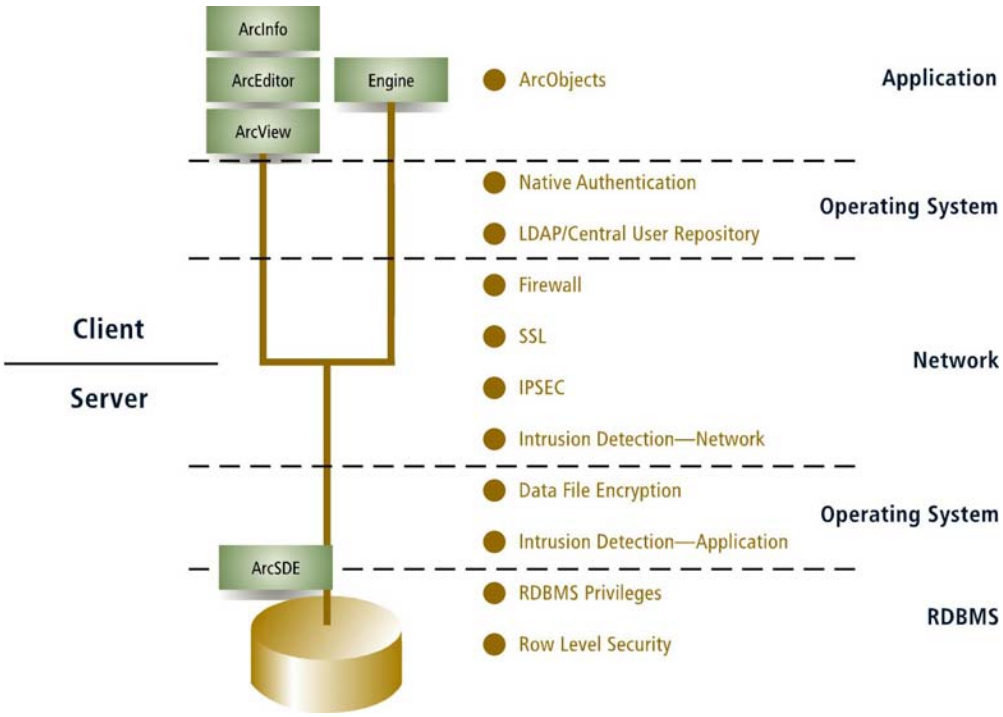
This section describes the ArcGIS solution.

ArcGIS Mitigation
Use of ArcObjects allows the developer to provide fine-grained access control to ArcGIS functionality to prevent deliberate destruction or manipulation of data (for example, preventing users from accessing the Editor toolbar) as well as unauthorized distribution (for example, copy/cut/paste/print).

ArcGIS Client/Server Architecture

The ArcGIS client/server architecture traditionally involves interaction between a user interface running on the client desktop (ArcInfo®, ArcEditor™, ArcView®, ArcGIS Engine) and centralized data source (RDBMS) managed by ArcSDE located on one or many servers. The application logic can run on either the ArcSDE/database server or ArcGIS client.

ArcGIS integrates with industry standards and technologies that provide infrastructure services. Industry best practices can be used to secure those services without impacting ArcGIS. The following security practices provide the architect with many options to secure the ArcGIS client/server architecture.



The ArcGIS security concepts presented in this section are organized into application, operating system, network, and RDBMS controls. ArcGIS application controls are mechanisms that are implemented either through ArcGIS out-of-the-box configuration or custom application enhancement (ArcObjects). Operating system controls are mechanisms that are implemented using operating system functionality and are integrated with ArcGIS through either out-of-the-box configuration or custom application enhancement (ArcObjects). Network controls are mechanisms that are implemented using standard networking techniques and practices. Finally, RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancement (using ArcObjects).

ArcGIS Application Controls

ArcGIS application controls are mechanisms that are implemented either through ArcGIS out-of-the-box configuration or custom application enhancement (using ArcObjects). The security solutions presented in this section are implemented on the ArcGIS client.

This section contains security solution concepts that mitigate threats at the application architecture level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

ArcObjects: Custom Control Extensions

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

The ArcGIS application layer in the client/server architecture consists of the out-of-the-box ArcInfo, ArcEditor, and ArcView applications as well as custom developed ArcGIS Engine applications. The security of the desktop application can be improved through the use of custom control extensions. Custom control extensions can be utilized to implement technologies such as Identity Management (IM) and access control. ArcGIS custom control extensions are developed using the ArcObjects development interface.

Using the standard out-of-the-box client ArcGIS Desktop applications (ArcInfo, ArcEditor, ArcView), the user has the ability to modify, copy, save, and print controlled assets to various forms of media that can be transported into nonsecure environments. Once accessed and downloaded locally, information is susceptible to various control risks. ArcGIS custom user interface controls can minimize these control risks using ArcObjects components-developed custom control extensions that disable standard ArcGIS interface functionality. This provides the ability to restrict ArcGIS client operations (edit, copy, save, print) that an authorized user can perform. Standard data access controls allow authorized users to access various data assets based on their role in the organization.

To control data manipulation operations, fine-grained access control is implemented in the ArcGIS application layer. ArcGIS application interface restrictions (edit, copy, paste, print) are determined based on a users' clearance or role with respect to an organizationally defined sensitivity level assigned to the data.

Additional restrictions on ArcGIS application layer functionality can be accomplished by "locking down" the control that the user has to customize the ArcGIS Desktop interface and Windows desktop environment. In this solution the user must not have the ability to customize (disable/enable) any ArcGIS extensible components. A strict Windows domain security policy must be in place to restrict desktop registry modification (software installation and configuration) and file system permission assignment.

ArcGIS Mitigation
Use of ArcObjects allows the developer to provide fine-grained access control to ArcGIS functionality to prevent deliberate destruction or manipulation of data (for example, preventing users from accessing the Editor toolbar) as well as unauthorized distribution (for example, copy/cut/paste/print).

ArcObjects: Utilize ArcObjects to Create and Store Geographic Transactions Created during the Business Process Work Flow to Provide an Audit Trail

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
		☑			

GML is an XML schema used for modeling, transporting, and storing geographic information. ArcObjects, utilizing GML and RDBMS storage functionality, offers a framework and method for auditing controls in ArcGIS multiuser geodatabase environments. A detailed history of GIS workflow activities can be recorded in a GML structure and stored in the RDBMS. In addition to recording who performed the edit, activities can be supplemented with comments and notes to provide a traceable, documented, activity log containing before-edit, after-edit, and edit justification history.

Geodatabase versioning functionality also provides many useful auditing controls. Versioned geodatabase datasets provide a controlled methodology for posting workflow edits to the default view of the enterprise database. The versioning model provides a dynamic, controlled process to post edits to a parent version. Each version represents a state or snapshot of data in a point in time. Based on user-defined business practices, edits can be reviewed by others providing quality as well as approval mechanisms.

By utilizing the GML schema in conjunction with ArcObjects and geodatabase functionality, a repeatable process can be established to investigate incidents and identify potential security vulnerabilities. Utilizing a time-stamped list of comments will log corollary information, such as issues, clarifications, and notes, related to an action for the quality control or management team. This chronological registry of edit-related information allows the enterprise architect the ability to track events back to a particular period of time and help identify potential security vulnerabilities and risks.

Note: Additional server resources and processing time are required to record and store feature edits.

ArcGIS Mitigation
Use of ArcObjects allows the developer to record user-initiated GIS transactions.

Operating System Controls

Operating system controls are mechanisms that are implemented using operating system functionality. Operating system controls are integrated with ArcGIS through either out-of-the-box configuration or custom application enhancement (ArcObjects). The security solutions presented in this section are implemented on the operating system of the ArcGIS client.

This section contains security solution concepts that mitigate threats at the operating system level. Any one concept described in this section may or may not meet all the

needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

LDAP/Central User Repository: ArcObjects Interface

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑		

Integrated operating system authentication and single sign-on (SSO) are two security infrastructures that can be leveraged by ArcObjects applications to authenticate against and connect to ArcGIS products using user names and passwords managed in a centralized location. This location can be an encrypted file, an RDBMS table, a Lightweight Directory Access Protocol (LDAP) server, or a combination of RDBMS tables and an LDAP server. The primary intent is to insulate users from having to continually authenticate themselves. This technique relies on users' authentication into their desktop workstation (integrated operating system authentication) or the organization's SSO infrastructure.

ArcObjects can be used to map a user's desktop login credentials to an appropriate geodatabase user name and password. Once the connection information has been retrieved from the user repository, a connection string is constructed and made through the ArcGIS application to the geodatabase. Information concerning the user may also include workspace properties.

ArcGIS customization to support Identity-Managed Login (IML) could also be implemented in the Add Data interface of ArcGIS clients. There are many options as to where the security administrator may request implementation of this customized interface. The organization's security policies and standards must be reviewed to determine the proper implementation.

Custom ArcGIS IML architectures are flexible with the centrally managed repositories with which they interact. A centrally managed security infrastructure, such as integrated operating system authentication or single sign-on, ensures this flexibility by providing a central location to map operating system or organizational credentials to geodatabase user names and passwords. The inability to determine the user name and password reduces the organization vulnerabilities to inappropriate access. It is also important to note that the architect should provide the necessary controls to ensure that user name/password credentials provided from these central repositories are never transmitted as clear text.

ArcGIS Mitigation
Use of ArcObjects allows the developer to interface with a centrally managed security infrastructure enforcing strong authentication and reducing the threat of identity theft by eliminating the local caching of credentials.

J-9450

Windows Native Authentication: ArcSDE and RDBMS Client

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑					☑

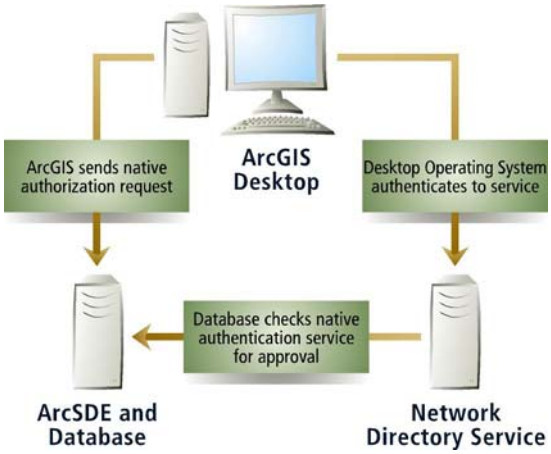
Traditional user name and password models (simple clear-text password sent over the network) introduce vulnerabilities to the security of the enterprise by transporting password information "in the clear" over the network. Utilizing trusted authentication methods using data encryption standards, strong authentication protects authentication information as it traverses the enterprise.

