KEMP | LOAD BALANCERS

Application Delivery in PCI DSS Compliant Environments

Technical White Paper

By Jason S. Dover, Director of Technical Product Marketing

Introduction

Protecting web applications is of critical importance for all organizations, especially those which process customer payments. In addition to general web application protection, all organizations that accept and process credit cards must also comply with Payment Card Industry Data Security Standard (PCI DSS) 3.0 requirements. Aside from the number of controls that must be implemented and processes that must be followed, application delivery technology, such as that provided by KEMP Technologies, further assists organizations with maintaining PCI compliance since the requirements have a targeted focus on the systems that serve applications.

The Cost of Data Leakage

Just over the last 5 years, security breach after security breach have broken records in terms of the amount of card holder data stolen in a single attempt as well as the financial impact on the compromised organizations. These breaches not only cause financial woes and class action lawsuits for companies that wind up at the wrong end but also can lead to irreparable reputation damage. Privacy Rights Clearing House points Chronology of Data Breaches identifies that over 608,087,870 records containing sensitive personal information were involved in security breaches in the US alone between 2005 and 2012. According to 2014 Internet Security Threat Report by Symantec, it's estimated that in 2011 alone, more than 232 million identities were exposed due to cyber security breaches and by 2013 that number almost doubled to more than 552 million. In terms of business impact, one study by the Ponemon Institute cited the cost to a company exposing sensitive data such as credit card information to be an average of $3.5 million per incident. In 2007, retailer TJ Maxx experienced one of the largest payment card leakage in history at the time at 45.6 million card numbers. The infamous Target breach of 2013 nearly rivaled that, resulting in 40 million compromised records and a $148 million loss to shareholders only to be quickly followed up by the now largest breach, in the Home Depot cyber-attack with estimates of payment information from 56 million cards having been put at risk costing the home improvement enterprise tens of millions of dollars to cover investigations, legal fees, enhanced support center staffing and credit monitoring services for customers.

While these were highly publicized and especially large cases, this crime is by no means uncommon. According to the 2013 Data Breach QuickView Report sponsored by Risk Based Security and the Open Security Foundation, in 2013 alone some 2,164 data breach incidents occurred exposing a total of over 800 million sensitive records with credit card and social security data making up a combined nearly 30 percent. Since data breach reporting requirements are not yet standardized or even mandatory, it's possible that the numbers are even higher. While some organizations may be lulled into a false sense of security that they are less at risk because of their size and scale, a recent Verizon data breach study found that nearly 75 percent of

data breaches that were analyzed involved businesses with less than 100 employees. What's more is that many organizations don't even realized that they've been compromised or at least not in a timeframe that puts customers and CISOs at ease. An article by Businessweek also detailed that three-year study by Verizon Enterprise Solutions identified that on average, enterprises discover breaches through their own monitoring in only 31 percent of cases and for retailers it's an anemic 5 percent. In the SMB arena the average time between breach and discovery is 8 months.

The net of the matter is that ANY company handling sensitive card holder data regardless of size is exposed to significant and multi-faceted risk and must make major considerations in order to mitigate the challenge of accepting and interacting with this data in the most insecure venue around – the internet.

PCI DSS – What and Why?

In order to mitigate these risks as well as comply with mandated requirements, organizations of varying size invest a great deal of time, effort and finances into technologies and frameworks that ensure that they achieve and maintain PCI compliance. This often drives a question from such customers directed towards technology vendors that they are evaluating for their infrastructure: "Are your products PCI compliant?" However, before we investigate the implications of that seemingly relevant question we first need to define what PCI DSS actually is.

Payment Card Industry Data Security Standards or PCI DSS is a set of standards for all organizations that process, store and transmit credit card information to ensure that they do so in a securely maintained environment. All organizations who fall into this category face a risk of PAN (primary account number) and other PII (personally identifiable information) of their end customers potentially being compromised and the requirements of PCI DSS help to minimize those risks by covering everything from the point of entry of card data into a system to how that data is processed, how the environment is audited and guidance for protection against application-targeted exploits. The PCI Security Standards Council (PCI SSC) was founded in 2006 by 5 major global payment brands – American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. and 4 of these companies originally incorporated the PCI DSS in 2004 as the requirements for their data security compliance programs.

The PCI-DSS defines six key objectives to ensure the security of infrastructures used for payment processing and prevention of PII misuse that can be summed up as follows

- *Maintenance of a secure network and systems*
  Covers the use of technologies such as firewalls as well as defines that factory supplied default authentication data and security parame ters be changed on network systems.

- *Protection of card holder data*
  Entails that controls be put in place to protect stored data against hacking and that effective encryption methods be used for data in transit.

- *Protection of systems against vulnerabilities and malicious activities*
  Mandates the use of regularly updated anti-malware software along with development of secure applications and use of protection methods such as web application firewalling.

