A Survey of Payment Card Industry Data Security Standard

Jing Liu, Yang Xiao, *Senior Member, IEEE,* Hui Chen, *Member, IEEE,* Suat Ozdemir, *Member, IEEE,* Srinivas Dodle, and Vikas Singh,

***Abstract*—Usage of payment cards such as credit cards, debit cards, and prepaid cards, continues to grow. Security breaches related to payment cards have led to billion dollar losses annually. In order to offset this trend, major payment card networks have founded the Payment Card Industry (PCI) Security Standards Council (SSC), which has designed and released the PCI Data Security Standard (DSS). This standard guides service providers and merchants to implement stronger security infrastructures that reduce the risks of security breaches. This article mainly discusses the need for the PCI DSS and the data security requirements defined in the standard to address the ongoing security issues, especially those pertaining to payment card data handling. It also surveys various technical solutions, offered by a few security vendors, for merchant companies and organizations involved in payment card transaction processing to comply with the standard. The compliance of merchants or service providers to the PCI DSS are assessed by PCI Qualified Security Assessors (QSAs). This article thus discusses the requirements to become PCI QSAs. In addition, it introduces the PCI security scanning procedures that guide the scanning of security policies of a merchant or service provider and prepare relevant reports. We believe that this survey sheds light on potential technical research problems pertinent to the PCI DSS and its compliance.**

***Index Terms*—Payment Card Industry, Data Security Standard, Security.**

I. Introduction

ACCORDING to a series of biennial surveys issued by Dove Consulting and American Bankers Association (ABA) [24], payment cards, such as credit, debit, and prepaid cards, are becoming an increasingly dominant method of conducting commerce across three important payment venues: in-store purchases, Internet purchases, and bill payments. The above surveys indicate that cash and check payments are declining and that electronic payment methods are gradually taking over. For example, in 2005, cash and check payments accounted for 45% of the total monthly payments, down from 49% in 2003 and 57% in 2001 [24]. Due to the convenience that payment cards can provide and new payment innovations, this trend is likely to continue [24].

Manuscript received 29 October 2008; revised 15 July 2009.

Jing Liu, Yang Xiao, Srinivas Dodle, and Vikas Singh are with Department of Computer Science, The University of Alabama,Tuscaloosa, AL 35487-0290 USA (e-mail: yangxiao@ieee.org).

Hui Chen is with Department of Mathematics and Computer Science, Virginia State University, Petersburg, VA 23806 USA.

Suat Ozdemir is with Computer Engineering Department, Gazi University, Maltepe, Ankara, Turkey, TR-06570.

Digital Object Identifier 10.1109/SURV.2010.031810.00083

Payment cards involve many players, including merchants, payment card issuers, merchant-acquiring banks, and payment card networks. Service providers and merchants are responsible for managing huge amounts of payment card data. For example, when a person buys something from a retailer using a payment card, the card must be verified with the card issuer via the retailer's merchant acquiring bank and the corresponding payment card network. After a successful verification, the amount of purchase can eventually be debited to the payment card account. This often requires the retailer to collect and store the payment card information and the transaction information in its computer systems, and to send the information over network to the card issuer. A security breach on a merchant's or a card issuer's database system may expose important payment card information, which can in turn cause significant damage to card users, merchants, and card issuers.

Major payment card networks have developed their own security programs separately to counter security breaches and credit card fraud. Examples of such programs include Visa Card Information Security Program (CISP), MasterCard Site Data Protection (SDP), JCB Data Security Program, Discover Information and Compliance, and American Express Data Security Operating Policy [1]. Compliance regulations were not very well organized and were fragmented, and therefore did not lead to much success. Facing growing concerns for security breaches, major payment card network operators jointly founded the PCI Security Standards Council (PCI SSC) in 2004. Then the council released the PCI Data Security Standard (DSS) on December 15, 2004, and updated this standard to versions 1.1 and 1.2 in September 2006 and October 2008 for minor revisions and clarification [1], [2], [3], [28]. In addition, the PCI also publishes PIN Entry Devices Security Requirements and Payment Application Data Security Standard (PA-DSS), and the information regarding Qualified Security Assessors (QSAs), Payment Application Qualified Security Assessors (PA-QSAs), and Approved Scanning Vendors (ASVs) in their web sites.

The PCI DSS basically standardizes a set of practices and measurements to secure sensitive cardholder data. It guides merchants, service providers, and acquirers involved in dealing with payment card data and helps prevent the risk of credit card fraud [3]. Moreover, it provides enhanced and consistent standards and practices to secure the payment card transaction data and hence provide a high degree of confidentiality and

integrity to stakeholder information [2]. The PCI DSS is now managed by the PCI SSC whose members are from various participating organizations besides the founding payment card networks [4].

In this article, we discuss the need for the PCI DSS in Section II by quoting interesting security breaches that took place in recent history. Section III gives a brief overview of the transaction process. Section IV discusses in detail the actual standard's set by the PCI SSC and various issues with the standards. Section V presents the PCI in present Information Technology (IT) context. Section VI discusses the solutions provided by various vendors to merchants and service providers that are involved in credit card transactions to comply with the standard. Section VII introduces the requirements of the PCI Qualified Security Assessors, and Section VIII shows the PCI Security Scanning Procedures. Finally, we conclude the topic in Section IX.

II. Background

On the one hand, the usage of payment cards keeps growing, and on the other hand, high-profile security breaches of payment cardholder data appear annually.

In February 2003, a credit card processing company, Data Processors International, lost five to eight million credit card account numbers [25]. Apparently, it is a result that an intruder broke in one of the company's computers. It was estimated that it would cost the relevant credit card companies $200 million just to replace the affected cards [25].

In 2005, ChoicePoint was a victim of Nigerian identity thieves who stole personal information of around 163,000 customers [1], [5]. ChoicePoint was fined $10 million in civil penalties and $10 million to recover victims of the attack [5]. There was a loss of sensitive and personal data in around 365 reported security breaches during the year 2006, and Visa alone issued a total of $4.4 million in merchant fines [2].

In 2006, Circuit City lost nearly 2.6 million cardholders' account information [6]. The reason was disclosed that Chase Card Services, the cooperative credit card institution, falsely discarded five hard disks [6].

