Achieving PCI compliance using WebSphere DataPower

Prithvi Srinivasan

October 24, 2012

PCI compliance is important to organizations dealing with cardholder data, and failing a PCI audit causes heavy fines and damage to a customer’s brand reputation. WebSphere® DataPower provides a "drop-in" solution for customers facing PCI audits. This article describes DataPower's capabilities for PCI compliance requirements, and how to position DataPower to achieve the maximum return on investment (ROI) in a short amount of time.

Introduction

If your organization deals with credit or debit cards, then you must have heard of the PCI DSS requirements. The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to improve and standardize cardholder data security measures.

PCI DSS applies to all entities involved in payment card processing, including:

- Retail (e-commerce, brick and mortar)
- Hospitality (restaurants, hotels, casinos)
- Convenience stores (gas stations, fast food)
- Transportation (airlines, car rental, travel agencies)
- Financial services (credit card processors, banks, insurance companies)
- Health care and education (hospitals, universities)
- Government (where payment cards are accepted)

Figure 1 shows a high-level overview of the twelve PCI DSS requirements.
PCI compliance comes up more and more these days in pre-sales cycles. The PCI DSS requirements are more than just technology requirements. Therefore, to be truly PCI compliant, an organization needs a combination of technology and organizational controls in place.

Most organizations have some combination of technology and organizational controls that cover a subset of the PCI DSS requirements, but a large number of them seem to be failing their PCI audits. WebSphere DataPower Appliances, with their extensive security and integration capabilities, are ideally positioned to fulfill the PCI requirements. These appliances are configuration-driven and are "drop-in" solutions.

**Build and maintain a secure network**

This section describes how to secure your network layer.

1. **Install and maintain a firewall configuration to protect cardholder data**

You can deploy DataPower as a security gateway in the demilitarized zone (DMZ), meaning that it terminates the incoming connections, ensures that the request messages are "safe", and then creates a new connection and passes them to services within the trusted zone. Traditional IP packet filtering firewalls cannot access the message payloads, and allow poisonous messages through.

DataPower can parse the messages payload and perform data validation to ensure no malicious or accidentally dangerous content reaches the backend applications in the trusted zone. Figure 2 shows some of the XML threats that DataPower can successfully handle.
Figure 2. XML threats

- XML Entity Expansion and Recursion Attacks
- XML Document Size Attacks
- XML Document Width Attacks
- XML Document Depth Attacks
- XML WellFormedness-based Parser Attacks
- Jumbo Payloads
- Recursive Elements
- Megatag – aka Jumbo Tag Names
- Public Key DoS
- XML Flood
- Resource Hijack
- Dictionary Attack
- Message Tampering
- Date Tampering
- Message Snooping
- XPath Injection
- SQL injection
- WSDL Enumeration
- Routing Detour
- Schema Poisoning
- Malicious Morphing
- Malicious Include – also called XML External Entity (XXE) Attack
- Memory Space Leech
- XML Encapsulation
- XML Virus
- False Message
- Replay Attack

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Setting up a "Password Policy" is part of an organization's internal controls mechanism. DataPower plays its part by enforcing the password policy, but the internal controls need to ensure that all the other players in the IT landscape play their part too.

There are two ways to set up access control to a DataPower appliance:

- **Authenticate users by locally defined accounts**: In this case, you can set up a password policy on the appliance that allows for parameters, such as Minimum Password Length, Require Mixed Case, Require Non Alphanumeric, Disallow Username as Substring, Maximum Password Age, Disallow Password Reuse, and so on.

- **Authenticate users’ off-device, such as LDAP or Active Directory**: In this case, the password policy has to be defined in the LDAP or Active Directory. This acts as the Policy Decision Point (PDP), while the appliance acts as the Policy Enforcement Point (PEP).

Protect stored cardholder data

The following requirements are the heart and soul of the PCI DSS requirements list. They basically mean that cardholder data must be secure both in-flight and while at-rest.

3. Protect stored cardholder data and 4. Encrypt transmission of cardholder data

DataPower can fulfill these requirements by implementing the following functionalities:

- **Securing data while at-rest**:
  - **Message confidentiality**: DataPower allows message and field level encryption, which ensures that no one can access the payload without the appropriate decrypt key.
  - **Message integrity**: A cryptographic hash allows the end user to check if a certain message was intercepted or tampered with.
  - **Non-repudiation**: Digital signatures are used to determine if the message was sent by the actual originator.
• **Securing data while in-flight**: DataPower provides in-flight security using the secure socket layer (SSL). It provides support for HTTPS, FTPS, SFTP, and MQ.

### Maintain a vulnerability management program

This section describes how to protect your PCI gateway against security vulnerabilities.

### 5. Use and regularly update anti-virus software

SOAP messages carry additional payload through attachments, and therefore attachments need to be scanned for viruses before they are permitted to enter the secure zone of any organization.

DataPower is *not* an anti-virus scanner product, but it does support the ICAP protocol. Therefore, it leverages the ICAP protocol with vendor-acquired anti-virus scanner products to complement its own in-built security features. The main objective of this configuration is to filter out any malicious SOAP messages at the DMZ layer of the network, where DataPower is deployed as a security gateway.

Figure 3 shows the Anti-Virus action that you can configure to offload the virus scan of an attachment to an external scanner through ICAP.