A common user complaint to the security architect is the wasted time involved in logging in to multiple components of a system. Each component of the enterprise system requires authentication before entry into that specific component. Security architects need a way to authenticate a user to a remote system, such as a database, based on a known, secure set of previously authenticated credentials. Strong authentication controls can be established between ArcGIS and system components through the use of native authentication allowing the user to be authorized by downstream systems. ArcSDE utilizing the direct connect architecture supports native Windows authentication from the ArcGIS client connecting to the RDBMS. The direct connect configuration allows ArcGIS clients to leverage RDBMS connectivity functionality.

Windows native authentication offers many security advantages over traditional RDBMS user name and password authentication schemes deployed in a three-tier ArcSDE architecture. Deployed utilizing a two-tier ArcSDE architecture configured with a RDBMS SSL transport layer, native authentication provides an encrypted communication channel between the trusted operating system and the RDBMS. Standard Windows security controls also provide added advantages of auditing, password aging, minimum password length, and account lockout after multiple invalid login attempts.

When a user logs on to the Windows operating system, the login mechanism confirms the user's identity to either the domain account or local computer. Domain accounts require that users log on to the network via a domain controller with a password or smart card using credentials stored in a directory service (Active Directory). A successful login to the domain account (domain controller) authorizes the user access to specified resources in the domain or other trusted domains.

J-9450



Once authenticated by the domain controller, the ArcGIS client can then log in to the RDBMS via native authentication. Over an SSL transport layer, the client submits a request for access to the RDBMS as the user that has been authorized by the domain controller. The RDBMS then permits (logged in to the domain) or denies (not logged in to the domain) login access based on that network user name alone, without requiring a separate user name and password.

Note: Currently, interoperability software (Java™ and Microsoft technologies) utilized in many ArcGIS solutions (J-Integra® for all Java applications on all platforms and Mainwin® for ArcGIS Server on UNIX®) do not support "packet privacy." Packet privacy is the practice of encrypting all data passed between the end points of a communication channel. In cases in which packet privacy is an issue, consider implementing IPsec to secure communication across platforms.

ArcGIS Mitigation
Use of native authentication eliminates the need for credentials to be unnecessarily transmitted over the network.

Network Controls

Network controls are mechanisms that are implemented using standard networking techniques and practices. Network controls are integrated based on ArcGIS configuration. The security solutions presented in this section are implemented on the network between ArcGIS components.

This section contains security solution concepts that mitigate threats at the network level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

Firewall: Restrict Communication to ArcSDE Application Server Process

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑				☑	

Firewalls should only be considered as a component of a multilayered strategy. There are many techniques commonly used in practice today to implement firewall security controls. With respect to the ArcGIS architecture, firewalls merely limit traffic between the ArcGIS client and the ArcSDE server. Packet data is still susceptible to exploitation.

At the most simplistic level, the firewall is configured to only allow communication between the ArcSDE application server and client on port 5151 (or the service port specified in the services.sde file). All communication to the ArcSDE application server from the ArcGIS client occurs on the same TCP/IP port number. After successful connection, the parent ArcSDE process transmits the port number to the child process.

For further information regarding accessing ArcSDE through a firewall, reference the "Managing ArcSDE Application Servers" documentation provided with the ArcSDE software.

For further information regarding accessing ArcSDE in the direct connect configuration, refer to the specific RDBMS documentation concerning communication to the RDBMS through a firewall.

ArcGIS Mitigation
Use of firewalls restricts ArcGIS communication to designated ports.

SSL: Establish a Secure Communication Channel between the ArcGIS Client and RDBMS Server

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

Utilizing ArcSDE in a direct connect configuration eliminates the use of the ArcSDE application tier by moving the ArcSDE functionality from the server to the ArcGIS client. By moving the ArcSDE functionality from the server to the client (dynamic link library), you enable the client application to communicate directly to the RDBMS through the RDBMS client software. ArcSDE interpretations are performed on the client before communication to the RDBMS. This provides the client application the ability to leverage network encryption controls supplied by the RDBMS client.

All four commercial databases supported by ArcSDE—IBM® DB2® Universal Database, Informix® Dynamic Server, Microsoft SQL Server, and Oracle® SQL*Plus® Database Server—provide open, standards-based network encryption protocols. Although some RDBMS vendors provide proprietary encryption controls, all RDBMSs mentioned

support SSL protocol. SSL is a protocol that communicates over the network through the use of public key encryption.

SSL establishes a secure communication channel between the client and server. Encryption functionality of the RDBMS converts clear text into cipher text that is transmitted across the network. Each new session initiated between the RDBMS and the client creates a new public key, affording increased protection.

Encryption algorithm and key lengths determine the "strength" of the encryption. Therefore, stronger encryption is constructed from larger keys. Well-known encryption algorithms contain 40- to 256-bit keys. Security best practices suggest selecting an algorithm with at least a 1,024-bit encryption key. Longer encryption keys make the task of discovering the session key and converting cipher text to clear text extremely difficult.

The ArcSDE direct connect configuration using the RDBMS encryption functionality works with ArcGIS client products accessing an RDBMS as a data store. Each software product client scenario requires that extra configuration steps be performed including client RDBMS software installation. Be sure to reference RDBMS, ArcGIS, or custom application vendor documentation to ensure that proper configuration steps have been followed.

Note: ArcGIS performance is impacted by adding the RDBMS SSL encryption processes on both the client and server. The architect may consider installing an SSL accelerator to mitigate the negative performance impact experienced by using SSL.

ArcGIS Mitigation
Use of SSL encrypts the communication between the client and server, preventing packets from being intercepted, modified, or corrupted.

IPsec: Establish a Secure Communication Channel between the ArcGIS Client and RDBMS Server

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

Another approach to securing the communication between the ArcGIS client and the RDBMS server is through the use of IPsec. IPsec is a set of protocols that secures the exchange of packets between the client and the server at the IP level.

IPsec uses two protocols to provide IP communication security controls: authentication header (AH) and encapsulation security payload (ESP). The AH offers integrity and data origin authentication. The ESP protocol offers confidentiality.

IPsec protocols are used in one of two modes: transport or tunnel. In the transport mode, AH and ESP protect the transportation headers by intercepting packets from the network layer into the transport layer. The tunnel mode is used when the destination of the packet is different from the security termination point. Essentially in tunnel mode, IPsec encapsulates an IP packet with IPsec headers and adds an additional IP header. The

additional IP header is used to account for the originating device providing the security because the final destination is beyond the security destination.

There are three basic implementations of IPsec that can deployed.

- Host Implementation (operating system)
- "Bump-in-the-Stack" Implementation (underneath IP protocol stack)
- "Bump-in-the-Wire" Implementation (router)

Implementation of IPsec is primarily an architectural choice. Implementing IPsec at the operating system levels limits the architect to the functionality provided by the operating system vendor. Windows XP, Windows 2000, and Windows 2003, for example, provide support for IPsec. Implementing IPsec underneath the IP stack or at the router levels provides the architect with flexibility, allowing integration with other controls such as firewalls and filters.

Providing confidentiality controls for ArcGIS, the ESP protocol of IPsec should be utilized to allow for encryption of packet contents. Depending on the depth of the client/server architecture, transport mode can be utilized for ArcSDE direct connect architectures and tunnel mode can be used for the ArcSDE application server when the application server is deployed on a separate server from the RDBMS. Implementation of IPsec should be driven by the existing operating system, architecture components, or enterprise security standards.

To provide integrity controls for ArcGIS, the AH protocol of IPsec creates and verifies an encrypted checksum for each packet transferred. Depending on the depth of the client/server architecture, transport mode can be utilized for ArcSDE direct connect architectures and tunnel mode can be used for the ArcSDE application server when the application server is deployed on a separate server from the RDBMS. Implementation of IPsec should be driven by the existing operating system, architecture components, or enterprise security standards.

ArcGIS Mitigation
Use of IPSEC provides a private communication channel between the client and server, preventing packets from being intercepted, modified, or corrupted.

Intrusion Detection: Monitor ArcGIS Infrastructure to Identify Suspicious Patterns that Might Identify Malicious Activity

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
				☑	

There are two primary types of intrusion detection systems available to ArcGIS users: network-based intrusion and host-based intrusion. Network-based intrusion detection involves analyzing network packets as they flow through the network. Network-based intrusion detection identifies malicious packets based on triggering events. Host-based intrusion detection monitors operations on a specific host. Network traffic as well as application executable characteristics can be monitored.

ArcGIS Server components (ArcSDE, ArcIMS) can utilize host-based intrusion detection systems. For example, architects can configure host-based intrusion detection systems to monitor predetermined application executable sizes and standard ArcGIS communication patterns to and from the host. Host-based intrusion can also be configured to watch for operating system-specific attacks. Should the host-based intrusion detection system a software executable change (checksum) or irregularities in communication to and from the geodatabase, an alert can be logged or sent to the enterprise administrator. Based on logs and alerts, swift, appropriate actions can be taken to identify and isolate issues.

ArcGIS Mitigation
Use of intrusion detection systems provides a mechanism to monitor network communications in an effort to identify and prevent the execution of known malicious code.

RDBMS Controls

RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancement (ArcObjects). The security solutions presented in this section are implemented in the RDBMS.

This section contains security solution concepts that mitigate threats at the RDBMS level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

Feature-Level Security: Restrict Access to Rows of Attribute Data in the Geodatabase Based on Organizational Responsibility or Role

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑				

DB2 Universal Database, Oracle Database Server, and SQL Server all support varying degrees of feature-level security either in current or future releases. Geodatabase features are synonymous with RDBMS rows.