Hotels.com Data Breach reported on June 2, 2006 that the personal information of its 243,000 customers was compromised [6]. This occurred because a laptop was stolen from an Ernst & Young employee. The theft occurred in late February, yet Ernst & Young did not report it to their client, Hotels.com, until May 3, 2006 [6].

Account information of 45.7 million cardholders in TJX was compromised from January 2003 to November 2003 due to a security breach on their computer systems [7]. It was found that TJX did not report this for a long time and also that they had deleted data pertaining to the transactions between the time of occurrence and the time of detection [7].

Incidents like the above demand an urgent requirement for enhancements in the present standards of the payment industry. The Federal Trade Commission puts in an effort to ensure enough protection on stakeholder information [2]. Companies failing to protect this data are prone to civil cases pursued by the Federal Trade Commission [1]. Despite these regulatory measures, security breaches and hacks on payment card holders' information remain frequent [8]. For example, it is estimated that online credit card frauds alone cost $3.2 billion in 2007 [1]. Under pressure from the general public and from legislative bodies at various levels, credit card companies, especially the credit card network operators, were motivated to develop a new standard for an additional level of protection for the customers. Nevertheless, the PCI DSS become technical and operational requirements for both merchants and service providers to protect cardholders' data. Compliance to the PCI DSS would help merchants and service providers to prevent and detect security breaches, and to limit loss of cardholders' data in case of security breaches, and thus reduce occurrences of similar incidents outlined in this section.

III. Payment Transactions architecture

A payment card transaction generally consists of two steps: transaction flow and clearing and settlement [9].

A. Transaction Flow

As illustrated in Fig. 1, a transaction process begins when a cardholder swipes a card on a payment terminal or enters the details of a card onto an E-commerce website [9]. The merchant that operates the terminal and the website records the type of card, account number, expiry date and other codes. It then forwards the card data and the transaction amount to a merchant-acquirer. A merchant-acquirer is a financial institution which is responsible for its merchant-customers' transactions with payment card networks. There are two different models. Payment networks such as Visa and MasterCard do not directly issue cards to customers. Instead, cards are issued through their member financial institutions. Other payment networks such as Discover and American Express can issue cards directly. In other words, Discover and American Express play two roles in Fig. 1: merchant-acquirer and payment network. After that, the acquirer forwards the transaction data to the card issuer via a secure payment card network.

The issuer checks the account status in the database and replies to the acquirer. The acquirer then forwards the authorization code to the terminal device [9]. In certain cases, the acquirer might authorize directly without sending the transaction data to the issuer. This complete process might differ in some countries.

Notice that the transaction flow does not result in an actual collection of funds at that time, even though the sales process proceeds at the merchant location [9]. Instead, it is simply a confirmation that the issuer authorizes the transaction and agrees to settle this transaction with the acquirer and its merchant customer. In general, small merchants send the details of the daily transaction to the acquirer at the end of the day, and large merchants send the details on a real-time basis. The process of collecting the funds from the issuing bank and reimbursing the merchant can only start after the transaction details are sent to the acquirer. The process is referred to as the "clearing and settlement" process or the "settlement" process [9].

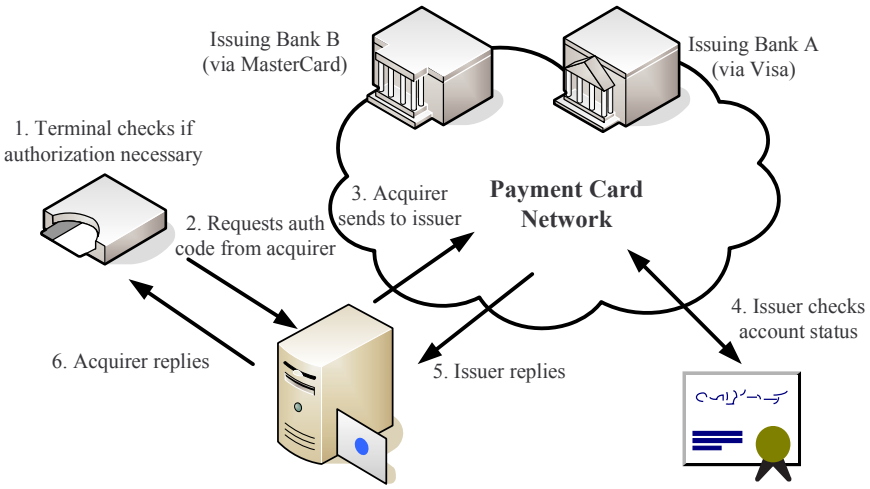


Fig. 1. Transaction Process [9]

B. Clearing and Settlement

In the clearing and settlement process [9], after the acquirer receives the transaction details, the acquirer sends the data to the appropriate payment network (such as Visa, MasterCard, etc.), by which the transaction data is guided to the respective card issuers. The issuer then charges respective card holders for the transaction amount and remits funds less the issuers' fee through the network to the acquirer. The acquirer then subtracts the fees for the issuer, the network, and itself, and then deposits the rest of the fund to the merchant's account with the acquirer. Typically, the customer is charged and the merchant is funded within 24-72 hours.

C. Scope of PCI DSS

In Fig. 1, it is clear that, merchants, especially large merchants, merchant-acquirers, payment networks, and card issuers hold large amount of sensitive data. These entities can also contract any number of functions to third parties, which are often referred to transaction processors, such as Data Processors International mentioned in Section II. Loss of this data often leads to significant financial and non-financial damage. The PCI DSS aims at improving data security for merchants and various payment card service providers. The PCI DSS applies to entities that store, process, or transmit cardholder data, and technical and operational system components included in or connected to cardholder data [10]. An entity as such is either a merchant or data processor, and sometimes, we refer it as an organization in this article. However, it does not apply to the payment card networks which standardize and mandates the compliance of the standard.

IV. PCI Data Security Standard

The PCI DSS sets 12 security requirements and classifies them into 6 main groups, which are known as "Control Objectives" [10], shown in Table I. The following discussion of the PCI DSS is based on the PCI DSS version 1.2. The comparison to its earlier versions can be found in [11] and [28].