- *Restricted access to system and operational information*
  Involves restriction of access to card holder data based on a need-to-know policy. In other words, card holders shouldn't be required to provide information unless that information is required for protection or to effectively complete a transaction. This objective also requires the implementation of controls that restrict physical access to card holder data.

- *Regular network monitoring and testing*
  Dictates that measures be enacted to ensure that networks security processes are behaving properly and that access to network resources and card holder data is tracked.

- *Implementation, maintenance and enforcement of a formal security policy*
  Requires that an information security policy be followed by all personnel along with audits and non-compliance penalties.

Each of these objectives are then further defined by 12 requirements that expand on testing procedures and guidance for satisfying each of them. Based on the context of these, we can see why the question at the outset of this section is often posed; the majority of these requirements apply directly to system or network components. However, it must be noted that PCI compliance in and of itself is not a certification that is granted to any device, appliance or network function but rather to an entire

deployment. Various vendor products may support satisfaction of PCI requirements through capabilities they provide but if improperly deployed or deployed in an environment with other violations the customer still would not be able to achieve compliance.

Implementation Challenges

As we're already starting to see, PCI DSS compliance is a complex arena to navigate and is the reason why a whole industry has been created around helping organizations meet the requirements. While the challenges for successful implementation are many, following are three common ones that many organizations face

- *Misconceptions*

One of the primary challenges to successful PCI DSS compliance is the misconceptions that surround the standards. In a paper published by the PCI SSC called "Ten Common Myths of PCI DSS" the number one item listed was that 'one vendor or product could make an organization compliant'. It points out that a "holistic security strategy that focuses on the big picture related to the intent of PCI DSS requirements" is what's actually needed in order to be compliant. That same paper lists the 4th most common myth as a belief that PCI DSS in itself will make an organization secure. In reality, while a successful pass of PCI DSS assessment is a great achievement and the right move for organizations handling card holder data, it's only representative of a snapshot in time. Since security exploits constantly evolve, compliance efforts must also be an ongoing cycle of assessment and remediation. Since some elements of PCI DSS are left to interpretation and security professionals may have strong and sometimes misplaced beliefs on the subject, misinterpretation is common. Seeing things for what they truly are and consulting with third-party objective specialists is critical to overcoming this first challenge.

- *Applying standards to virtualized and cloud environments*

Since the architecture and deployment of virtual technologies and cloud infrastructure can vary widely from environment to environment, organizations pursuing PCI DSS compliance must conduct in depth discovery and assessment to firstly, identify and secondly, understand all of the inner workings of their implementation and how the various components interact with payment processes and card holder data transmission and storage. Because of this, environment-specific controls are needed and will differ across organizations making it more difficult to implement.

- *Scale*

While it already has been noted that small organizations are by no means exempt when it comes to PCI DSS, this particular challenge primarily impacts larger companies. Since the majority of large entities such as banks, retailers and eCommerce companies have expansive card holder data processing environments it is far more challenging to meet PCI DSS compliancy since the sample size will be wider and addressing requirements at the various system and environment levels will be more costly and time consuming.

Keys to Successful Implementation

Organizations must recognize that achieving PCI DSS compliance and maintaining it are two distinct practices. Implementing the system controls and configurations to create a compliant deployment require one field of view and focus but maintaining them and preventing configuration creep entails that processes and measures be put in place that can be easily tracked and checked real time to keep from falling out of compliance.

An understanding of the 'systemness' of the environment and how different components and sets of components relate to one another is also critical as changes in one area can adversely impact others. For instance, credit card payment transactions often involve may different systems and because of this it's important to have clearly identified each and every system that participates in the process and to what degree. If even just one of the systems lacks the required controls, not only is it possible to fall out of compliance but even worse, it will often expose a vulnerability that could be exploited by attacks. Controls for regularly evaluating the functions of involved systems helps to minimize this risk.

It's claimed that writer Dick Brandon once said, "Documentation Is like sex: when it's good, it's very, very good; and when it's bad, it's better than nothing." When it comes to PCI DSS compliance documentation truly is king. Product, configuration, prior audit, process, chain of custody, workflow and personnel data are all needed for successful audits. Having the discipline to meticulously create, update and version control documentation and creating a culture that fosters and rewards this behavior are important steps to take in order to maintain compliance. Because of this it's vital that proper training be held with regular cadence for all employees that play a part, big or small, in the handling of card holder data.

Supporting PCI Compliance with Application Delivery Technology

Web facing applications are the leading target of cyber-attacks because of the potential gains that can be achieved by those who stage them. As seen by the earlier examples, significant losses can be inflicted on organizations that suffer breaches which result in compromised card holder data. Because of that it's key to

leverage technologies serving and delivering web facing applications that support the satisfaction of PCI DSS requirements. Application delivery controllers (ADCs), more commonly referred to as load balancers, have long been used to accelerate, scale and ensure the availability of web applications. Given their criticality to application deployments and key placement between clients and workload servers it's naturally expected by customers that they provide mechanisms to help organizations meet compliance.