Implementing feature-level security in parallel with ArcSDE allows organizations to assign privileges at the feature level, restricting data access within the geodatabase object. Feature-level security in all RDBMSs is based on the concept of adding a column to a table that assigns a sensitivity level for that particular row. Based on the value in that column, the RDBMS determines, through an established policy, whether the requesting user has access to that information. If the sensitivity level is met, the RDBMS allows access to the data; otherwise, access is denied.

The use of feature-level security integrated with ArcGIS can be best illustrated through an example of a government agency and its classification of hazardous material locations. The government agency has developed an ArcIMS application that allows individuals to

log in and view hazardous material sites in their area of responsibility. Depending on the types of hazardous materials stored at a site, it may be necessary for some agencies to be aware of the hazardous materials location and others not to. For example, local government agencies in state A may need to view all local chlorine sites but do not need other state locations.

To minimize the access to hazardous material sites and the possibility of this information being used in a malicious manner, data can be classified in a manner in which certain data is only shared with certain individuals. The government agency has chosen to utilize its RDBMS feature-level functionality. For each hazardous site, a sensitivity level has been placed on the record, designating the group of individuals that has access to view the data.

OBJECTID	Site Name	State	Class	Material	Capacity (Units)	Sensitivity
1	Bobs Pool Supply	FL	Oxidizer	Chlorine	12000	FL1
2	Joe's Chemicals	FL	Unstable	Acetylene	2200	FL3
3	Acid-Mart	FL	Polymerizing	Acrylic Acid	1200	FL2
4	Wholesale Chemicals	FL	Oxidizer	Chlorine	24000	FL1
5	Cleaning Clearinghouse	FL	Oxidizer	Nitric Acid	10000	FL1

As users access this information via ArcIMS, Florida government agencies assigned a sensitivity level of FL1 are granted access to view the least hazardous material sites containing oxidizer classified materials designated as FL1.

OBJECTID	Site Name	State	Class	Material	Capacity (Units)	Sensitivity
1	Bobs Pool Supply	FL	Oxidizer	Chlorine	12000	FL1
4	Wholesale Chemicals	FL	Oxidizer	Chlorine	24000	FL1
5	Cleaning Clearinghouse	FL	Oxidizer	Nitric Acid	10000	FL1

The same view to a Florida government agency that is granted access to view all classifications of materials will display FL1, FL2, and FL3 sensitivity designated data.

OBJECTID	Site Name	State	Class	Material	Capacity (Units)	Sensitivity
1	Bobs Pool Supply	FL	Oxidizer	Chlorine	12000	FL1
2	Joe's Chemicals	FL	Unstable	Acetylene	2200	FL3
3	Acid-Mart	FL	Polymerizing	Acrylic Acid	1200	FL2
4	Wholesale Chemicals	FL	Oxidizer	Chlorine	24000	FL1
5	Cleaning Clearinghouse	FL	Oxidizer	Nitric Acid	10000	FL1

Feature-level security is based on an assignment made to each row of data. Protection is determined based on the sensitivity assigned. The lowest value represents the lowest

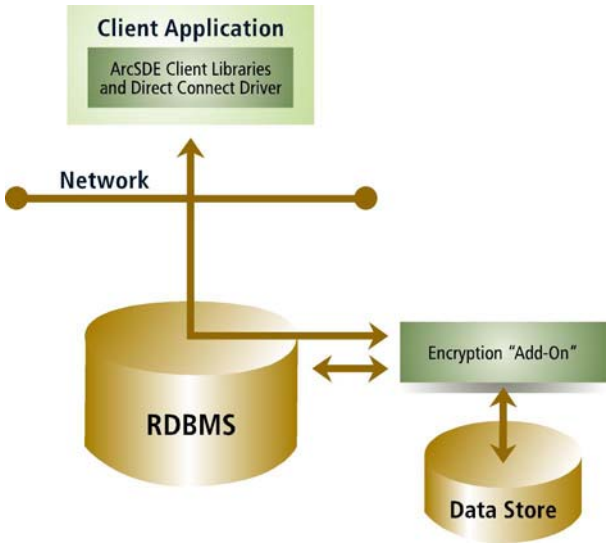
level of protection. Users are granted access to data based on the level assigned by the RDBMS administrator to their role.

ArcGIS Mitigation
Use of feature-level security provides an organizational-based mechanism that restricts a user's ability to access and manage data.

Data File Encryption: Encrypt ArcGIS Data Stored on Disk in the RDBMS

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

RDBMS functionality is becoming more available to encrypt data stored at the operating system layer. There are many commercially available products available to manage the process of encrypting data at the data file level. Most encryption management products are based on the execution of functions and stored procedures upon a triggering event. Data is initially loaded into alternate database tables and encrypted based on an object key. Once the data has been migrated, a view is created in place of the original table name. Database triggers are then created on the view so INSERT, UPDATE, and DELETE operations can be performed on the encrypted data.



At the row level, additional unique encryption keys with limited life spans exist, resulting in a unique encryption key for each column and row in the database. Encryption key algorithm is configurable, and reencryption of existing data is typically supported.

The ArcSDE direct connect architecture using a data encryption "add-in" in the RDBMS works with ArcGIS products accessing an RDBMS as a data store, custom ArcObjects applications, and custom non-ESRI technology-based applications using the ArcSDE C and Java APIs to access nonversioned data. Each software product scenario requires that extra configuration steps be performed including client RDBMS software installation and

additional add-on RDBMS installation. Be sure to reference RDBMS, ArcGIS, data encryption add-on vendor, or custom application vendor documentation to ensure that proper configuration steps have been followed.

ArcGIS Mitigation
Encrypting data stored in RDBMS data files on the file system prevents data from being mined by unapproved methods.

RDBMS Privileges: Restrict Access to Geodatabase Datasets Based on Organizational Responsibility or role

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑				

Out of the box, the geodatabase provides the functionality to assign certain privileges to tables, feature classes, and feature datasets. After the geodatabase dataset has been created, the ArcSDE administrator can assign privileges to other users or roles (inherently, the geodatabase object owner has full control of the geodatabase datasets it creates) either via command line or through the ArcCatalog™ application. With respect to the RDBMS, geodatabase datasets are a logically grouped set of tables. The RDBMS supports assigning SELECT, UPDATE, INSERT, and DELETE privileges to either a user or role. The ArcSDE command line and ArcCatalog leverage the RDBMS privilege assignment functionality and provide an interface that allows the administrator to assign privileges.

- SELECT: The user/role may query the designated object(s) data.
- UPDATE: The user/role may modify the designated object(s) data.
- INSERT: The user/role may add new data to the designated object(s).
- DELETE: The user/role may delete data from the designated object(s).

In role-based access control, permissions are associated with roles and roles are assigned to users. Once roles are established in the RDBMS, the management of object permissions is simplified as a user can be assigned zero to many roles. This provides the ability to easily manage access to geodatabase datasets based on the user's role in the organization. Role permissions can be granted and revoked at the RDBMS level, providing central security policy management as new objects are incorporated into the geodatabase.

ArcGIS Mitigation
Use of RDBMS privileges provides a role-based mechanism that restricts a user's ability to access and manage data.

J-9450

Intrusion Detection: Establish a Mechanism to Restrict and Detect When the Geodatabase Is Accessed by Unauthorized Applications

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
				☑	

Successful intrusion detection systems are composed of the functionality to monitor and the policies to regulate the enterprise system. Security policy management involves identifying the software, users, and assets that you wish to permit or deny access. Once identified, mechanisms can be put in place to monitor use of the enterprise system and reduce system vulnerabilities.

ArcGIS geodatabase solutions are deployed using standard COTS relational database management systems. The use of commercially available systems provides users with many options for accessing data in the database. It may be necessary to restrict access to the geodatabase by ArcGIS clients to ensure that the business process work flow is maintained. For example, an organization may wish to only allow geodatabase edits from either standard ArcGIS software or custom applications developed with ArcObjects. Limiting users to ArcObjects components-based applications ensures that geodatabase integrity is maintained.

Limiting geodatabase access can be implemented in two phases: prevention and detection. Prevention consists of instituting a security policy on the desktop to ensure that users are not allowed to use or download commercially available database access products such as Oracle SQL*Plus. Detection involves creating database objects that monitor system tables to log application access to the database.

The prevention step involves implementing strict desktop configuration control. File system access should be controlled based on the user's role in the enterprise. If certain applications are available on a corporate desktop and are considered a potential threat to the geodatabase, then those applications must be restricted from being accessed by certain geodatabase users. In addition to file system and application control, strict download policies must be incorporated.