A. Build and Maintain a Secure Network

As a few examples in Section II shows, hackers can exploit weakness and vulnerability of merchants' networks and computers to gain access to payment card data. Firewalls play an important role in the protection mechanism by controlling the traffic to and from the company's network, including its sensitive internal network [2]. Thus, the PCI DSS requires an organization to install and maintain a firewall configuration to protect its network and computer systems, and thus protect cardholder data.

Nevertheless, an organization must have a formal process to approve and test external connections and changes to firewall configurations. The standard demands a justified documentation of unapproved or risky protocols, a description of network managing groups, roles and their responsibilities, and lists of services and ports needed to operate the business. It also requires a review of the firewalls and router settings on a quarterly basis. Every connection from an un-trusted area must be blocked by the firewall.

In addition, the PCI DSS recommends a three-leg firewall configuration among the Internal Network Zone (INS), the Demarcation Zone (DMZ, sometimes also perimeter network), and external networks of an organization as depicted in Fig. 2. The INZ stores the payment card data. The DMZ hosts servers accessible from external networks. The organization is required to implement a firewall for each interconnection between the DMZ and the INZ and that between the DMZ and external networks. DMZ, unlike internal network, isolates sensitive shared information and private data from external networks. To deny accesses between cardholder databases and external networks, the firewall must filter out direct traffics between the INZ and external networks [3], [10]. The other measures to be taken as part of firewall configuration standards include stateful inspection (dynamic packet filtering), segregating the database from the DMZ by placing it in the INZ, securing and synchronizing the router configuration files, implementing perimeter firewalls and personal firewall software wherever necessary, and implementing IP masquerading and RFC 1918 address space to prevent revealing internal addresses.

TABLE I
PCI DSS VERSION 1.1 [10]

Control Objectives	Security Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	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
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

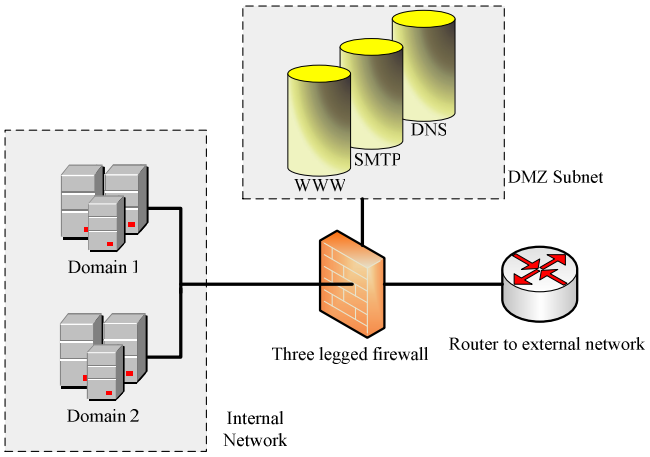


Fig. 2. A common implementation of the firewall within a company's intranet has a DMZ (Demarcation Zone), and an internal network where the most sensitive data is stored to protect it from unauthorized access

Vendor default passwords and settings are easily accessed and used by hacker communities to compromise the systems. To overcome such situations, the standards recommend changing the default settings (e.g., passwords). Wireless vendor defaults like wireless encryption keys, and Service Set Identifier (SSID) must also be changed [10]. SSID broadcasts must be disabled and strong encryption such as WiFi Protected Access (WPA) should be enabled for both authentication and encryption [10]. There are some other requirements for this control objective, i.e., 1) implementing separate servers for each of primary functions, 2) developing configuration standards, 3) disabling services, protocols and functionalities that are not required and risk prone, and 4) encrypting non-console administrative access via VPN, SSH, and anything similar [3].

B. Protect Cardholder Data

The stored data should be encrypted so that intruders cannot make sense of the data even if intruders break the firewall or gain access to physical storage [10]. The PCI DSS also recommends several other measures to protect cardholder data.

Firstly, an organization should minimize the cardholder data storage and limit the retention time in accordance with business, legal, and regulatory purposes [3]. Also, an organization should not store full contents of any track from a magnetic stripe, as well as the card-verification code, and Personal Identification Number (PIN) [10]. Also, at the minimum, an organization should render the Primary Account Number (PAN) into an unreadable form when stored via using pads, index tokens, truncation, and strong one-way hash functions or a strong cryptography with an appropriate key-management procedure [10]. Encryption keys utilized for encrypting cardholder data must be restricted to the fewest numbers of custodians and stored securely in as few locations as possible [3]. Implementing and documenting key management procedures by following strong key generations, periodic key changes, old key destructions, unauthorized key substitution preventions, dual key control establishment, suspected and known key replacements, and signed acceptance from key-custodians of their responsibilities are also significant measurements required by the PCI DSS [10].

In order to protect sensitive cardholder data during transmission, strong cryptographic and security protocols like Internet Protocol Security (IPSEC) and SSL/TLS must be used [10]. Cryptographic libraries like certified AES and 3DES are encouraged [3]. In wireless environment, Wired Equivalent Privacy (WEP) is considered obsolete. At least, technologies such as WPA, WPA2, VPN, and SSL are supposed to be used [10]. Also, access control based on physical addresses is required, and unencrypted PANs must be restricted from being sent through e-mails [10].

The study in [3] indicates that cryptographic key management is more important and difficult when compared to the encryption itself. Enterprise Key Management Infrastructure (EKMI), which achieves key management through standardized protocols, implementation guidelines, and controls, is a potential solution for the companies under the PCI compliance, though it has certain hurdles, like digital certificate protection at client machines, which requires a hardware security model [3].

C. Maintain a Vulnerability Management Program

Malicious software, i.e., Malware, including viruses, worms, and Trojans can give access to unauthorized and malicious people [2], [10]. Malware can even enter a computer system via legitimate means such as e-mails and portable computing devices (e.g., laptop computers, PDAs, and smart phones) and storage devices (such as flash drives). Since anti-virus software is capable of removing or quarantining known Malware, and

it is able to generate audit logs actively, the PCI DSS suggests deploying it in vulnerable systems [10].

