6.8 Enterprise Partner Communication

Enterprises often partner with third parties to support their business model. These third parties may include application and managed service providers, consulting firms, vendors, outsourcing development teams, and satellite offices. As part of this relationship, access must be granted to allow data to travel between the organizations. Without attention to the protection of that data and the methods by which they are transferred, one or both organizations may be at risk.

Example

The museum has received a sum of money and is expanding! It wants to expand its services in the following ways:

1. Publish an RSS news feed advertising all upcoming museum events and information.
2. Sell goods online from its Web site. The museum has created a merchant account with a popular payment processor and financial organization. The Web site application will use a programmatic API provided by the payment processor.
3. Outsource the development of a Web site to a third party. One component of the Web site will be a public, e-commerce site selling goods and promoting museum events and exhibits. The second component will be a private, intranet Web site containing an employee directory as well as confidential corporate funding and research and development data. The museum realizes that the third party will require some confidential database tables and documents in order to design and test the application.
4. Subscribe to the International Museum Consortium (IMC) service. This service will publish current and rolling exhibit information to other subscribers. Membership of this service will allow the museum to search and bid for rolling exhibits from any other subscribing museum around the world. They feel it would give them a competitive advantage over other regional and local museums, and will substantially increase their patron attendance. The IMC will provide the software application, centrally manage user accounts and facilitate a bidding and messaging process. The museum already has an infrastructure capable of operating and managing the software application, and simply needs to configure it to access the museum's inventory database.

Each of these projects involves exchanging information with other parties, but vary in the degree of security requirements and in the method of data exchange. The museum clearly recognizes the value of these projects, but is concerned that its personnel, customer, and confidential exhibit information will be at risk of unauthorized access, modification, or denial of service. It would like to implement these projects but needs to protect its data, systems, and reputation.

Context

An enterprise has an existing business process, or is proposing a new business process, that requires information to be exchanged with another entity across a computer network. The business factors that initiated the partnership have already been determined and a high-level service level agreement, complete with disaster recovery and business continuity planning, has been established.

Problem

When an enterprise engages in a business relationship, it typically exchanges information and allows users and/or applications to access privileged resources. Not only can there be risk of theft or manipulation of data, but also risk of unauthorized access to resources by another organization. Furthermore, you may trust the partner with whom you entered into a relationship, but can you trust their contractors, application vendors, networks, or firewall configuration? A breach in their network may lead to a breach in your own.

How can an enterprise protect its systems and data while communicating with external partners?

An enterprise must resolve the following forces:

- It needs to be reasonably assured that sensitive information is protected when traveling beyond its control.
- Security procedures become difficult to manage when one entity does not share the same security requirement and considerations as the other.
- It must conform to legislation when storing and transferring financial or personal health information.
- Applications that communicate with business partners become vulnerable, not only to attack from that partner, but also from attacks from users who defeat the partner's security.
- The services that the partner may access might require special or custom network paths that are not used by regular customers or internal users.
- An enterprise may not have the time or ability to properly evaluate the security controls of the partner, and the partner may not be able to conform to the security requirements imposed by the enterprise (in time).

- Outsourcing software development efforts creates additional challenges, as the data and people may reside across the planet and beyond the immediate reach of the enterprise.
- Both parties must commit to the agreement but be flexible enough to modify the policy should the risk or business requirements change. For example, if transaction volumes dramatically increase, or if vulnerabilities are suddenly discovered in an application.
- The enterprise may require the business partners to conform to a particular interoperability scheme that the partner is not able to match.

Solution

Specify enterprise partner communication in five areas: define the scope and security requirements of the information to be exchanged, audit the business partner, identify and protect communication channels, define exchange methods and procedures, and identify service termination activities.

1. Define scope and security requirements.

   First, define which data or application services are to be exchanged between organizations. Then identify the security requirements for this information.
2. Audit business partner.

   Perform a security audit of the partner organization commensurate with the security requirements of the information and the policies of your enterprise.
3. Identify and protect communication channels.

   Identify and protect communication channels in the following ways:

   - Communication channels: identify the preferred channels of communication.
   - Traffic separation: separate business partner traffic from regular enterprise traffic, and from other partners, wherever possible.
   - Ports and portals: determine the required SINGLE ACCESS POINT (279) connecting the two organizations and secure them.
   - Access controls: apply administrative, physical and technical access controls, as appropriate, to protect the data throughout its life cycle. These controls serve to protect the data while stored either at the enterprise or business partner and as it passes from one system to another.