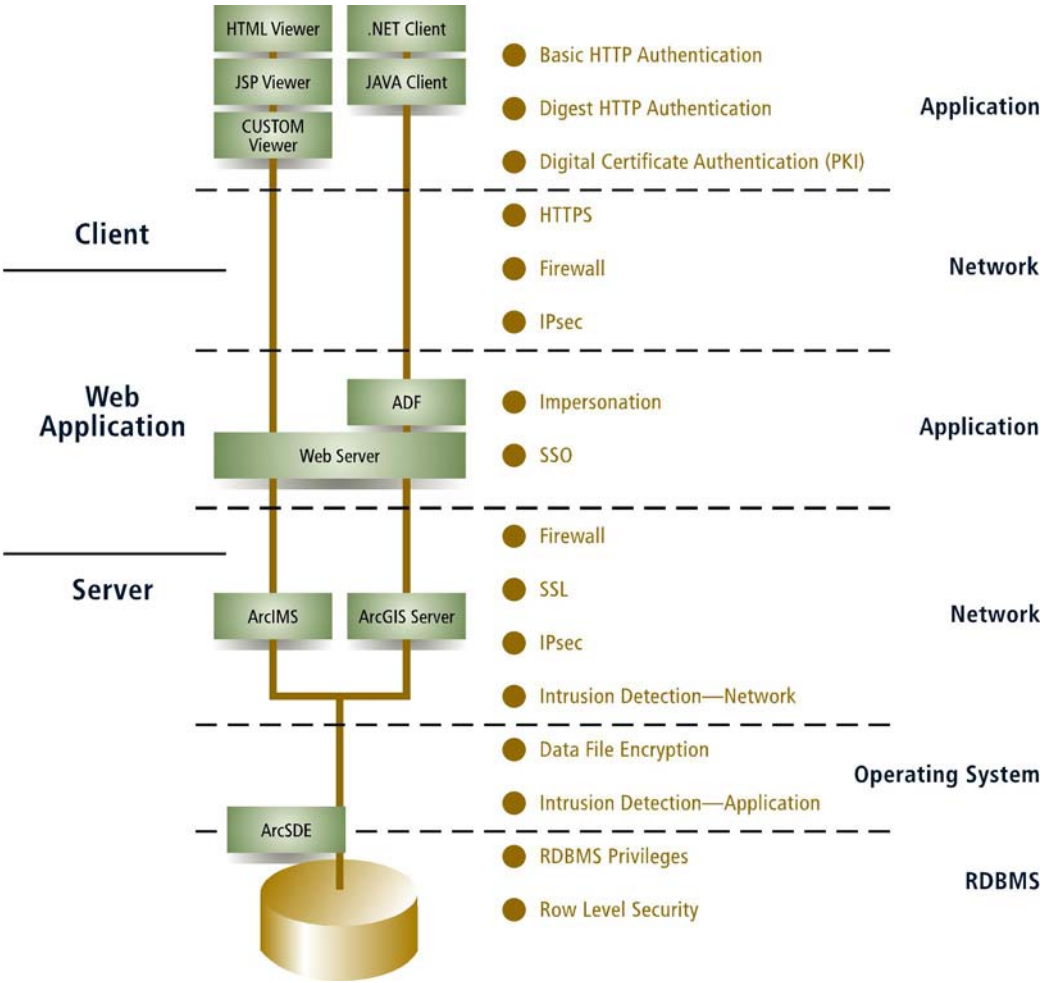
The detection step involves developing database objects that monitor system tables that log access to the database. Objects should be constructed to monitor the system tables, watching for access by a predetermined list of applications. If access is detected by an unauthorized application, the object should log that intrusion, and then terminate the RDBMS session corresponding to that application.

ArcGIS Mitigation
Use of custom intrusion detection systems provides a mechanism to monitor data access in an effort to identify and prevent the unapproved access to data.

ArcGIS Web Application Architecture

The Web application architecture traditionally involves an HTML, .NET, or Java-based browser user interface accessing centralized application logic (ArcIMS, ArcGIS Server, ArcSDE) located on one or many servers utilizing a centralized data source.

ArcGIS integrates with industry standards and technologies that provide infrastructure services. Industry best practices can be used to secure those services without impacting ArcGIS. The following security practices provide the architect with many options to secure the ArcGIS Web application architecture.



Although not the primary subject of this paper, it is also important to note that Web Map Services (WMS) can also be secured. WMS is an Open Geospatial Consortium, Inc. (OGC), standard for producing "maps of spatially referenced data dynamically from geographic information" and is supported by both ArcIMS and ArcGIS Server. WMS services are utilized for their abilities to produce standardized maps from numerous sources. These sources are accessed via URLs that produce maps using a predefined style. Essentially, each URL produces a layer to the resulting image requested by the user of the WMS. Although many of the concepts presented in the ArcGIS Web

application and Web services architecture sections of this paper can be applied to Web Map Services, it is recommended that you proceed with caution as the real benefit of WMS services is the collective use of distributed mapping and data services across enterprises.

The ArcGIS security concepts presented in this section are organized into application, network, and RDBMS controls. ArcGIS application controls are mechanisms that are implemented either through ArcGIS out-of-the-box configuration or custom application enhancement (using ArcObjects). Network controls are mechanisms that are implemented using standard networking techniques and practices. Finally, RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancement (using ArcObjects).

ArcGIS Application Controls

ArcGIS application controls are mechanisms that are implemented either through Web application standards and protocols or through ArcGIS out-of-the-box configuration. The security solutions presented in this section are implemented in the ArcGIS Web client.

This section contains security solution concepts that mitigate threats at the application architecture level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

Standard HTTP Authentication: ArcGIS Web Application Authentication

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑					☑

Simply stated, HTTP authentication is a mechanism by which an HTTP authentication method is used to verify that someone is who they claim to be. The standard methods of HTTP authentication integrated with ArcGIS Web applications are the basic, digest, form, and client certificate methods. Basic authentication involves protecting an HTTP resource and requiring a client to provide a user name and password to view that resource. Digest authentication also involves protecting an HTTP resource by requesting that a client provide user name and password credentials; however, the digest mechanism encrypts the password provided by the client to the server. Form-based authentication is identical to basic except that the application programmer provides the authentication interface using a standard HTML form. Client certificate is the most secure authentication method in that it uses the organizational PKI environment to provide and authenticate digital certificates for both client and server.

It is important to note that HTTP is a stateless protocol. Every resource requested from the server that is protected will require authorization credentials. Even though Web browser-based clients do provide some caching of user name and password on a per-session basis, great care should be taken to determine which resources to protect.

If an HTTP resource has been protected by an authentication method, the HTTP server replies to the client with a "401 Authorization Required" header. If the Web application uses HTTP basic authentication, the browser client responds to this header by providing the user with a user name/password dialog box for providing credentials. The user name/password provided by the client is compared to a password list (password file) stored on the HTTP server to determine whether the user is who he/she claims to be. Once authorized, the HTTP server provides a realm name associated with the parts of the ArcGIS Web application that are protected. The realm name is used by the browser to cache the user name/password realm association and use it to respond to subsequent 401 Authorization Required headers.

One of the major drawbacks to implementing basic and form HTTP authentication with ArcGIS Web applications is that these HTTP authentication methods send user name and password information between the client and server in the clear. Digest authentication works the same as basic authentication; however, digest authentication addresses the drawback of basic HTTP authentication by encrypting the password returned by the client.

For information concerning the encryption used by digest HTTP authentication, reference the Internet standards document Request for Command 2617.

It is important to note that digest HTTP authentication may not meet all requirements of an enterprise's secure solution. There are many security aspects that digest HTTP authentication does not address. It is also important to note that Web server implementations of HTTP authorization may differ. Refer to Web server documentation for specific instructions in implementing HTTP authentication.

ArcGIS Mitigation
Use of basic and digest authentication provides secure credential management between the client and authorizing agent.

Single Sign-On: Integrate ArcGIS Web Applications with Single Sign-On Systems

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑		☑

Single sign-on systems are growing in popularity across organizations. Integration of ArcGIS applications and single sign-on systems can provide a secure authorization mechanism through open standards such as Security Assertion Markup Language (SAML). SAML ensures that all communication with the centrally managed repository is secure.

The Organization for the Advancement of Structured Information Standards (OASIS) defines SAML as "an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. A typical example of a subject is a person, identified by his or her e-mail address in a particular Internet Domain Name Services. Assertions can convey information about authentication acts performed by subjects, attributes of subjects, and authorization decisions about whether subjects are allowed to access certain resources. Assertions are represented as XML constructs and have a nested structure, whereby a single assertion might contain several different internal statements about authentication, authorization, and attributes. Note that assertions containing authentication statements merely describe acts of authentication that happened previously. Assertions are issued by SAML authorities, namely authentication authorities, attribute authorities, and policy decision points. SAML defines a protocol by which clients can request assertions from SAML authorities and get a response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols; SAML currently defines one binding, to Simple Object Access Protocol (SOAP) over HTTP. SAML authorities can use various sources of information, such as external policy stores and assertions that were received as input in requests, in creating their responses. Thus, while clients always consume assertions, SAML authorities can be both producers and consumers of assertions."

Similar to the custom ArcObjects solution, the single sign-on solution contains a centrally managed repository that stores user database connection properties. Database connection properties are managed in the central repository as user attributes and are unknown to the user of the client application. Once password information has been obtained, the users log in to the geodatabase as themselves, allowing for identifiable access into the geodatabase.

SAML provides the enterprise architect with four primary advantages: cross-domain authentication standard, cross-domain single sign-on standard, standard authentication and authorization between Web services, and federated identity managed login.

ArcGIS Web applications integrate seamlessly with SSO systems the same as any other Web application being protected by an SSO system. Web deployment descriptor information is updated to redirect Web server requests to single sign-on components. SSO authentication is configurable and supports a wide range of authentication methods such as SAML, X509, two-factor tokens, and smart cards. Once authenticated, the SSO system evaluates the user-driven security policies and determines if the user has access to a specific resource. If the resource is protected and the user has been authorized for it, then the SSO system permits the Web server to fulfill the request.

ArcGIS Mitigation
Integrating with a single sign-on management system provides centrally managed mechanisms that perform strong authentication and authorization, support digital signatures, encrypt sensitive data, and support privilege management.

Access Control List: Restrict Access to ArcIMS Map Services Using an Access Control List

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑				

ArcIMS provides two methods for restricting access to map services through the servlet connector using access control lists (ACLs). The first method uses an ArcXML text file stored in the installation directory of the Servlet Engine. The second method utilizes a Java Database Connectivity (JDBC) connection to a database.

The primary advantage of a file-based ACL is its simplicity to manage. The file-based ACL can be created and managed using any text-based editor such as Microsoft Notepad or Linux® vi. ACL files contain user names and passwords of users that are authorized to utilize certain map services. The contents of the ACL file are loaded into memory at the time the servlet initializes. This requires a restart of the servlet engine for changes to take effect. For more information concerning file-based ACLs, reference your ArcIMS help documentation under "Enabling authentication with a file-based ACL."

Using a JDBC connection to a database provides the flexibility of maintaining a dynamic access control list without restarting the servlet engine. The database-driven ACL consists of two tables: ACL_USERS and ACL_PERMISSIONS. The ACL_USERS table assigns a unique identifier to each user as well as an application user name and password. The ACL_PERMISSIONS table associates users with available map services being provided by the current ArcIMS system. For more information concerning JDBC-based ACLs, reference your ArcIMS help documentation under "Enabling authentication with a JDBC-based ACL."