Unscrupulous individuals, like hackers, gain unauthorized access to systems by using security vulnerabilities [3]. Because vendors' security patches may fix the majority of bugs, installing the latest official security patches no later than one month after the release is recommended. A formally established process is also required to identify newly discovered vulnerabilities [3]. That means that organizational standards need to be updated to handle new vulnerability issues. Moreover, all of the patches must be tested before deployment. Generally speaking, there should be separate environments and duties for development, testing, and production. Of course, production data cannot be used for testing, and test data need to be removed before activating production data [10]. Before being released, the code must be reviewed thoroughly to detect coding vulnerability. In addition, change control procedures must be followed for changes in both software and hardware configurations [10]. They should include impact documentation, operational functionality testing, back-out procedures, and management sign-off. In certain cases, developing web applications must follow the *Open Web Application Security Project Guide*. Common coding vulnerabilities, such as invalidated input, cross-site scripting attacks, injection flaws, buffer overflows, broken access control, and so on, should be prevented [10]. Public-facing web applications need to be protected by installing a firewall layer in front of them or by reviewing them for vulnerabilities with the help of security specialists [10].

D. Implement Strong Access Control Measures

As the PCI DSS mentioned, the data must have access control, and only those having business needs can be allowed to access the data. That means that only the authorized entities can access the critical information [3]. For systems with multiple users, one may restrict the critical resources based on a need-to-know mechanism, or "deny all" access unless specifically admitted [10].

The standards also mentioned that, each person with computer access should be assigned an ID, which makes him/her accountable for his/her actions [3]. To begin with, all users should provide a unique identification such as username, password, token device, or biometric [10]. Relevant technologies may involve RADIUS, 2-factor authentication, TACACS with tokens, and VPN with personal certificates. Besides, all of the system access codes must be encrypted before being transmitted and stored. Password management is necessary in each component, as well as user authentication, especially for system administrators [3]. In addition, any changes in data of users' identifiers must be recorded.

More specifically, the PCI DSS establishes a set of rules for access control: 1) before resetting password, the user identity should be verified [3]; 2) the default password for every individual must be unique and has to be reset after user login; 3) revoke the access immediately once it is terminated; 4) delete inactive users at least every 90 days; 5) disable vendor's account for remote maintenance unless it is really needed [10]; 6) distribute password policies and procedures to those who can access the cardholder data [10]; 7) user accounts and passwords are not allowed to be shared in a group; 8) passwords should be changed every 90 days, and the minimum length is seven characters, where alphabetic and numeric characters are both required [10]; 9) any of the last four used passwords cannot be submitted as a new one; 10) the user whose repeated access attempts are over six times should be locked out; 11) the lockout time can be half an hour or set by the administrator [3]; 12) if a session idles for over 15 minutes, the password should be re-entered to re-activate it; 13) all accesses are needed, even from administrators, to any database storing cardholder data [3].

Since only authorized personnel are allowed to access to cardholder data, it is required to limit every possible physical access to cardholder data or system devices. To limit and monitor those physical accesses, appropriate control strategies and cameras should be deployed at facility entry and sensitive areas, respectively, unless restricted by law [3]. The monitor log or footage should store for at least three months [3]. One also should restrict the use of wireless and Internet access points, handheld devices, and gateways [3]. In addition, one needs to set up a proper inspection routine to effectively distinguish visitors from employees, especially in confidential areas [10]. Usually, every authorized visitor will be assigned an appropriate physical token, such as an access device or a badge with a valid duration, to indicate as a non-employee [10]. When they are about to leave the facility or the tokens expire, they must surrender the physical tokens [10]. Visitor activity should be recorded on a physical log file for at least three months, unless restricted by law [10]. In the same manner, backup media files in a safe and off-line facility (e.g., commercial storage device or third party) [10]. For the media (e.g., paper or electronic devices) that contain cardholder data, one not only should physically secure them, but also maintain a strict distribution control procedure [3]. Generally, before sending those media via secured courier or similar traceable agency, they should be labeled as confidential packages [10]. Meanwhile, if the media comes from a secured area, management must approve the action [10]. Besides, the accessibility and storage of those media require strict control strategy too. The media inventory should be stored securely. While those media are useless for legal or business reasons, they must be destroyed permanently [10].

E. Regularly Monitor and Test Networks

The PCI DSS demands that all accesses to cardholder data and network resources should be tracked and monitored. Using log files or audit trails, critical activities can be tracked and analyzed in a further step if something goes wrong. Without the log files and audit trails, it would be difficult to determine the cause of any problem [10]. Thus, logging mechanisms are critical for tracking the activities of users. In addition, establishing a process to link every access from a single user to system components is required. To determine whether a user has accessed cardholder data, audit trails should be recorded for all system components automatically [3]. All invalid actions and logical access attempts with administrator privileges should be recorded in associate with the authentication and

identification mechanisms. For all system components, audit trail entries like user identification, event type and time, success or failure indication, event origination, and affected data identification, should be recorded. Meanwhile, clocks and times in critical system components should be synchronized. Moreover, make sure that the audit trails are secured so that they can be viewed by only authorized users, and can never be changed [10]. In order to do so, there should be stored in a centralized safe area [10]. According to the PCI DSS, change detection or file integrity monitoring software should be deployed. Therefore, any change on log files will generate an alert [10]. The logs for each system component, especially the security functions, should be reviewed daily [10]. The history of audit trails should be kept for a period due to effective use and legal rules [10]. The preferred strategy is to keep them at least one year with no less than 3 months available for immediate analysis [10].

New vulnerabilities should be identified regularly and continually, especially after maintaining or updating system components [10]. Network connections, security controls, and limitations or restrictions must be tested routinely so as to ensure that any unauthorized access is adequately handled [10]. To identify all wireless devices work well, wireless analyzers should be periodically used [10]. If there is a new system component installation, or there is a new network topology, all internal and external vulnerabilities scans should be performed. Even if there is no change, the scans should still be run quarterly [10]. The scans must be performed by a PCI qualified scan vendor. Penetration testing should be done on network infrastructure and application level at the minimum once a year, or whenever there is a significant modification or upgrade [10]. Besides, all prevention and intrusion detection engines must be updated regularly [10]. Network traffic should be monitored using host or network based intrusion detection systems. Meanwhile, relevant persons should be alerted about suspected compromise [10].

F. Maintain an Information Security Policy

This control objective defines information sensitivity and employees' information protection liability [10]. This policy should be established to address all requirements in the specification [10]. On the one hand, an organization should annually identify vulnerabilities, threats, and results in formal assessments [10]. On the other hand, daily tasks, like user accounts maintenance and review procedures, are also needed [10]. Policy updating should be performed once a year, or during environment changes [10].