KEMP's flagship LoadMaster ADC is delivered with support for private, public and hybrid environments and are compatible with deployment on a wide array of platform types making it easy for customers to scale and optimize their application infrastructures. Integrated distributed denial of service (DDoS) mitigation, intrusion prevention/intrusion detection (IPS/IDS), authentication verification and web application firewalling (WAF) help customers protect their deployment. Based on the fact that the ADC has a requirement to inspect incoming traffic, even in encrypted streams, it's an ideal placement for these types of services. While KEMP's LoadMaster ADC makes no claims of making an environment PCI compliant it definitely helps customers meet the requirements for their deployments and here's how.

- *Requirement 1.2: Deny traffic from untrusted networks and hosts*

  All systems in a PCI DSS complaint environment must be protected from unauthorized access from the internet, regardless of source and network firewalls play a key role in meeting this requirement. KEMP's LoadMaster with web application firewall protection further supports this by enabling the capability of limiting access to only explicitly allowed entities and using only the protocols that are dictated as allowable on published services. IP reputation checking and blacklisting also make it possible to explicitly prevent access to application services by untrusted networks and hosts.

- *Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters*

  Default passwords make up one of the easiest ways for hackers to infiltrate networked environments and exploit vulnerabilities. Failure to change default passwords at deployment is a leading contributor to successful attacks. To support this requirement, KEMP's LoadMaster products enable and require customers to change credentials at initial deployment to ensure that this task is always completed with every LoadMaster instantiation.

- *Requirement 3.3: Mask account numbers when displayed*

  While the parent objective of this requirement touches significantly on encryption at rest of data, requirement 3.3 primarily focuses on the obfuscation

of PAN data when it is displayed. KEMP's web application firewall engine can be easily configured through supplied and custom rules to look for patterns in web application server response data to prevent the leakage of sensitive personally identifiable information such as credit card and social security numbers.

- *Requirement 3.5: Protect encryption keys from disclosure and misuse*

The protection of cryptographic keys used to encrypt transmitted card holder data is imperative since access to these keys would result in the ability to decrypt data. The default protection afforded encryption keys by all KEMP LoadMasters is strong; all key exports can only be accomplished with strong passphrase protection. But by supporting FIPS 140-2 Level 2 compliance, the LoadMaster 5305-FIPS load balancer goes a step further, protecting encryption keys through the use of a readily auditable physical hardware security module while delivering the application delivery functionality and support for all other listed PCI requirements along with the entire LoadMaster family.

- *Requirement 4.1: Use strong cryptography and security protocols*

Since the internet is an open and public network, criminals can easily intercept cardholder data that is transmitted over it. For this reason, efficient and up to date encryption methods must be used for card holder data in transit. KEMP's LoadMaster provides a security overlay for applications, even which may have not been originally developed to leverage TLS (SSL) sessions, to improve infrastructure security. LoadMaster further extends capabilities for administrators to restrict ciphers that can be used to access protected services as well as enable re-encryption for terminated traffic streams to ensure secure end-to-end flows.

- *Requirement 6.6: Audit and correct application vulnerabilities or implement a web application firewall*

Application and system vulnerabilities are often used to gain malicious access to card holder data. PCI DSS requirement 6.6 stipulates that all compliant organizations address new threats and vulnerabilities on public-facing web applications on an ongoing basis and ensure that they are protected against known attacks by reviewing them via application vulnerability security assessment at least annually and after any changes or by installing an automated technical solution that detects and prevents web-based attacks (e.g. a web application firewall). It should be noted that these vulnerability scans and checks to meet this requirement are distinct from the assessments that must take place under other PCI DSS requirements. In order to reduce the amount of manual or automated checks that an organization must conduct as well as to ensure that protection is automated, the deployment of a web application firewall is often opted for. KEMP's web application firewall known as the

Application Firewall Pack (AFP) integrates one of the world's most deployed Open Source web application firewall engines, ModSecurity, augmented by information security threat intelligence and research, to comprehensively enable ongoing real-time protection against the latest application threats and prevent the exploitation of potential application code vulnerabilities. With a targeted focus on application-specific exploits missed by traditional firewalling techniques, AFP supports a defense-in-depth security posture, mitigates risk and helps organizations meet PCI DSS compliance.

Conclusion

While PCI doesn't guarantee that data breaches will never happen it does mean that an organization is doing their absolute most to keep customer data safe and out of the reach of malicious attackers. By maintaining secure systems, customer confidence and brand strength is built and organizations are better protected against always-evolving threats on the internet. The exercise of achieving and maintaining compliance helps companies better define their security strategy as well as improve efficiency across their IT ecosystem.

PCI DSS focuses on systems used to serve web applications and for this reason application delivery technology and its ability to help customers meet these standards plays a key role. Understanding how to leverage it in achieving and maintaining a PCI compliant environment should be a definite consideration for organizations that are chartered to do so. KEMP's LoadMaster platform enables organizations to address many of the core requirements and has proven to be a valuable asset to many for securing their web application infrastructures.