Note: An ArcIMS ACL cannot be used in conjunction with any additional security controls provided with your Web server software. Although simple to manage, ACLs should not be used when more robust security functionality is required by the organization and provided by the Web server software. ESRI does not recommend use of file-based ACLs, in production environments as the primary authentication mechanism.

ArcGIS Mitigation
Use of ArcIMS application control lists prevents unauthorized access to data.

Digital Certificate Authentication: Securing ArcGIS Web Applications Authentication Using PKI

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑		☑

Digital certificates are electronic documents used to identify people and resources over a network and are used as a basis for secure, confidential communication using encryption.

Digital certificates are issued by a third party or organizational Certification Authority (CA) and typically include the following information about its owner:

- Name of the Holder
- Holder's Public Key
- Name of the Certificate Authority that Issued the Certificate
- Serial Number
- Lifetime of the Certificate

Information provided in the digital certificate is digitally "signed" by the certificate authority. Any alteration of this information will void the CA's signature and render the digital certificate untrusted.

Digital certificate authentication uses HTTP over SSL to authenticate both client and server using a pair of public and private keys to encrypt/decrypt information. Communications encrypted with a public key can only be decrypted with its corresponding private key and vice versa. Digital certificates provide a mechanism to bind your identity (information verified by a third-party CA) with your public key.

ArcGIS software-developed Web applications can be integrated with third-party products that provide centralized authentication management. Centralized authentication management takes authorization out of the application logic and places it in a central authority. The central authority authenticates the validity of the digital certificate and authorizes access to the ArcGIS Web application. Once authorized, the central authority determines which application functionality is presented to the user based on that user's membership in a role. Subsequent encryption and decryption between the client and the ArcGIS Web application is performed based on the public and private key pairs provided by the digital certificate.

ArcGIS Mitigation
Use of digital certificate authentication can be integrated with other secure solutions to protect a user's identity from compromise.

Network Controls

Network controls are mechanisms that are implemented using standard networking techniques and practices. Network controls are integrated based on ArcGIS configuration. The security solutions presented in this section are implemented on the network between ArcGIS components.

This section contains security solution concepts that mitigate threats at the network level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

J-9450

ArcGIS Security Solutions

Firewalls: Restrict Access to ArcGIS Components Accessed through ArcIMS Using Advanced Network Configurations

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
				☑	

Advanced network configurations are controls at the network level that filter outgoing and incoming traffic into a network. Typically, this is accomplished by restricting or allowing communication to different port assignments. Varying levels of security can be achieved by placing advanced network configurations at various points on the network. The control establishing rules for communications over specified ports by restricting access is referred to as a firewall.

When restricting access to an enterprise system where an ArcIMS application is deployed, use of the firewall is merely a component of the overall security strategy. There are three standard firewall configurations for ArcIMS, each providing a different level of security.

- Firewall between the Network and the Web Server

The recommended technique for configuring a firewall with ArcIMS is to place the firewall between the Internet connection and the Web server. In this configuration, the Web server port (typically port 80) is configured to receive requests. All other port requests are restricted and are not allowed to be fulfilled. The primary advantage of this configuration is that all application components of the system are behind the firewall and cannot be accessed directly.

- Firewall between the Web Server and ArcIMS Application Server

A slightly more complex configuration is the placement of the firewall between the Web server and the ArcIMS application server. In this configuration, the ArcIMS application server's communication port (usually port 5300) is configured to receive requests through the firewall, enabling Web server communication with ArcIMS. When publishing Image Map Services, it is important to either mount the output drive for the Web server on the ArcIMS server or enable image streaming so images can be displayed by the Web server. When mounting the output drive, special considerations should be made to address the vulnerabilities of mounting an external drive to a server.

- Demilitarized Zone (DMZ)

The DMZ is a network established to physically separate the main internal network from the Internet. The machines in the DMZ can be accessed from the Internet but do not have access to the machines on the internal network. If a network breach occurs in the DMZ, then damage is limited to the machines in the DMZ.

A more common DMZ configuration is to place a second firewall between the DMZ and the internal network. Restricted access from the DMZ to the internal network is allowed (for example, opening port 5151 to access an ArcSDE instance on internal network). This configuration isolates DMZ servers from the internal network while allowing network administration to be performed from the internal network. The primary advantage of the DMZ configuration is that it provides a buffer between external and internal systems, providing a greater level of security between the external and internal networks.

Reverse proxies can be used in conjunction with firewalls to reduce the risk of external threats. Reverse proxies act on behalf of the HTTP server, brokering requests to internal servers to fulfill a user's request for information. Client browsers on the Internet can only see the reverse proxy server, and internal network servers are only allowed access from the reverse proxy server. Placing a reverse proxy in the DMZ can further mask the locations and addresses of the servers that fulfill client requests.

ArcIMS firewall information can be found in the *Security and ArcIMS* white paper available from the ESRI Support Web site.
http://support.esri.com/index.cfm?fa=knowledgebase.whitepapers.viewPaper&PID=16&MetaID=229

ArcGIS Mitigation
Use of firewalls restricts ArcGIS communication to designated ports.

IPsec: Secure the Communication Channel between ArcIMS and ArcSDE across Platforms

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

Some enterprises deploy enterprise server components on separate platforms. For instance, the ArcIMS server is commonly deployed on a Windows platform and the ArcSDE and RDBMS is deployed on a UNIX platform. Having enterprise components on different platforms can often introduce implementation hurdles specifically in the way the application logic utilizes operating systems based controls for security.

Refer to the IPsec discussion presented in the Client/Server Architecture section.

ArcGIS Mitigation
Use of IPsec provides a private communication channel between the client and server, preventing packets from being intercepted, modified, or corrupted.

HTTPS: Securing ArcGIS Web Applications with HTTPS

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

HTTPS provides many secure enhancements to the standard HTTP protocol utilized to communicate between client and servers. HTTPS is symmetric and provides similar functionality to requests and replies while supporting the implementation characteristics of standard HTTP.

In an HTTPS transaction, a Web server sends the Web client a server certificate that both identifies itself and gives the Web client a means to encrypt information it receives. To identify itself, the server refers to a Certification Authority that can validate its authenticity.

ArcIMS supports the use of HTTPS with minimal configuration. The initial step is to ensure that the Web server being utilized by ArcIMS is configured to serve HTTPS. Refer to your Web server's documentation for specific instructions on serving HTTPS Web pages. Other steps include updating your existing ArcIMS services to reflect the use of HTTPS and updating all HTML (ArcIMSParam.js) and Java (default.axl) viewer configuration files. Refer to the ESRI Support Center document "HOW TO: Configure ArcIMS to Work with HTTPS" (http://support.esri.com/index.cfm?fa=knowledgebase.techArticles.articleShow&d=21669) for more detailed instructions.

ArcGIS Mitigation
Use of HTTPS encrypts the communication between the client and server, preventing packets from being intercepted, modified, or corrupted.

RDBMS Controls

RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancements. The security solutions presented in this section are implemented in the RDBMS.

RDBMS layer security controls span all ArcGIS architectures. Typically, the RDBMS is central to the enterprise. All application architectures utilize a geodatabase. The most important aspect of utilizing RDBMS layer controls is understanding how your Web application accesses the central data store. Whether through an application database user or as an individual account, you must ensure that the user accessing the data has the proper permissions to access the data.

Reference the RDBMS layer controls described in the client/server architecture for further information concerning RDBMS layer controls for the Web application architecture.

ArcGIS Web Services Architecture

There are inherent operational differences between a Web application and a Web service. Web applications typically are designed to meet the requirements of a user from a thin client (browser). Web services, on the other hand, typically are designed to provide functionality to other applications or objects. Web services exchange requests for activities to be performed against some resource via messaging.

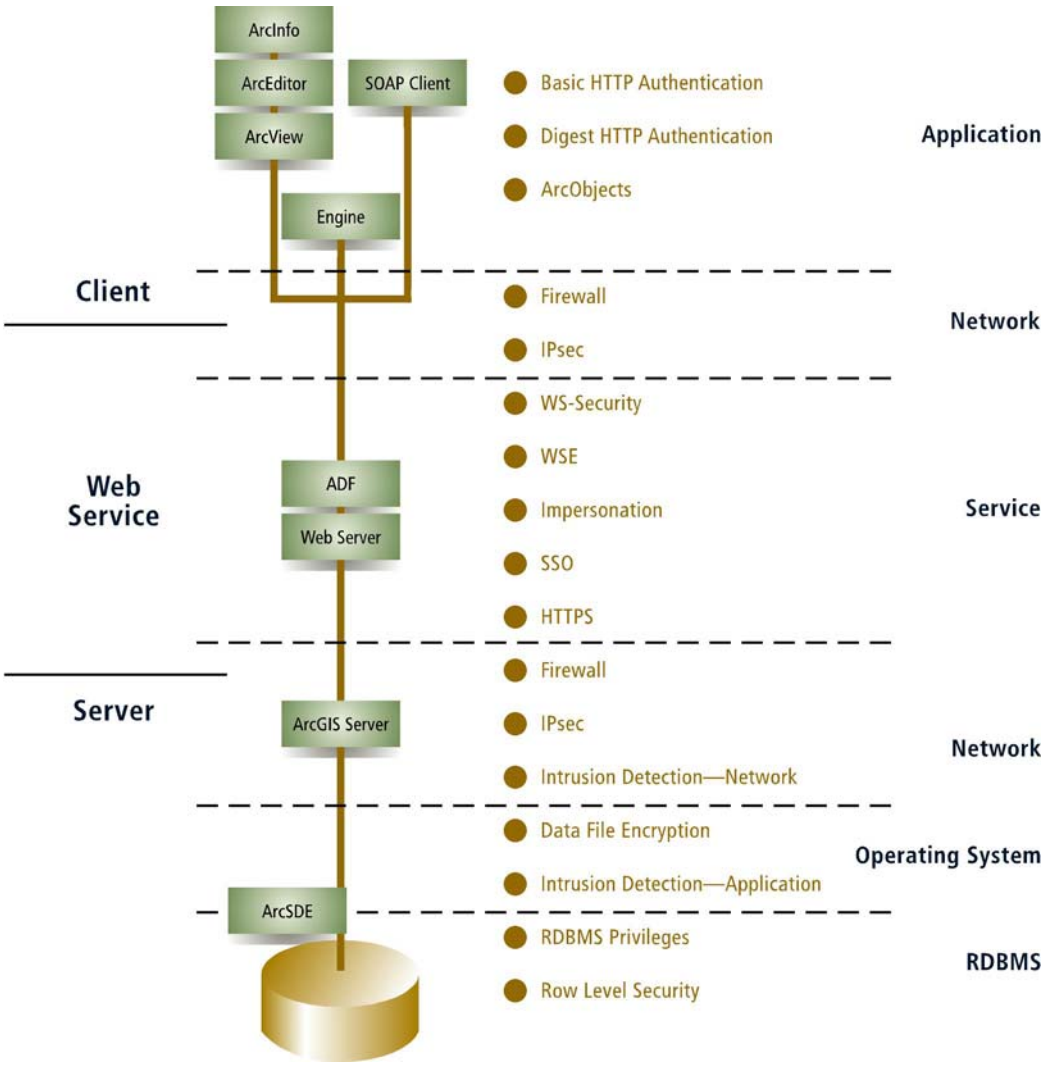
For the purposes of this paper, Web services described are SOAP based. SOAP is the messaging framework that defines a suite of XML elements to communicate to arbitrary systems. Web services are discovered using Universal Description, Discovery, and Integration (UDDI). UDDI is a metadata structure that categorizes Web services. Once discovered, the Web Services Description Language (WSDL) is read to understand how to call and invoke services. The WSDL is simply a standards-based XML file readable across platforms.