4. Define exchange methods and procedures.

   First, identify the pre- and post-processing procedures that are to be applied to the data and communication channels. Then maintain and monitor usage logs and reports. This will provide an early warning of performance and stability issues, as well as indication of malicious activity.

5. Perform service termination activities.

   At the completion of the partner agreement, perform the following service termination activities:

   - Access revocation: user accounts, authorization privileges and system access should be promptly removed.
   - Data sanitization: purge all sensitive information from disk drives, databases and other files
   - Repurpose assets: network devices, servers, application resources can now be re-used for other partner communications or internal functions

Structure

The structural components of this pattern are displayed in the figure on page 177.

SINGLE ACCESS POINT (279)*s* provide a central, auditable entry point into the enterprise. Access controls at these access points enforce restrictions on inbound and outbound traffic. Dedicated communication channels and encryption controls protect the data throughout its transmission and storage. Partitioned storage facilities provide dedicated separation of information between enterprise and partner data.

Implementation

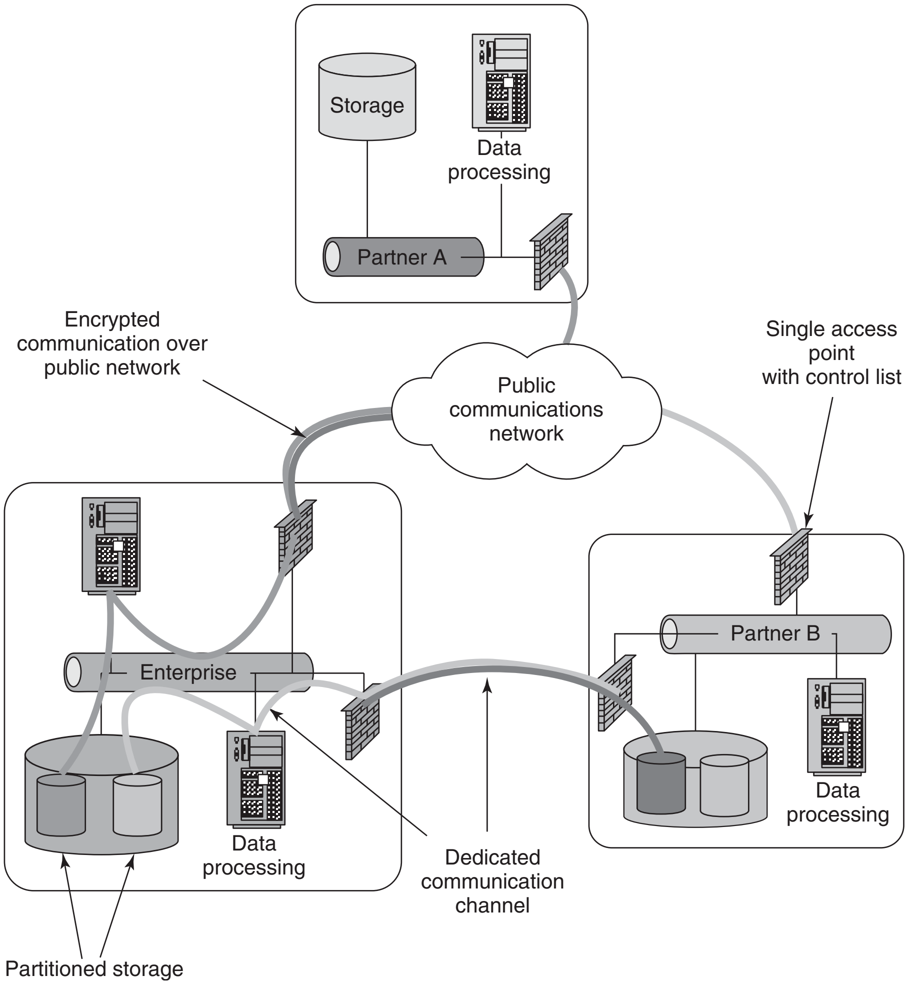
The following steps should be considered during the pattern implementation:

1. Define scope and security requirements.

   Determine the minimum set of data that should be exchanged by sanitizing it as much as possible. That is, strip it of any confidential or unnecessary information. Personally identifiable financial or medical numbers, for example, can be substituted for another unique identification number. There is no need to send more information than necessary. Indeed, extra data may inflate security requirements, incurring additional infrastructure, costs and delays.