Usage policies should be developed for employees using critical devices or technologies, such as remote-access technologies, wireless technologies, removable electronic media, laptops, PDAs, and even e-mails [10]. These policies must require authentication for the use of the technologies, and there should be an explicit management approval [10]. Hence, a list of all critical devices should be maintained, and each device must have a label stating the owner, owner's contact information, and purpose [10]. Moreover, all of the products used must be evaluated and approved by the organization [10]. Remote-access sessions should be automatically disconnected after a specific period of inactivity [10]. In other words, remote-access technologies can be activated to a vendor only when needed and should be deactivated immediately after use [10]. The cardholder data, when accessed remotely, should not be allowed to be stored on any local or removable physical media [10].

There should be proper documents that clearly define security policies and procedures. First of all, the responsibilities should be distributed to employees that will implement and monitor those procedures [10]. Then, monitored and analyzed security alerts should be forwarded to appropriate personnel [10]. At last, establish and document a security incident response and escalation procedure [10]. To monitor and control the access to data, all user accounts should be administered for additions, deletions, and modifications [10]. Another issue worth to mention is that, all employees should guarantee in writing that those policies and procedures are fully understood [10]. All individuals should be screened regularly to avoid the internal attacks [10].

There should be a proper contract stating the responsibility of a third party with access to cardholder data [10]. Each payment card brand, acquirer, and merchant that possesses cardholder data are supposed to declare ownership, and acknowledge the legitimate usage of those data [10]. A provision should be in place to state that the third party will continue to protect the cardholder data even after the termination of the contract [10].

The company should have an emergency response strategy in the case of a system breach [10]. There should be a solid plan to deal with solutions like business recovery and continuity procedures [10]. It should be tested at least once a year. Sensitive data should be monitored by trained personnel 24 hours a day, 7 days a week [10]. Intrusion detection and prevention, and file integrity examination should be provided [10]. There should be an appropriate process to update those plans based on the prevention experience and the industry developments [10].

V. PCI IN PRESENT IT CONTEXT

Fig. 3 shows an example of retail IT infrastructure with regarding to the PCI. It can be divided into five major subsystems: store environment; e-commerce environment; back-office and ERP systems; business administration environment; information technology department and its development, testing, and implementation environment. Each subsystem must be mediated by firewalls. Key components can be elaborated as shown below,

- *Electronic Point of Sale Equipment (EPOS)*: An EPOS is a payment terminal at the retailer [2]. It is a customer-facing environment and responsible for collecting transaction data and cardholder data. The PCI DSS requires that the Point of Sale (POS) environment or device must not store or retain sensitive data at all, even in the encrypted form. In some implementations, a POS terminal contacts an acquirer for payment card transactions. The POS terminal can use a phone line and a modem to communicate with the acquirer via asynchronous protocols such as Visa-1 and Visa-2, via synchronous protocols

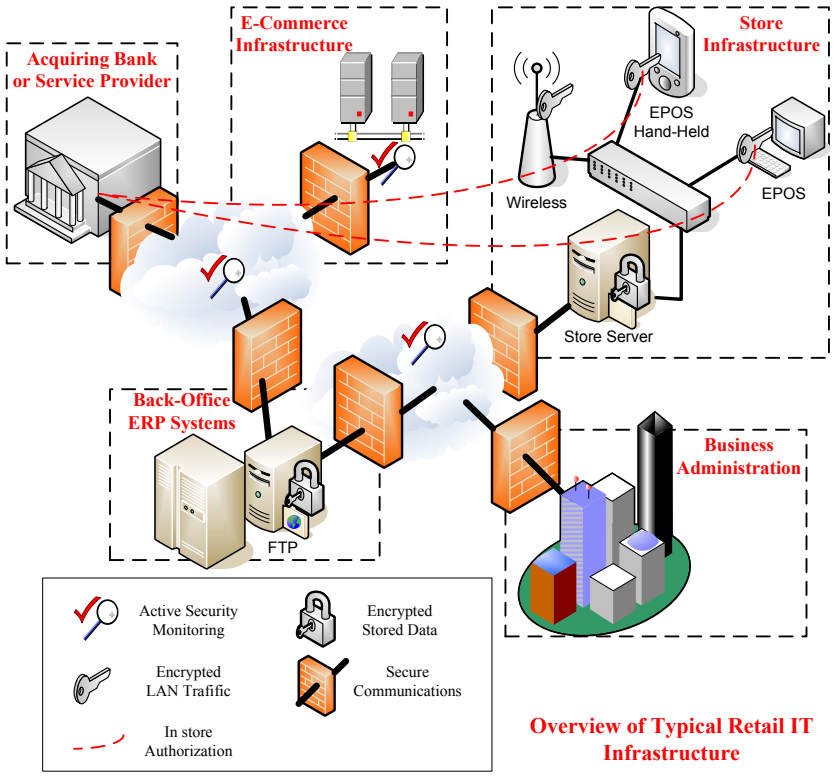


Fig. 3. PCI in retail IT infrastructure context [2].

such as ISO 8583/SDLC. The POS terminal can also use the Internet Protocol (IP) to communicate with the acquirer. An IP connection can be obtained via plain-old-dial-up, DSL, Cable Modem, Leased Lines (such as T1), Ethernet, and even satellite. However, more than often, the POS terminal only forwards the transaction data to a store server, and the store server communications with the acquirer via an IP connection. Any communication between the EPOS device and the store server must be encrypted [2]. Large retailers often create virtual private networks for their stores, and thus the transaction data are first transferred in their Intranet and aggregated in a server in their back-office, and it then in turn communicates with the acquirer via secure connections, usually via IP connections. The PCI DSS requires that any network connection that transmits cardholder data must be encrypted.

- *Store Server*: It is the repository of cardholder data and the associated transaction data. The data must be encrypted. Even if an intruder gains access to the system, the data should not be understandable. Thus, the encryption of this data should be separated from the operating system. A store server also runs store applications such as inventory replenishment and accounting, and labor management.
- *Applications*: Connectivity between the POS environment and the applications must be mediated by a firewall [2]. All data transmitted must be encrypted [2].
- *E-commerce Site*: Like an EPOS device, the E-commerce portal website must be separated from the rest of systems using firewall [2]. When sensitive data are transmitted between the site and the Internet, the portal site must encrypt the transmission [2].
- *Database*: The databases and applications must have a production environment that is physically and logically separated from the test and development environment [2]. The applications, databases, and portal sites should reside on separate, physical, and server infrastructure [2].