The differentiation between standard Web services and ArcGIS Web services is that ArcGIS Web services return ArcObjects instead of native object types from server objects running within the server. The primary development framework for creating ArcGIS software-based Web services is the .NET and Java Application Development Framework (ADF) provided by ArcGIS Server. ArcGIS Server is a distributed system consisting of several components that can be distributed across multiple machines. Each component in the ArcGIS Server system plays a specific role in the process of managing, activating, deactivating, and load balancing the resources that are allocated for a given server object or server objects. ArcGIS Server provides the framework to build and deploy centralized GIS applications and services to meet a variety of needs using a variety of clients. The power of ArcGIS Server is the ability to remotely execute core ArcObjects against the geodatabase.

ArcGIS Web service developers utilize the Web controls and templates of the .NET and Java ADF to build applications that communicate with an ArcGIS Server. On the Web server, ArcGIS Server Web services, each containing a distinct HTTP end point, expose ArcObjects running in the ArcGIS Server for access across the Internet. A Web service catalog can exist for each ArcGIS Server, defining ArcGIS Web services and their respective accessible URLs.

The following security controls provide the architect with many options to secure the ArcGIS Web services architecture.

J-9450



The ArcGIS security concepts presented in this section are organized into application, network, and RDBMS controls. ArcGIS application controls are mechanisms that are implemented either through an ArcGIS out-of-the-box configuration or custom application enhancement (ArcObjects). Network controls are mechanisms that are implemented using standard networking techniques and practices. Finally, RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancement (ArcObjects).

ArcGIS Application Controls

ArcGIS application controls are mechanisms that are implemented either through Web service standards and protocols or through ArcGIS out-of-the-box configuration. The security solutions presented in this section are implemented in the ArcGIS Web service.

J-9450

This section contains security solution concepts that mitigate threats at the application architecture level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

Securing Java Web Services with Standard HTTP Authentication

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑					☑

As previously discussed in this document, Java-developed Web services can also be secured at the application level using standard HTTP authentication.

The initial step to ensuring that ArcGIS services are secure is defining user access and roles. Defining user access and roles involves identifying which Web services are available for consumption by users who own membership in a designated role. The security realm is utilized by Web and application servers to protect objects and services. The security realm is the database of roles, users, and groups that identifies valid users of the object or service. Role membership allows access to objects or services in a realm.

Once security realms and roles have been established for your Web server, it is important to assign security elements to your Web service catalog. This is accomplished by updating the Web service catalog's deployment descriptor (Web.xml). The deployment descriptor for the Web service catalog defines the security role authorized to access the service and the type of authorization required (basic, digest, form, client certificate).

ArcGIS Mitigation
Use of standard authentication provides secure credential management between the client and authorizing agent.

Securing .NET Web Services with Standard HTTP Authentication

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑					☑

Securing .NET Web services with standard HTTP is conceptually the same as securing Java Web services. The primary difference between .NET and Java Web services is that .NET Web services are aware of Windows security settings.

Once the Web services catalog has been created, .NET Web services provide you with three authentication methods: digest, basic, or integrated Windows. Basic and digest authentication leverage Windows security settings to determine which users can be authenticated. Default domain and realm are specified in the authentication methods

dialog to guide Windows to the user store for authentication. Integrated Windows authentication uses the domain controller to authenticate the user name and password. This enables the security architect to use centralized mechanisms such as active directory.

As discussed earlier in this document, use of custom (form-based) authentication is an option for securing .NET-based Web services; however, the introduction of the custom mechanism no longer permits the administration of Web service catalogs from ArcCatalog or any other ArcGIS Engine application. Additional custom development will be required to administer the Web services catalog.

ArcGIS Mitigation
Use of basic and digest authentication provides secure credential management between the client and authorizing agent.

Securing ArcGIS Java Web Services with Native Security Policy Management Capabilities Found in the Web Application Server and Providing Authorization to Specific Content Based on Assigned Role

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑		☑

The concept of securing ArcGIS Java Web services using basic and digest authentication can be taken one step further by altering Web service application code to take advantage of membership in a security realm and assignment of role to authorize specific Web service content.

Assume, for example, that you wish to modify the DynamicLayers sample Web service provided as part of the ArcGIS Server Software Development Kit. For the sake of this example, assume the use of a commercial Web application server. Commercial Web application servers have identity management components that manage user identities and roles. Two roles are created to demonstrate how layers provided by the service can be accessed by specific users. The first role, the "Administrator" role is granted access to all data elements of the Web service. The "Customer" role is granted access to a designated subset of data elements. Two users are created, "Admin" and "Customer," and assigned to the newly created roles.

The next step involves creating an authorization policy for the ArcGIS Server DynamicLayers Web service application. The Admin role is allowed to see four layers, whereas the Customer role is only allowed to see two of the four administrative layers. In the Web service application code, distinct text-based CATALOG_FILEs are identified for each role in the security realm. The CATALOG_FILE for the Admin role contains all four data layers, and the CATALOG_FILE for the Customer role only contains the designated subset. Additional Web service application logic is included to associate CATALOG_FILEs with the appropriate role assigned to the authenticated user.

As with any secure Web services, the deployment descriptor must also be updated to reflect the security role and authentication method. This maps the URL or Web service resource membership in a realm. It is important to note that if the security policy utilizes a form-based authentication method, the Web service can no longer be administered by ArcCatalog or any ArcGIS Engine application. Additional development must be

performed to administer the Web service protected by form-based authentication methods.

ArcGIS Mitigation
Integrating with a policy management system provides centrally managed mechanisms that perform strong authentication and authorization, support digital signatures, encrypt sensitive data, and support privilege management.

Impersonation: Mapping External Web Users to ArcGIS Users

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑				

Impersonation is a technique used to simulate a user that is logged on the server while performing protected operations. Basically, the execution of the requested operation will execute in the context of the logged-in user, with privileges granted to the user's identity and not those of the service. Impersonation can occur for the entire execution of the session or for only a part of the execution. For example, impersonation can be set to occur only during the access of a database but not when accessing files on the file system.

Impersonation can be utilized at the service level. Impersonation controls can be developed through the .NET or Java components. .NET's impersonation features are integrated closely with the Windows process identity. Impersonation in .NET will result in the Web application's Windows execution thread utilizing the security token of the calling Web application's calling process or, through configuration, a predefined credential. Java uses the Java Authentication and Authorization Service to implement impersonation at the application level. Java impersonation is limited to application level only. This means that specifications do not define any relationship to user accounts on the underlying OS. Vendor-specific implementations (WebSphere®, WebLogic®, Sun ONE, Apache™ Tomcat, etc.) can implement functionality that maps the logged-in user to the OS domain names. Check with your specific vendor for available functionality.

ArcGIS Server utilizes impersonation to control access to ArcGIS Server functionality. ArcGIS Server components are managed by two operating system groups: ArcGIS Server users (agusers) and ArcGIS Server administrators (agsadmin). Access to ArcGIS Server objects is only permitted to members of the agusers group. To add and remove ArcGIS Server objects, you must be a member of the agsadmin group. Impersonation allows for consumers of ArcGIS Web servers to utilize ArcGIS Server objects by impersonating a user that is a member of the agusers or agsadmin group.

Impersonation can be incorporated into ArcGIS services through the .NET-provided impersonation control configuration in the ArcGIS Web service or through the application layer in the Web.config file. Impersonation control can be established at Web service development time. The Identity property is used to define the user name, password, and domain information. All authentication credentials provided as part of the impersonation control are encrypted into the application, and the Web service can be executed impersonating the authenticated user who is consuming the Web service. If the consumer of the Web service is not a member of the agsusers group, a specific user can

be additionally configured in the web.config file.

The following reference should be added to the web.config file:

```
<identity impersonate="true"
username="registry:HKLM\Software\AspNetIdentity,Name"
password="registry:HKLM\Software\AspNetIdentity,Password"
/>
```

This method of impersonation encrypts the user name and password of the impersonation account in the registry of the ArcGIS Server. For further information on encrypting the user name and password information in the registry, reference the Microsoft Knowledge Base Article #329290 (HOW TO: Use the ASP.NET Utility to Encrypt Credentials and Session State Connection Strings).

For additional information concerning ArcGIS Server and impersonation, reference the *ArcGIS Server Administrator and Development Guide* provided as part of the ArcGIS Server media kit.

ArcGIS Mitigation
Use of impersonation provides the developer and administrator with control of how the user accesses protected data and services.