   If application services are used, provide interfaces (APIs, URLs) for only those functions that are necessary to fulfill the business requirement. This improves security by limiting the access to the enterprise and its systems.

   The data owner will be able to provide the security requirements of the data. If not, SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89) can be used. This enterprise pattern provides a process whereby a data owner (or other) can


Storage
Data processing
Partner A
Encrypted communication over public network
Single access point with control list
Public communications network
Enterprise
Partner B
Data processing
Data processing
Dedicated communication channel
Partitioned storage

Enterprise partner communication structure

determine the security properties necessary for the exchange of data between organizations. The properties are expressed as follows:

- Protection against inadvertent or unauthorized disclosure: confidentiality
- Protection against inadvertent or unauthorized modification: integrity
- Making business assets available for authorized use: availability
- Attribution of responsibility for actions: accountability

2. Audit business partner.

   An enterprise may require a security audit of the partner before exchanging any information or entering into any business agreement. The purposes of the audit are twofold:

   - To evaluate the security policies, practices and controls of the partner. Policies and practices can be evaluated by the enterprise, or it may prefer to acquire independent results from an external consulting firm. Security controls can be tested with a vulnerability scan and/or penetration test.

- To compare and reconcile these results against 'prescribed standards of performance' [Swan00]. Such standards may be enforced by a number of sources: federal or local legislation may define a basic (minimal) level of protection for information exchange, use and storage. The enterprise, itself, may impose much stricter restrictions.

3. Identify and protect communication channels.

   Communication channels include all protocols, hardware devices, communication lines (dedicated and public) and computer network segments over which data will be traveling should be identified. Both the type of data as well as its security requirements will determine (or, at least, strongly effect) the type of communication channel necessary or available. For example, many payment transactions are still sent over value added networks (VANs) using X.400 messaging. Conversely, many modern applications communicate across a public TCP/IP network using a combination of HTTP, HTTPS protocols and HTML, XML or a proprietary message format. Other influencing factors of the type of communication channel include the available technology of the partner organization, industry conventions and budget.

   For traffic separation, dedicated communication channels are preferred, because they reduce the risk of harmful (malicious or inadvertent) events originating from one partner and affecting others, as well as eliminating single points of failure across multiple users. When possible, isolate partner traffic either physically or logically. Physical separation is achieved by using dedicated hardware (servers, firewalls, communication lines) and software. Logical separation is achieved through segmented IP addressing, virtual environments such as multiple operating systems on a mainframe, virtual Web hosts, and multiple databases on a shared installation.

   For each of these communication channels, identify and protect the SINGLE ACCESS POINT (279)*s* into the enterprise and its systems. Relevant questions to ask are: do additional ports need to be opened up at the firewall or edge routing device, and how will this affect the overall security posture of the environment? Does the network or application need to be modified to allow access for a particular set of users or hosts and will this result in additional threats or vulnerabilities? Will physical access be required by the partner to the enterprise office (or its affiliates)? Will any special arrangements be necessary to support the partner, such as segregated network connectivity (VPN), analogue phone lines, and so on. How will enterprise systems be protected while external partners are on the premises?

Access controls must be applied at any point at which data is passing from one system (user, hardware device, application) to another. Types of access controls include the following:

- Technical access controls used at the network (transmission) layer in routers, firewalls and servers to prevent access from unauthorized hosts. These can be used at the application layer as well, to grant and deny access to specific users.
- Administrative access controls used to define policies and procedures that govern the acceptable circumstances and conditions under which the data can be accessed.
- Physical access controls used to ensure physical protection of the data. For example mechanical door locks to offices, server rooms, and cabinets.

For all implementations of access control, employ a 'failed closed' policy by preventing all access, then granting access for specific entities. This is most commonly used on network perimeter devices such as firewalls, routers and internet servers.

User authorization should be enabled according to the principles of Least Privileges and Separation of Duties [Sal75] and by applying ROLE-BASED ACCESS CONTROL (249). Least Privileges is also known as Need to Know, and is discussed in Security Principles and Security Patterns on page 504). Least Privileges ensures that a particular subject (human or application user) only has the necessary privileges required to perform a given task. An example would be to grant access to write or modify files in a repository, but not delete files. ROLE BASED ACCESS CONTROL is used to assign a subject (user) to one or many roles, with each role allotted a unique collection of privileges. This abstracts the subject from their privileges, providing a business-centric approach and improving the management of access control. The roles of system administrator, sales advisor and purchaser, for example, would all have unique collections of privileges in a corporate directory. Finally, Separation of Duties distributes responsibility (trust) across multiple subjects and is often used in conjunction with ROLE-BASED ACCESS CONTROL (249). For example, partitioning roles (and therefore privileges) of a bank customer with teller and auditor.