The user management and segregation of duties are done as following. Each individual user's role is defined according to job function and uniquely identified [2]. Monitoring and assessing the rights must be done in real-time. Users of central repository should be controlled and administered and locked-down instantly whenever necessary [2].

VI. Solutions from Various Companies

We will introduce several PCI compliance solutions from selected companies in this section. Most companies' products only address partially the PCI DSS requirements. We give a brief comparison of a few products surveyed in this article in Table II.

A. Vormetric Solutions

To safeguard sensitive customer data from unauthorized individuals and from misuse, Vormetric introduced the CoreGuard information protection system [12]. The system integrates several feasible technologies into a centralized management system that is suitable in a heterogeneous network environment. Its functionalities mainly involve high speed data encryption, comprehensive access attempts auditing, context-aware access control, and integrity protection of applications and hosts [12].

TABLE II
COMPANIES' SOLUTIONS FOR THE PCI DSS

Company	Solution	Focused Requirements
Vormetric	CoreGuard	3, 4, 6, 7, 10
Oracle	Oracle DB	3, 7
Motorola	KMF	4
Endava	CMDB	1, 3-7, 10, 12
Decru & NetApp	CardVault	1, 3-7, 9-10
Altiris	SecurityExpressions	10, 11, 12
Secure Works	iSensor IPS/IDS	1-12

The high-speed data encryption provides transparency to the application and network layers using an AES (128/256-bit) algorithm [12]. For common file system management operations without exposing the contents of the files, only the contents of files are encrypted, and the file system metadata are kept in clear data. In addition, the system has secure key management including secure key generation, distribution, storage, hot backup, and rotation [12].

The access attempt auditing has functions of administrative alert and event logging, deriving from IT governance policies and procedures that are cost and time effective [12]. It provides host and application integrity protection that prevents viruses and unauthorized codes from running on the network [12]. In addition to these functionalities, it also provides several advantageous capabilities, like disaster recovery, high availability, and failover to safeguard the encrypted data [12].

The context-aware access control is a host-based function that can block the unauthorized users to access data [12].

The integrity protection function and the above capabilities are provided by its information protection system. The architecture of the system is depicted in Fig. 4. Two major components are the Policy Enforcement Module (PEM) and the Security Server Appliance.

The CoreGuard PEM is a thin software module that can intercept file system calls and examine the context attributes [12]. With this capability, CoreGuard is able to check every access attempt to see whether it violates audits and predefined policies. The PEM is specific to the Operating System (OS) platform and provides transparency. It includes various storage technologies like DAS, NAS, SAN, etc [12].

The CoreGuard Security Server Appliance is a mountable hardware, which supports multiple PEMs and provides policy management, secure key management, policy violations, and file access attempts monitoring and auditing [12]. To achieve high availability, these servers provide multi-path redundancy. They are configured in clusters and managed centrally, which help the organizations to protect the data [12].

Separating the above two components in the CoreGuard design enables separate management of the host-server platform for the IT administrators and the policy for the security administrators [12]. This shows the highly secure nature of the CoreGuard design for host protection. In practice, the PEM can connect to the security server appliance in three modes [12]. The highest security mode is "No Caching", in which all security keys, together with their corresponding protection policies, are stored on the security server appliance without appearing on the PEM protected host [12]. In "Caching in Memory" mode, if those credential information is stored in

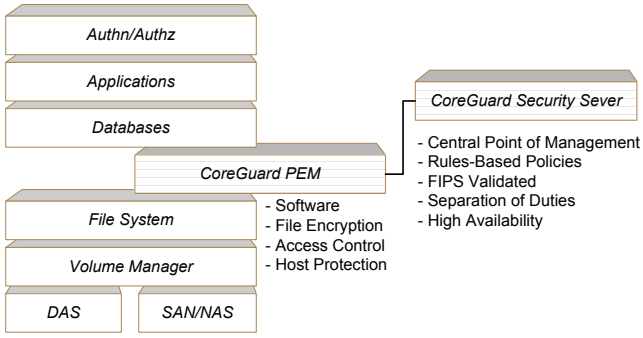


Fig. 4. The CoreGuard architecture within an integrated solution [12].

the non-swappable volatile memory, they will appear on the PEM [12]. The third mode is the "Caching on the Local Disk", in which the PEM is allowed to store those credential data on the local disk [12].

The CoreGuard information protection system has already been adopted by many leading corporations in various sectors. This system focuses on the PCI DSS requirements related to cardholder data protection and access control [12].

B. ORACLE Solutions

Oracle provides encryption techniques to protect data stored in Oracle relational databases. There are two main encryption techniques: DBMS_CRYPTO and TDE (Transparent Data Encryption) [13]. These techniques can be used to protect selected columns in database tables.

DBMS_CRYPTO, formerly DBMS_OBFUSCATION, has useful factors, depending upon the people using this encryption. One has to manually program encryption/decryption into existing applications [13]. This factor provides encryption based and fine grained access control to sensitive data. Users are responsible for managing the keys at the risk of losing encrypted data because once the keys are lost, the user cannot decrypt the data. DBMS_CRYPTO has extensive control options such as the number of keys generated, manual salt generation, choice of algorithms, and chaining mode [13]. This provides limited transparency to the encrypted data. The data is stored in raw format, and customer programming is required in order to use the encryption [13]. The technique has a few advantages, such as, 1) it encrypts only the sensitive data, which results in minimal performance impact; 2) it keeps the encryption transparent to the application; and 3) it is easy and secure [13].

In TDE process, the security DBA first opens a wallet that contains a master key [14]. This master key is used to encrypt column keys, and the master key is physically separated from data, i.e., stored outside a database [14]. The column keys encrypt the data present in those respective columns. Oracle provides various commands such as creating and opening a wallet; and creating, altering and encrypting master keys and column keys [14].

