

Data: Transferring the Burden Under PCI DSS

Jonathan Lampe, Ipswitch - 08 Jun 2010

Despite widespread adoption of Simple Object Access Protocol (SOAP) and transaction sets in the financial industry, a surprising high percentage of the data flow is still represented by files or bulk data sets. In 2009, Gartner determined that bulk data transfers comprise around 80% of all traffic. This is probably a surprise if your company is among the many with millions invested in just managing individual transactions - but there are good management and security reasons for this continuing situation.

Why is File Transfer Still Common?

Financial institutions and item processors are still 'FTP'ing' (file transfer protocol), emailing, or sending and sharing files instead of transactions for a number of reasons. First, it helps hide the complexity of systems on both ends - there is no reliance and concern regarding libraries of transactions and responses related to one system and a different set related to another system. Second, it reduces the risk of transmission failure and makes it less risky for employees to send a small number of files or bulk data sets rather than a large number of transactions. Finally, it also increases the reliability of an overall operation.

The Managed File Transfer Industry

The managed file transfer (MFT) industry is comprised of providers whose solutions manage and protect these bulk data sets as they move between partners, business areas and locations. Collectively they address challenges presented by bulk data transfers and principles-based rules of the sort that have become common over the past few years - for example the Data Protection Principles or International Financial Reporting Standards (IFRS). Fundamentally, rules that tend to embody real-world outcomes as a standard. So, for example, the reported outcomes of penetration testing depend for certification as much upon the experience of the tester (who may be an employee) as upon the integrity of the network. This is all fine - until your network meets the real world. Principles-based rules tend to put the onus squarely on us to make and maintain systems.

For consumers, consultants and Payment Card Industry (PCI) assessors, this is undoubtedly 'a good thing'. For those handling card data, the costs of validated and effective compliance represent a potentially significant burden that's worth passing on to an industry that has quietly got on with the job well before buzzwords, such as 'cloudsourcing' or even 'outsourcing', entered the lexicon.

Vendors and Technologies Need Evaluation

It therefore makes a great deal of sense to place as much of that onus, and indeed risk and potential liability, on the shoulders of others - suppliers and consultants - as we can. Although PCI Data Security Standard (PCI DSS) can, and does, descend into tick-box detailed level rules in some places - which it makes very good

When evaluating for data security technology, a company should look at four categories: confidentiality, integrity, availability, and auditing. These headlines are designed to assist in assessing whether a data technology or process is likely to provide one-time compliance for the purposes of PCI DSS.

sense to sign off to trusted third parties - nevertheless, significant ongoing parts of our obligations under PCI DSS are essentially management issues. Despite subjective components and PCI requirements to take ongoing account of best practices, the technologies themselves can still be evaluated on a relatively straightforward mechanistic basis, provided that they are submitted to sufficient scrutiny.

At the most basic level, subjective terms such as 'adequate' or 'insecure' are sometimes to be understood (explicitly or otherwise) as denoting specific technologies or other standards in line with industry best practice and are, therefore, a route to initially evaluating software on a tick-box basis.

Beyond Ticking Boxes - Four Initial Considerations

When evaluating for data security technology in the context of regulated activities, you should look at how four categories - confidentiality, integrity, availability, and auditing - contribute to security and compliance. These headline considerations are designed to assist in assessing whether a data technology or process is likely to provide one-time compliance for the purposes of PCI DSS.

Confidentiality ensures that information can be accessed only by authorised individuals and for approved purposes. For the purposes of PCI DSS this means that employees should have the minimum level of access necessary to do their job. Confidentiality begins with authentication of login credentials on every secure application and starts with putting a strong password policy in place, with robust account expiry procedures and password management.

Integrity, as repeatedly addressed in PCI DSS rules 10, 11 and 12, is relatively under-appreciated and understood solely as a security issue, but is a critical component to compliance. It means ensuring the uncompromised delivery of data, with full Secure Hash Algorithm (SHA)-512 support. In the case of file transfer operations, non-repudiation takes data security to the highest level currently available by adding digital certificate management to secure delivery and data encryption beyond the requirements of PCI DSS. The setting up of alerts is a relatively easy goal - a box ticked on the route to compliance.

Availability is not explicitly addressed in PCI standards but is a critical component of any overall security strategy. It can and should be addressed, if not guaranteed, through load balancing and clustering architectures that support automatic failover and centralised configuration data storage to minimise the chance of a data breach.

Auditing capabilities should be demonstrated by vendors in the form of comprehensive logging and log viewing with tamper evident measures to guarantee the integrity of log files. For technology, security, and other auditing purposes, all client/server interactions and administrative actions should be logged.

The Hitchhiker's Guide to File Transfer in the PCI DSS Galaxy

The main body of the PCI DSS is divided into 12 requirements.