**Figure 3. Anti-Virus action**

![Image of Anti-Virus action configuration]

### 6. Develop and maintain secure systems and applications

You can implement this requirement through a mix of technology and internal controls. Following are some of the ways DataPower can help:
• **Install the latest firmware**: Firmware upgrades are easy and quick. If there are any issues with the newly installed firmware, then rolling back to the previous version can be achieved in a manner of minutes.

• **Use change control**: Any changes to the DataPower service objects leave a trail in the audit logs. For more information about best practices to change control on the appliance, see [*Managing WebSphere DataPower Device configurations for high availability, consistency, and control*](#).

• **Use secure coding guidelines**: Many of the secure coding guidelines in this subsection seem to match the top 10 list of security threats by the Open Web Application Security Project (OWASP).

DataPower provides 100% coverage for the top 10 security threats listed by OWASP, as shown in Figure 4.

**Figure 4. Top 10 security threats**

![OWASP Top 10 – 2010 (New)](Image)

- A1 – Injection
- A2 – Cross-Site Scripting (XSS)
- A3 – Broken Authentication and Session Management
- A4 – Insecure Direct Object References
- A5 – Cross-Site Request Forgery (CSRF)
- A6 – Security Misconfiguration (NEW)
- A7 – Insecure Cryptographic Storage
- A8 – Failure to Restrict URL Access
- A9 – Insufficient Transport Layer Protection
- A10 – Unvalidated Redirects and Forwards (NEW)

**Implement strong access control measures**

This section describes how to set up strong access control measures for your PCI gateway:

7. **Restrict access to cardholder data by business need-to-know**

8. **Assign a unique ID to each person with computer access**

9. **Restrict physical access to cardholder data**

All the above requirements can be satisfied by having strong:

1. **Authentication**: Verify the identity of the request sender.
2. **Authorization**: Determine if the sender has access to the requested resource.
3. **Auditing**: Keep records of any attempts that access the resources process.

Figure 5 illustrates how DataPower implements these security measures using the aforementioned "AAA" action.
Figure 5. Security measures implemented by DataPower

The DataPower AAA action performs the three security processes mentioned above - authentication, authorization, and auditing:

1. In the first step, it extracts the identity token from the message. To verify the claims made by this token, the action authenticates it against either an on-board ID store or an external access control server. Once the client's identity has been confirmed, you have the option of mapping the client’s credentials to one of the users or groups defined by the service.
2. In the second step, the action extracts the requested resource form the message. It then checks if the authenticated user has permission to access the requested resource.
3. In the final step, the action performs auditing and accounting. The action records any access attempts, successful or unsuccessful, for monitoring and non-repudiation purposes. Additionally, the action can also perform post-processing steps, such as generating SAML or LTPA tokens for single sign on.

Regularly monitor and test networks

This section describes how to monitor and regularly test the PCI gateway.

10. Track and monitor all access to network resources and cardholder data

This requirement is met by maintaining a strict audit trail of all activities related to services that process cardholder data. This is what the internal controls of an organization mandates. While DataPower plays its part, all the players in the IT landscape need to follow these logging requirements.

DataPower supports off-appliance logging, using protocols such as syslog and syslog-ng, or by writing logs to a remote NFS mount. DataPower appliances never share their file system, but they can connect to shared file systems on other servers. There is a full suite of logging formats and protocols to use as well as a model for specifying event notifications at various levels or granularity.
The logging utility on the appliance works on the principle of publish and subscribe. Objects publish log messages. Log targets subscribe to message streams. More than one log target can subscribe to the same set of log messages. This allows the appliance to distribute log messages to multiple destinations, including network management consoles, file servers, and databases.

11. Regularly test security systems and processes

This requirement is met by having stringent testing policies in place. This requirement calls for testing security controls annually and running vulnerability scans quarterly. Penetration tests are run annually or after any significant change, such as introducing a new server, upgrading an operating system upgrade, or adding a sub-net.

Maintain an information security policy

This section describes using security policies with the PCI gateway.

12. Maintain a policy that addresses information security

The sub-sections of this specification require that an organization maintain an up-to-date security policy. This includes documents on daily operational security procedures, usage policies for critical technologies, defined information security responsibilities for all personnel, formal security awareness program, and an incident response plan.

You can use DataPower as the Policy Enforcement Point (PEP) to implement the security policies. These security policies are hosted by an external policy store, such as IBM® Tivoli® Policy Security Manager. They are designed to be "universally understood" by multiple software solutions.

XACML is an XML-based standard from the Organization for the Advancement of Structured Information Standards (OASIS) that is useful in expressing and evaluating access control decisions on a protected system resource. Figure 6 shows how DataPower can use its AAA framework to implement security policies, which are authored in XACML.
Conclusion

This article described how to position WebSphere DataPower for PCI compliance requirements. DataPower is not the "whole" solution, but rather a "part" of the PCI compliance solution. This article provided high-level information to start a conversation about PCI compliance. If you need a deeper dive, then a WebSphere DataPower services engagement would be the next logical step.

Acknowledgements

The author would like to thank Rafi Afzal for his review of this article.
Related topics

• Payment Card Industry (PCI) Data Security Standard
• OWASP Top Ten Project
• IBM Redbook: WebSphere DataPower SOA Appliances Part II: Authentication and Authorization
• Comment lines: Robert Peterson: High value features of WebSphere DataPower SOA Appliances that you're probably not using
• developerWorks WebSphere DataPower zone

© Copyright IBM Corporation 2012
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)