WS-Security: Securing Java-Developed Web Services Consumed by SOAP and Custom ArcGIS Clients

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑	☑	

Web Services Security (WS-Security) is a standard set of SOAP extensions used to build secure Web services that implement integrity and confidentiality. WS-Security supports a wide variety of security models including PKI, Kerberos, and SSL. Specifically, WS-Security provides support for multiple security tokens, trust domains, signature formats, and encryption technologies.

WS-Security involves messages providing security tokens to the service. Services have a set of requirements that need to be satisfied to perform a specific action. If the service receives the required information and the message token is validated, then the service request is authorized.

For example, implementing WS-Security-enhanced ArcGIS Web services using a user name token profile would involve "signing" the XML communication with a secure hash of a random number, creation time, and password or shared secret into the SOAP request made to the ArcGIS Server. The ArcGIS Server would perform the same hash and compare it to the incoming hash passed by the client. If the hash from the client is the same as the hash on the server, then the communication is determined to be uncompromised and the request is fulfilled.

WS-Security can be integrated with ArcGIS published Web services consumed by SOAP (non-ArcGIS) clients. A custom ArcGIS extension for ArcGIS clients would be required for performing the secure hash operations currently not performed by core ArcGIS. Communications between client and service can be enhanced using WS-Security standards to ensure that requests have not been altered and cannot be intercepted by third parties. Confidentiality, integrity, authentication, and authorization can all be provided through WS-Security standards.

It is important to note that once custom ArcGIS Web service WS-Security controls have been designed into the application, out-of-the-box ArcCatalog, ArcMap™, and ArcGIS Engine software-based applications can no longer consume the Web service. ArcCatalog, ArcMap, and ArcGIS Engine software-developed applications will need a custom ArcObjects interface to administer and consume a WS-Security controlled Web service. Look for future releases of ArcGIS Server to support WS-Security standards from ArcGIS consumers.

ArcGIS Mitigation
By utilizing industry security standards and methods in Web Services, strong authentication, strong authorization, digital signatures, encryption, and logging can be implemented at the message level.

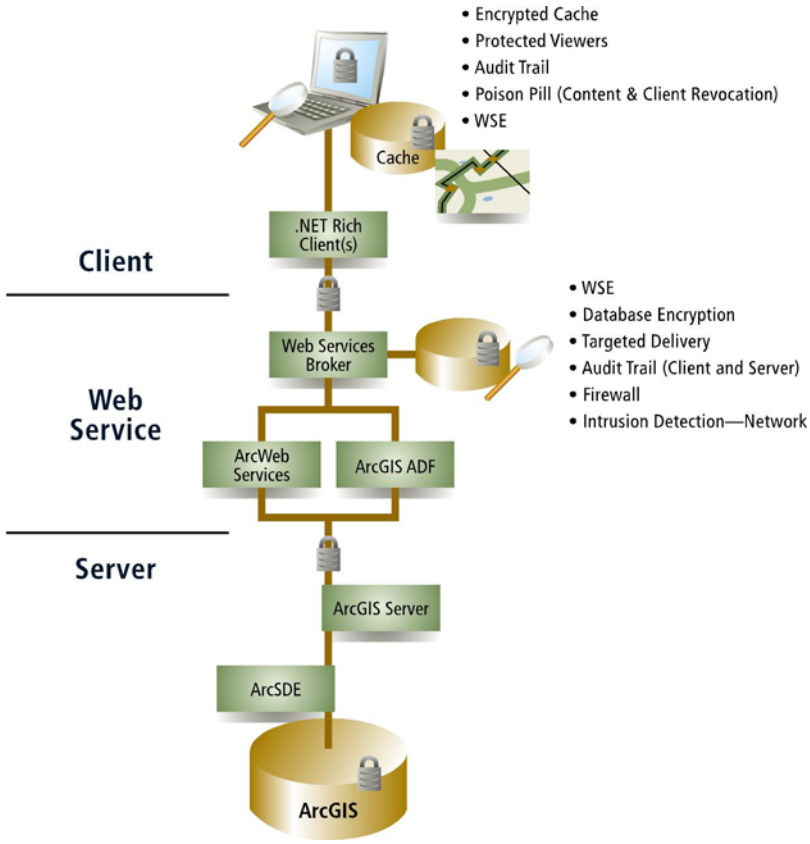
WSE: Securing .NET-Developed Web Services Consumed by Custom ArcGIS Clients

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
☑	☑	☑	☑	☑	

Web services enhancement (WSE) is the Microsoft .NET implementation of the WS-Security standards to provide such functionality as end-to-end message-level security. WSE is deployed as an add-on to the .NET framework and can be downloaded free of charge from Microsoft's Web site (http://msdn.microsoft.com/Webservices/building/wse/default.aspx). WSE allows .NET developers to secure interoperable Web services.

In deployment environments where client-side information security is important—even after dissemination—more robust WSE-based solutions may be appropriate. Vendor specific solutions can provide higher levels of end-to-end information assurance by combining server-side content encryption, fine-grained content publisher controls (rights management), precise content targeting, and enhanced client-side security integrated with WSE. Client-side security enhancements are accomplished through a combination of encrypted client content caching, protected client viewers (no cut/paste/forwarding of viewed content) that are permitted to open and view encrypted cached content, detailed event auditing, and "poison pill" content and client application disabling and/or removal. A unique client identifier, combined with a user name and password, enables multifactor authentication (something you have, plus something you know), in turn, making nonrepudiation possible.

J-9450



As with WS-Security, WSE can be easily integrated with ArcGIS published Web services. Communications between client and service can be enhanced using WSE-provided WS-Security standards to ensure that requests have not been altered and cannot be intercepted by third parties. Confidentiality, integrity, authentication, and authorization can all be provided through WS-Security standards.

Again, it is important to note that once custom ArcGIS Web service WSE controls have been designed into the application, out-of-the-box ArcCatalog, ArcMap, and ArcGIS Engine software-based applications can no longer consume the Web service. ArcCatalog, ArcMap, and ArcGIS Engine software-developed applications will need a custom ArcObjects interface to administer and consume a WSE-controlled Web service. Look for future releases of ArcGIS Server to support WSE standards from ArcGIS consumers.

ArcGIS Mitigation
By utilizing industry security standards and methods in Web Services, strong authentication, strong authorization, digital signatures, encryption, and logging can be implemented at the message level.

J-9450

Network Controls

Network controls are mechanisms that are implemented using standard networking techniques and practices. Network controls are integrated based on ArcGIS configuration. The security solutions presented in this section are implemented on the network between ArcGIS components.

This section contains security solution concepts that mitigate threats at the network level. Any one concept described in this section may or may not meet all the needs of an organization's secure architecture. It is the responsibility of the security architect to build on these concepts presented to construct a secure ArcGIS solution that meets the policies and standards of their enterprise.

ArcGIS Security Solutions

Securing ArcGIS Web Services behind Firewalls

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
				☑	

Securing ArcGIS Web services behind firewalls is somewhat more complex than securing ArcGIS Web applications. ArcGIS Server COM components are supported in both .NET and Java environments. The basic communication between ArcGIS Server components utilizes the Distributed Component Object Model (DCOM) protocol.

The use of DCOM involves dynamically acquiring TCP/IP ports for communication between components. A port is required for each transaction between components. When the transaction ends, the port is released. This type of communication requires a range of ports to be allocated for communication.

The primary concept of instituting firewalls is to restrict as many inbound ports as possible, thus reducing vulnerability. Since DCOM uses a range of ports on which to communicate, the security architect can minimize the risk to the enterprise by constructing a DMZ between the enterprise's secure network and the Internet and utilizing a reverse proxy. By utilizing a reverse proxy in the DMZ, a single port is exposed to the Internet allowing only communication through the designated Web server port. The reverse proxy funnels requests through an open port to the secure network for service of requests by ArcGIS Server components. All ArcGIS Server components exist on the secure network, minimizing exposure to external threat.

ESRI recommends that the security architect only place a firewall between the Web server/application server and ArcGIS Server components when necessary. Placing a firewall between the Web server and ArcGIS Server components requires communication over a range of ports. As the number of open ports increases, so does your security risk. Every effort should be made to restrict traffic through a firewall to as few ports as possible.

ArcGIS Mitigation
Use of firewalls restricts ArcGIS communication to designated ports.

Securing .NET and Java Web Services with HTTPS

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
	☑		☑		

HTTPS can be utilized to provide transport-level security for .NET- and Java-based Web services. As described earlier in this document, HTTPS relies on authentication through the organization's PKI infrastructure. Web service consumers connect to the server hosting the secure Web service. The consumer and server exchange certificate information. The Web service consumer and server use each other's public key to agree on a symmetric key to use for further encrypted communication.

.NET-based Web services used in conjunction with HTTPS can leverage client certificate mapping. Client certificate mapping provides the ability to map client certificates to individual users in an active directory. Java-based Web services can also leverage client certificate mapping through integration with the organization's PKI infrastructure. Additional configuration can be applied to designate a one-to-one relationship between certificates and users or a one-to-many relationship between certificates and users. The one-to-many relationships provide the capabilities to let a single certificate represent users that may be assigned a specific role in an organization.

Out-of-the-box ArcGIS clients (ArcCatalog, ArcMap, ArcGIS Engine, etc.) cannot consume HTTPS Web services. Custom ArcObjects extensions can be developed to consume HTTPS-protected Web services from ArcGIS clients. Look for future releases of ArcGIS to support consumption of HTTPS-protected Web services from core ArcGIS clients.

ArcGIS Mitigation
Use of HTTPS encrypts the communication between the client and server, preventing packets from being intercepted, modified, or corrupted.

Securing Web Service Message Content with a Security Gateway (XML/SOAP Firewall)

Threats					
Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
				☑	☑

One of the more important components of securing Web services is ensuring that the message communication is secure in transit. As discussed in this paper, utilizing SSL in transport ensures that secure message communication occurs between the Web service and requesting source. Although messages communication is secure, often security threats are embedded in the messages themselves. Since Web services allow platform-independent communication, most Web services utilize well-known XML schemas. This

introduces a threat. A common control used to ensure message content is not threatening is implementing a security gateway.