Section 1 establishes firewall and router configuration standards by requiring all managed file transfer (MFT) vendors to build a product architecture that puts a proxy, gateway or tiered application into a demilitarised zone (DMZ) network segment. This requirement also puts the actual storage of data and any workflows associated with it into internal networks.

The best architectural implementations ensure that no transfer connections are ever initiated from the DMZ network segment to the internal network. Typically this is accomplished using a pool of proprietary, internally established connections. In this way, clients can connect using FTP Secure (FTPS), Secure File Transfer Protocol (SFTP), etc to the DMZ-deployed device, but the transfers involving internal resources are handled between DMZ- and internally-deployed vendor devices by the proprietary protocol.

Section 2 demands that no default or backdoor passwords remain on the system and that systems are hardened. These best practices are generally enforceable with MFT technology, but the best implementations include a hardening utility that also extends protection to the operating system on which the MFT software runs.

Section 3, particularly subsection 3.4, covers encryption of data and storage of keys. To address these issues MFT vendors have an array of synchronous and asynchronous encryption technologies, such as OpenPGP, to

ensure data is secured at rest. Cryptography is almost always performed using Federal Information Processing Standards (FIPS)-validated modules and secure overwrite of data is commonly used.

Section 4 covers encryption of data in motion. All MFT vendors currently support multiple open technologies such as Secure Socket Layer (SSL), Secure Shell (SSH) and Secure/Multipurpose Internet Mail Extensions (SMIME) in multiple open protocols, including SFTP, FTPS and Applicability Statement 2 (AS2), to provide this protection.

Section 5 ensures anti-virus (AV) protection is in place for systems and the data that passes through them. Most MFT vendors provide the ability to provide both types of protection with their software. The best allow integration with existing AV implementations and security event and incident management (SEIM) infrastructure.

Section 6 requires secure systems and applications. Most MFT vendors conform to the guidelines here, particularly subsection 6.5 on web application security. However, there are large variations on fidelity to subsection 6.6 in the industry. The best vendors use a battery of security assessment and penetration tools, such as HP WebInspect and protocol fuzzers, to ensure that their software exceeds PCI security requirements - and remains that way from release to release. The best vendors also have multiple security experts working with developers to ensure new features are secure by design. These attributes are not always easy to find on a vendor's website, but they are critical to the long-term viability of an MFT application - be sure to ask.

Sections 7 and 8 cover the establishment of identity and authority. MFT solutions typically have built-in features that cover these issues from multifactor authentication to sharing of accounts. However, there are two common areas of difference between MFT vendors in these sections. The first is the ability to rapidly 'de-provision' users (i.e. disable or delete the account upon termination). The second is the proper storage of passwords: some vendors still use unkeyed hashes or weak Message-Digest algorithm 5 (MD5) hashes, both of which are susceptible to either rainbow table or collision attacks.

Section 9 is about physical access and is one that many software vendors erroneously ignore. However, subsection 9.5 is about off-site backups and is a function that MFT software often provides. One advantage of using an MFT solution for this purpose is that all the security benefits from the MFT solution flow into the backup process as well.

Section 10 is about auditing and visibility into data. MFT vendors also typically have a strong story around these attributes. Common features of MFT include visibility into the full 'life cycle' of files, aggregate reporting, detailed logging of every administrative action, and enforcement of specific service level agreements (SLAs). Some MFT solutions also ensure that audit logs and transfer integrity information are tamper-evident to ensure complete non-repudiation of data delivery.

Section 11 is about regular testing of systems and processes. As mentioned above, MFT vendors who perform these types of tests on their own solutions before releasing their software to the public should be sought out and preferred by companies that must adhere to PCI DSS.

Section 12 is about maintaining and enforcing a security policy down to the level of end user training. Like section 9, section 12 is another section many software providers erroneously ignore. However, the best MFT vendors know that providing fingertip reporting and good user experience to both administrators and end users can go a long way toward encouraging proper use of technology.

PCI DSS Appendices A ('Additional PCI DSS Requirements for Shared Hosting Providers') and E ('Attestation of Compliance - Service Providers') are also often used when managed file transfer services through virtual area network (VAN), software-as-a-service (SaaS), hosted or cloud providers are used. Key requirements here include ensuring that the service provider is not allowing shared users, that different organisations can only see their own logs and that the provider has policies that provide for a timely forensics investigation in the event of a compromise.

Summary

The substance of the PCI burden is an ongoing one. To look down the list of PCI requirements is to scan a list of joiners to 'maintain', 'monitor' and 'ensure', that echo the 'manage, monitor and secure' objectives of

basic FTP technology. However, and, as the March 2008 Hannaford data breach shows, it is possible to be ostensibly compliant - to have ticked all the boxes - and yet not be fully secure.

PCI DSS compliance requires organisations to protect the security, privacy, and confidentiality of information - and to document who accesses the information and the security measures taken to prevent theft, loss, or accidental disclosure.