TDE supports a few algorithms and modes, such as Encryption [AES (128, 192, and 256), Triple DES (168)], Salt, SHA1, and CBC mode [14]. In the process of TDE integration, it supports a list of operations, such as all SQL operations,

scalar data types, equality indexes, OCI direct path load, datapump import/export, and physical standby. It does not support foreign key constraints, range scan indexes, abstract data types, LOBs data types, and features that bypass the SQL engine for direct data manipulation (logminer for example) [14]. TDE's primary use in the PCI is to encrypt sensitive information, such as encryption of social security numbers, credit card numbers, and other personally identified numbers. As TDE backs up the encryption wallet every time, the master key is re-keyed and so on [14].

One competitive advantage of TDE is application transparency. On the one hand, TDE protects only the sensitive data leaving behind unnecessary encryption [14]. On the other hand, some ordinary modules are not required in TDE, such as database triggers, database views, stored procedures, changes in application SQL, changes in a general query plan, complicated overhead, and simple key management [14].

Users can choose either DBMS_CRYPTO or TDE to comply with the data encryption requirements in the PCI DSS. TDE adopts automatic key management while DBMS_CRYPTO keys have to be managed manually. Access control in TDE is provided through VPD, label security, or a database vault, while that in DBMS_CRYPTO is up to the users' implementation. TDE is easily adopted for existing applications. DBMS_CRYPTO is shipped after release 8 and is free, while TDE is only available with advanced security options after release 10gR2 [13], [14].

Besides the above contributions, Oracle also proposed a general implementation guidance for each application in accordance with associated requirements of the PCI DSS. For instance, all of the application servers residing in the DMZ must only be web servers, and the Reports Server must be disabled if not in use. Other details can be found in [15].

C. Motorola Solutions for Key Management Facility

This section discusses the Key Management Facility (KMF) provided by Motorola [16]. The KMF can be used by various vendors and credit processing companies to achieve the compliance to the PCI DSS [16], in particular, when wireless communications such as wireless LANs are used. It enables planning, implementation, and execution of a wide range of security features [16]. Communication requirements of a KMF operator are categorized as units, namely key references and user groups. Key assignments are then distributed to each of these categories [16]. This method of rekeying is done either via Over-the-Air rekeying, or via store and forward functionality in conjunction with a KVL 3000 Plus. Over-the-Air Control (OTAC) is a feature that exists within the KMF and allows the operator to inhibit and enable the radio within the network [16]. Additional features of this facility are logging, archiving, and reporting. The system elements are the Windows 2000 architecture, OTAC services in conjunction with an ASTRO 25 integrated voice and data system, and a KMF Crypto Card [17]. OTAC is used to eliminate the burden of manually rekeying for radio communications on a regular basis. It also helps in enabling the key management and distribution securely over the air [17]. In the store and forward operations, KMF helps in reaching those units which may be out of range, making it more efficient in managing their systems [17]. Secure user group management is an innovative concept for managing secure radio communications among user groups commonly known as common key reference [17]. To see exactly which radio is ready for communications, KMF has offered a new management system known as currency [17]. In addition, KMF offers automated retries of rekey messages with key updates, can inhibit a compromised radio over-the-air, can protect the integrity of a network, can determine whether a radio is within the range of the system network via KMF Hello, and has a certified key material generator to relieve operators from the burden of relying a third party key supplier or manual key generation [17].

D. Endava Solutions

Endava provides effective and efficient solutions to organizations regarding specific vendor technologies, secured messaging for payment systems, card processing, and authorization. This is highly relevant and applicable to organizations that are looking to implement the PCI DSS to manage secure and business-critical systems [2].

Addressing security risks from inside an organization is one key area of growing exposure and market concern since most products and solutions focus more on protecting data from external threats [2]. Endava is specifically designed to address exposures and to have a complete and centralized control over personal data and its access rights, and payment systems with rigorous audit trails. This will provide the organization with a more positive profile with customers and trading partners [2].

1) Endava's analysis: At Endava, the analysis of the PCI DSS objectives, its impact, and its requirements is done at three levels: process definition and implementation; technology requirements and audit; and test and evidence.

Endava maintains secure networking standards from unauthorized access by enforcing traffic and access controls with the help of firewalls and strict processes [2]. Standard firewall build and baseline security policies, including personal firewalls, are defined, documented, and audited periodically [2]. Centralized policy management is done with appropriate reports and periodic reviews. A periodic business review of the security policy is maintained with centralized management of software and patch updates, with logs, exception reports, and audits [2]. Change/release management and approval process are documented and audited with continuous monitoring of firewalls and network components [2]. Documented incident classification process and escalation path are achieved through real-time monitoring of network traffic between sensitive systems. Roles and responsibilities in the management are defined and reviewed periodically [2].

According to Endava, stored data are protected by encrypting and validating through controlled authentication methods. This has been achieved by reviewing and documenting regulatory and process requirements for the transmission and retention of sensitive data with disk-encryption technology implementation and periodic audits [2]. Defined data storage policies for encryption, key management, rotation, protection, and disposal are maintained with continuous monitoring of traffic and access.

Endava mitigates unauthorized accesses by keeping software and anti-virus tools up to date, and monitoring infrastructure components for known vulnerabilities, with a proactive maintenance program to manage the necessary changes and releases to reduce the intrusions [2]. Endava follows a defined standard build policy and library with centralized repository management of software patches and updates from secure location and continuous monitoring systems [2]. It establishes change and release management policies to ensure adequate testing and roll back policies in place with a centralized antivirus management console. It defines the authorization and escalation processes, incident classification, exception management with centralized log management, reviews, and continuous monitoring with appropriate audits [2].

The roles and responsibilities of the individuals within the process are strictly and clearly defined, monitored, reported, and audited to ensure that only authorized personnel have access. This is done with strict access to card holder data based on business needs, assigning a unique ID for each individual [2]. Access rights according to job roles are defined, saved, and monitored. Several control procedures and approval processes for changes are defined and audited. Attempted unauthorized accesses are reported [2]. Policies for third parties' access rights, times, control, and logging are defined, managed, and tested. Password policy management, including logout policy with removal of stored data using wipe technologies, is maintained, monitored, and tested with regular audits [2].

Accesses to data, devices, and applications are monitored and tracked to provide a detailed audit trail and basis for investigation analysis and remediation [2]. Security systems and processes are tested regularly by maintaining centralized repository and management of all users, roles, responsibilities, and exception reporting on attempted unauthorized accesses [2].