Often security gateways are also referred to as XML/SOAP firewalls. As the name suggests, XML/SOAP firewalls provide a range of security services focused on the processing of XML. Like traditional packet-level firewalls, XML/SOAP firewalls can be implemented through either a network device or through server-side software on the Web server. Unlike traditional packet-level firewalls, XML/SOAP firewalls can filter, encrypt, and validate digital XML signatures and data at the message level. This ensures that a threatening message does not compromise the security of the Web service resource by looking for message content that could cause buffer overflows, denial of service, or other threatening vulnerabilities.

Software implementations of XML/SOAP firewalls are readily available from most commercial Web and application server providers. Deploying XML/SOAP firewall functionality at the Web server may hinder Web service response time and should be considered. Hardware deployments, however, tend to improve network throughput. Hardware XML/SOAP firewalls should be deployed in front of the server where the ArcGIS Server Object Manager/Server Object Container reside.

ArcGIS Mitigation
Use of security gateways can restrict ArcGIS communication to specific ports and reduce the threat of buffer overflow by monitoring message content to identify known malicious activities.

RDBMS Controls

RDBMS controls are mechanisms that are implemented in the RDBMS and integrated with ArcGIS through out-of-the-box configuration or custom application enhancements. The security solutions referenced in this section are implemented in the RDBMS.

RDBMS layer security controls span all ArcGIS architectures. Typically, the RDBMS is central to the enterprise. All application architectures utilize a geodatabase. The most important aspect of utilizing RDBMS layer controls is understanding how your Web services access the central data store. Whether through an application database user or as an individual account, you must ensure that the user accessing the data has the proper permissions to access the data.

Reference the RDBMS layer controls described in the client/server architecture for further information concerning RDBMS layer controls.

J-9450

Implementations

ESRI is committed to being in a secure component in the enterprise solution and continues to configure and test our products so they can be readily integrated in secure enterprise solutions, typically in concert with other products that deliver or enable security functions. Below you will find a list of possible solutions that can be deployed to meet security requirements of secure enterprise solutions.

Category	Solution	More Information
Application		
	ArcObjects: Custom Control Extensions	http://arcobjectsonline.esri.com/ http://www.esri.com/software/arcgis/arcgisengine/index.html
	ArcObjects: Utilize ArcObjects to Create and Store Geographic Transactions Created during the Business Process Work Flow to Provide a Traceability Mechanism	http://opengis.net/gml/ http://www.esri.com/software/arcgis/extensions/jobtracking/index.html
	Basic and Digest HTTP Authentication: ArcGIS Web Application Authentication	http://www.ietf.org/rfc/rfc2617.txt?number=2617
	Single Sign-On: Integrate Web Applications with Single Sign-On Systems	http://www3.ca.com/Solutions/SubSolution.asp?ID=4348 http://www.passlogix.com http://www.oblix.com http://www-306.ibm.com/software/tivoli/solutions/security/
	Access Control List: Restrict Access to ArcIMS Map Services Using an Access Control List	http://support.esri.com/index.cfm?fa=knowledgebase.techarticles.articleShow&d=25472
	Digital Certificate Authentication: Securing ArcGIS Web Applications Authentication Using E-Signatures	http://www.verisign.com http://www3.ca.com/Solutions/SubSolution.asp?ID=4348 http://www.passlogix.com http://www.oblix.com http://www-306.ibm.com/software/tivoli/solutions/security/
	Securing Java Web Services with HTTP Basic and Digest Authentication	http://java.sun.com/Webservices/docs/1.0/tutorial/doc/WebAppSecurity4.html#64191
	Securing .NET Web Services with HTTP Basic and Digest Authentication	http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpguide/html/cpconbasicdigestauthentication.asp

J-9450

Category	Solution	More Information
Application (cont.)		
	Securing ArcGIS Java Web Services with Native Security Policy Management Capabilities Found in the Web Application Server and Providing Authorization to Specific Content Based on Assigned Role	http://developers.sun.com/prodtech/appserver/reference/techart/access_control.html
	Impersonation: Mapping External Web Users to ArcGIS Users	http://arcgisdeveloperonline.esri.com/ArcGISDeveloper/default.asp
	WS-Security: Securing Java-Developed Web Services Consumed by SOAP and Custom ArcGIS Clients	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
	WSE: Securing .NET-Developed Web Services Consumed by Custom ArcGIS Clients	http://www.swanisland.net/ http://msdn.microsoft.com/Webservices/building/wse/default.aspx?pull=/library/en-us/dnwse/html/programwse2.asp
Operating System		
	LDAP/Central User Repository: ArcObjects Interface	http://arcobjectsonline.esri.com/ http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx http://publib-b.boulder.ibm.com/redbooks.nsf/RedbookAbstracts/sg244986.html?Open http://www.ietf.org/rfc/rfc3377.txt?number=3377
	Windows Native Authentication: ArcSDE and RDBMS Client	http://arcsdeonline.esri.com/ http://www.oracle.com/technology/deploy/security/index.html http://www.microsoft.com/sql/default.mspx http://www-306.ibm.com/software/data/db2/udb/edition-ese.html http://www-306.ibm.com/software/data/informix/
Network		
	Firewall: Restrict Communication to ArcSDE Application Server Process	http://support.esri.com/index.cfm?fa=knowledgebase.whitepapers.viewPaper&PID=16&MetaID=229

Category	Solution	More Information
Network (cont.)		
	SSL: Establish a Secure Communication Channel between the ArcGIS Client and RDBMS Server	http://www.oracle.com/technology/deploy/security/index.html http://support.microsoft.com/default.aspx?scid=kb;en-us;316898 http://www-306.ibm.com/software/data/db2/udb/edition-ese.html http://www-306.ibm.com/software/data/informix/ids/
	IPsec: Establish a Secure Communication Channel between the ArcGIS Client and RDBMS Server	http://www.ietf.org/html.charters/IPsec-charter.html http://www.microsoft.com/windows2000/techinfo/planning/security/IPsecsteps.asp
	Intrusion Detection: Monitor ArcGIS Operations to Identify Suspicious Patterns that Might Identify Malicious Activity	http://arcobjectsonline.esri.com http://www.sans.org/resources/idfaq/
	Firewalls: Restrict Access to ArcGIS Components Accessed through ArcIMS Using Advanced Network Configurations	http://support.esri.com/index.cfm?fa=knowledgebase.whitepapers.viewPaper&PID=16&MetaID=229
	IPsec: Secure the Communication Channel between ArcIMS and ArcSDE across Platforms	http://www.ietf.org/html.charters/IPsec-charter.html http://www.microsoft.com/windows2000/techinfo/planning/security/IPsecsteps.asp
	HTTPS: Securing ArcGIS Web Applications with HTTPS	http://support.esri.com/index.cfm?fa=knowledgebase.techArticles.articleShow&d=21669
	Securing ArcGIS Web Services behind Firewalls	http://support.esri.com/index.cfm?fa=knowledgebase.techArticles.articleShow&d=28703
	Securing .NET and Java Web Services with HTTPS	http://arcobjectsonline.esri.com
	Securing Web Service Message Content with a Security Gateway	http://www.datapower.com http://www.sarvega.com http://www.reactivity.com http://www.cisco.com

J-9450

Category	Solution	More Information
RDBMS		
	Feature-Level Security: Restrict Access to Rows of Attribute Data in the Geodatabase Based on Organizational Responsibility or Role	http://arcobjectsonline.esri.com http://www.oracle.com/technology/deploy/security/index.html http://www.microsoft.com/sql/default.mspx http://www-306.ibm.com/software/data/db2/udb/edition-ese.html http://www-306.ibm.com/software/data/informix/
	Data File Encryption: Encrypt ArcGIS Data Stored on Disk in the RDBMS	http://www.protegrity.com
	RDBMS Privileges: Restrict Access to Geodatabase Based on Organizational Responsibility or Role	http://arcobjectsonline.esri.com http://www.oracle.com/technology/deploy/security/index.html http://www.microsoft.com/sql/default.mspx http://www-306.ibm.com/software/data/db2/udb/edition-ese.html http://www-306.ibm.com/software/data/informix/
	Intrusion Detection: Establish a Mechanism to Restrict and Detect When the Geodatabase Is Accessed by Unauthorized Applications	http://www.oracle.com/technology/deploy/security/index.html http://www.microsoft.com/sql/default.mspx http://www-306.ibm.com/software/data/db2/udb/edition-ese.html http://www-306.ibm.com/software/data/informix/

Summary

ESRI is committed to building open and interoperable commercial off-the-shelf software products. In the last decade, ESRI launched a major initiative to re-architect its GIS product line to adhere to important, emerging IT and GIS standards. With respect to security, ESRI is currently addressing the role of emerging security standards across all software products. By integrating security standards, ESRI can provide the security architect the flexibility to integrate trust across all ESRI components of the solution. This allows security architects the ability to effectively meet more precise requirements of mission-critical solutions.

For more information concerning ArcGIS enterprise security, e-mail esinfo@esri.com.

About ESRI

Since 1969, ESRI has been helping organizations map and model our world. ESRI's GIS software tools and methodologies enable these organizations to effectively analyze and manage their geographic information and make better decisions. They are supported by our experienced and knowledgeable staff and extensive network of business partners and international distributors.

A full-service GIS company, ESRI supports the implementation of GIS technology on desktops, servers, online services, and mobile devices. These GIS solutions are flexible, customizable, and easy to use.

Our Focus

ESRI software is used by hundreds of thousands of organizations that apply GIS to solve problems and make our world a better place to live. We pay close attention to our users to ensure they have the best tools possible to accomplish their missions. A comprehensive suite of training options offered worldwide helps our users fully leverage their GIS applications.

ESRI is a socially conscious business, actively supporting organizations involved in education, conservation, sustainable development, and humanitarian affairs.

Contact ESRI

1-800-GIS-XPRT (1-800-447-9778)
Phone: 909-793-2853
Fax: 909-793-5953
info@esri.com
www.esri.com

Offices worldwide
www.esri.com/locations

ESRI
380 New York Street
Redlands, California
92373-8100 USA