4. Define exchange methods and procedures.

Any form of data exchange will require special pre- or post-processing, depending both on the method of exchange and on any requirements to comply with internal policies or legal regulations. Examples of four common exchange methods and procedures are listed below.

Method 1: On-demand Transfer

This refers to the ad-hoc exchange of information of raw data from one site to another. For example, weather data, news feeds, stock ticker data, and batch file transfer.

Security related procedures:

1. By what mechanism will data be transferred? FTP, HTTP, private line?
2. How will the data be transferred: pushed or pulled? Automated, batch, manual?
3. What will be the naming convention of the files? For example dated, static, other?
4. Must a file always exist? Will null files be accepted?

Method 2: Real-time Information Exchange

For example, payment processing, EDI. This is payment transaction information, either between financial organizations, or a merchant and a payment processor. The information is sent real-time and contains account (credit card) data and a monetary value. These can be both high or low volume and high or low value transactions. Generally, when a transaction is sent, an authorization or confirmation number is returned for logging.

Security-related procedures:

1. Will a custom programming API be necessary? If supplied by another entity, will it require review, modification to operate within the enterprise's infrastructure?
2. What are the possible response codes? What do they represent?
3. Can batching (near real-time) be used, or are all transactions individual?
4. Is a notification to other business processes necessary to continue a workflow?

Method 3: Large Volume Information Transfer

For example, managed security outsourcing, and application development outsourcing relationships. This is the large volume shuffling of corporate data. Managed service providers are sent large log files for processing. Development outsourcing companies are provided corporate, and sometimes confidential customer, information used for developing or repairing an application on behalf of the enterprise. Information transfer can occur at any time although not real-time. It requires large bandwidth transmission as well as privacy and integrity controls.

Security-related procedures:

1. Is electronic transfer of the data prohibited? Instead, should the data be transferred physically?
2. What scheduling requirements are required: can the exchange wait until a predetermined time, or does it need to be transferred and processed immediately?
3. What sort of notification, if any, must be made to either humans or applications before or after the data transfer?
4. Will the outsourcing company require direct access to the enterprise's internal networks or servers? Will they require extra privileges to data or user stores?

Method 4: Interactive Application Services

These applications can be accessed by a human or another application in order for one enterprise to provide services to another enterprise. That is, one enterprise is extending its business model to incorporate the services of another enterprise. For example, a Web-based airline reservation site that incorporates the services of a car rental and hotel reservation company, or a third party with network access into the enterprise.

Security-related procedures:

1. What communication and messaging protocols are used?
2. What authentication procedures will exist between applications or networks extensions and what auditing will be performed?
3. What sort of notification, if any, must be made to either humans or applications before or after the data transfer?
4. Who will access the services? Just employees of business partners, contractors or third or fourth parties?

Logging and monitoring

Log files from application servers, firewalls and other application and networking devices will provide important use and access audit trails. They will identify where the access originated, potentially what was being accessed, and for how long. They can be used to monitor use for performance and quality assurance reasons, as well as to provide information for forensic investigations. Such processes may already be employed at the enterprise, but they should also be enabled by the business partner.

Implementation steps (continued):

5. Perform service termination activities.

Access revocation

Temporary and expired user accounts are often a convenient way of gaining access to a system. Therefore, remove all user accounts and entries from access control lists from any network device (firewalls, routers, VPN concentrators), server (hosts files), applications and user stores (database, LDAP, and so on).

Data sanitization

Proper cleaning of disk drives is a critical but often-overlooked task. Specialty tools are available to completely erase entire hard drives or particular files. Also, one or both parties posses data belonging to the other: this data should be completely erased or returned to the business partner in a secure manner.

Asset Repurposing

Only when access controls have been reset and data sanitization has occurred is the asset ready to be reused for another business partner or internal function.

Example Resolved

The museum has chosen to address its four projects as follows:

On-demand News Feed

The museum will make its news data available to other museums or organizations through a free RSS subscription service: the museum just wants to know who's accessing their feeds. The information will be updated as necessary and can be retrieved ad hoc by the other entities. Using SECURITY NEEDS IDENTIFICATION FOR ENTERPRISE ASSETS (89), the museum recognizes that prior to release, the information will require medium confidentiality and integrity, while after release only a low degree of integrity is required. The application server will site behind a firewall in a DEMILITARIZED ZONE (449) and both devices will undergo moderate host hardening and patching. The read-only information will be accessible via FTP or XML over HTTP, and all connections will be logged. To prevent abuse of the feed, request attempts will be limited to ten per hour.

Real-Time Transaction Processing

Payment transactions are initiated from the museum's application and sent real-time from the museum to the payment processor. Each transaction travels across the public internet over TCP/IP and is encrypted end-to-end using the API's encryption algorithm. This ensures confidentiality and integrity of the transaction. The authorization number is stored by the museum.

The payment processor provides this service to hundreds of other merchants and is quite proficient at high availability of all of its systems. The museum is not dual-homed and therefore accepts the risks due to an outage of its Internet service provider. In the event of a failure, however, the museum has obtained contact information for both the payment processor and its ISP.

Outsourcing Web Site Development

Clearly, the transmission of confidential information to the development company, as well as their use of that data, requires protection, specifically, confidentiality and integrity. The museum has performed a security audit of the development company. From this audit, it agrees that the application will be developed and tested on servers protected behind both a corporate perimeter firewall and separate firewall, isolating their development environment from other projects. The development party is the only group with system access to the museum database: data will be incrementally backed up on a nightly basis, fully on a weekly basis, and stored in a locked cabinet to which only the immediate team members and managers have access. Finally, the development company will not share any of the enterprise's information with a third party without prior consent of the museum.

IMC service

The museum recognizes that the exposure of its entire database containing all corporate and personnel information would pose too great a risk. Therefore, the museum chooses to install the IMC software and a new database on a separate network segment from the internal corporate systems in a DEMILITARIZED ZONE (449), isolating it from the corporate network. On a daily basis, only necessary portions of museum and exhibit information will be exported from the authoritative corporate source and imported into the local IMC database. Specifically, donators and funding sources are not exported, nor is financial or human resource information. The museum is provided with an administrative interface that can be used to retrieve messages or update museum information as necessary. The IMC server will marshal all messages between museums over HTTPS only and all user-level requests will be logged.

Variants

[IBM2] describes several patterns for enterprise partner communication. Each pattern builds on the previous pattern's flexibility and ability to meet the increasingly sophisticated demands of the enterprise:

- B2B Topology 1: Document Exchange
- B2B Topology 2: Exposed Application
- B2B Topology 3: Exposed Business Services

- B2B Topology 4: Managed Public Processes
- B2B Topology 5: Managed Public and Private Processes

IBM has also introduced the Trading Partner Agreement [IBM3], an XML-based standard for defining 'how trading partners will interact at the transport, document exchange and business protocol layers. A TPA contains the general contract terms and conditions, participant roles (buyers, sellers), communication and security protocols and business processes, (valid actions, sequencing rules, etc.).' [OASIS00]

[ISO17799] describes security requirements that should be considered when allowing physical or logical access for on-site contractors, trading partners or support staff to enterprise data systems. Examples include the following:

- Description of each service to be made available
- Target level of service and unacceptable levels of service
- Right to monitor and revoke user activity
- Controls to ensure protection against malicious software
- Involvements of third parties with subcontractors
- Clear and specified process of change management

Known Uses

These secure communication procedures are part of many enterprise policies for managing business relationships. For example, many enterprises require a provision in business contracts allowing them to perform a security audit of any third party. Since federal legislations are often the driving force behind this, audits are becoming more and more a priority for senior executives as they become personally responsible for the overall security of their organizations.

Consequences

Use of this pattern provides the following benefits:

- Expectations with respect to security controls and procedures are properly managed.
- Activity and transaction logs are maintained for auditing and compliance for both parties.
- Trustworthy communications enable new business opportunities.
- Sensitive corporate data and systems are not exposed to unnecessary threats or vulnerabilities.
- The exchange procedures can be documented to create a repeatable guideline for subsequent partner agreements.

It also incurs the following liabilities:

- Complex negotiations with business partners may delay the implementation of a new project.
- The cost of a security audit or required controls may be beyond the financial capabilities of the partner entity—but necessary if they wish to do business with the enterprise.
- This pattern does not address integration issues (programmatic interfaces, process flow, messaging) between organizations or applications.