Endava maintains a policy that addresses information security by implementing monitoring tools to collect and provide audit and logging data regarding to compliance requirements in real-time to facilitate establishing a review board and internal audit processes and contracts with independent suppliers to conduct regular audits to test status vs. security policy [2].

2) Endava's compliance achievement plan: To achieve compliance, a step-by-step approach to understand the current infrastructure and investment is required to achieve and operate within the confines of the PCI DSS. Step 1 is to understand the infrastructure of a company by identifying all of the systems and personnel involved in the cardholder data, and by examining the data flow [2]. Step 2 is an investigation of the current posture in relation to the standard, and any immediate issues that may require urgent actions with the help of self-assessment guides [2]. Step 3 is an independent gap analysis where a third party with specialist skills in information security is recommended to undertake the process of self-assessment of business requirements [2]. Step 4 is business planning where the information from the gap analysis is used to complete a comprehensive business plan by identifying the priorities based on the assessment of risk, necessary investments, timing, and business case [2]. Step 5 is a remediation to ensure that the IT team is fully prepared [2]. Step 6 is a pre-assessment where a re-audit health check is done to ensure that all identified issues have been addressed or accounted for [2]. Step 7 is an assessment in which costs are captured as part of the gap analysis and the business planning to identify the most appropriate supplier to conduct the audit and issue a report of compliance (ROC) [2].

3) Identifying the business challenges: To implement a robust security environment, the processes and controls should require internal changes and investments in the IT infrastructure [2]. Prioritizing the PCI activities, having a common understanding of the rational and business drives, documenting the standard and security policy, and audit trail, and managing the resource and cost burden of maintaining compliance in line with identified business risks, and budget constraints will contribute to identifying the business challenges [2].

4) The IT infrastructure: The components in the environment must encrypt the stored data and the transmitted data. Communications must be mediated by firewall and logged via secure network [2]. Each asset must be monitored and assessed for vulnerability in a timely manner [2].

5) Compliance management, governance & demonstration: Monitoring compliance posture has become a challenge for the organizations implementing the PCI DSS. In order to maintain and support the compliance management architecture and to map its technology requirements, several key disciplines are followed for incident prevention and management [2]. Incident prevention is done by risk analysis and assessment, with the completion of independent compliance audits, and with self, external, and database security assessments. Data protection is achieved through firewalls, antivirus tools, secure application configuration, and access control with strong authentication contributes to security incident prevention. Incident management is done with proper detection, investigation, and response [2]. To ensure that compliance can be tested properly, standards and audit requirements are categorized into four levels [2]. Level 1 category is for merchants of processing over 6 million payment card transactions annually [2]. Annual audits, self assessment, and quarterly scans are required. Merchants of processing payment card transactions between 150,000 to 6 million annually belong to level 2. Merchants of processing payment card transactions between 20,000 to 15,000 card transactions annually belong to level 3. Merchants of processing payment card transactions belong 20,000 belong to level 4, and are required for self-assessment and quarterly scans [2].

Endava maintains significant and complex compliance-management architecture. The governance for managing compliance is established, and processes are integrated with the overall IT service management environment [2]. This is done through configuration and asset management by maintaining a library or a configuration management database (CMDB) of all hardware configurations and software versions [2]. The CMDB is used to track all technologies and configuration items that are used to support payment infrastructure. Proactive maintenance, change, and release management are its features [2].

The management tool set is maintained by identity management, access control, authentication, encryption, key management, and log management [2]. The integrated monitoring platform is maintained to ensure that an organization is able

to respond proactively during any unauthorized access, suspicious network activity, or unscheduled infrastructure changes [2]. Endava helps choose the suppliers that support the PCI DSS implementation by understanding the existing IT teams, capabilities, limitations, and gaps [2]. The suppliers can be separated into three categories like 1) risk analysis and audit; 2) advisory, implementation and operational support; and 3) forensics and investigation [2].

E. Decru and NetApp Solutions

Decru DataFort and NetApp offer several secure storage solutions to protect cardholder account with turnkey data storage, data encryption, and access control enforcement, in accordance with the PCI DSS [18]. They named their product CardVault. CardVault can be transparently deployed without changing any existing database, application, or workflow, and it has no negative effect on the network's performance [18]. CardVault fulfills almost 8 of the 12 requirements specified by the PCI Security Standards: requirements 3, 4, 6, 7, 9, and 10. Internet access and security solutions from NetApp directly address requirements 1 and 5. Decru DataFort secures stored data using secure access control strategy, wire-speed AES-256, and secure logging [18].

The designers claimed that it might be the first integrated secure storage system across the enterprise [18]. It can support all of the storage types, such as SAN, DAS, NAS, iSCSI and Tape [18].

1) CardVault Features: Hardened Appliance: Decru's Storage Encryption Processor (SEP) is a robust hardware that enables key management, multi-gigabit-speed encryption, and full-duplex [18]. The encryption is done by using strong AES-256 encryption to protect stored data. The National Institute for Standards and Technology (NIST) has certified it for compliance with FIPS 140-2 level3 [18]. Decru DataFort provides robust key security by incorporating all encryption and key management into secure hardware [18].

Compartmentalization: In CardVault, the security administrator is able to compartmentalize the stored data in shared space using storage vaults [18]. These vaults provide an additional layer of threat containment by partitioning the stored data cryptographically. Techniques like access authentication and control can also be integrated into those vaults [18].

Lifetime Key Management: This system can archive and recover the encryption keys across enterprises safely and automatically [18]. Even stored over decades, the data is still able to be decrypted [18]. If Decru DataFort hardware is unavailable, then a software recovery tool can be used to access the data [18].

Secure Logging: Cryptographically-signed and tamper-evident logs of activities are generated by Decru's DataFort [18]. Due to these logs, events like intrusions, cryptainer access, failed authentication attempts, and administrative actions are traceable [18].

Endpoint Security: It is not necessary to deploy endpoint security on every client. This module secures end-to-end transmissions over the entire data path by extending security policy enforcement to desktops and servers [18].

Operational Transparency: CardVault can be deployed on the network without modifying any existing infrastructure [18]. For the maximum transparency, its applications are able to support many typical protocols, such as NFS, CIFS, iSCSI and Fiber Channel [18]. Current management utilities and applications of the company can work normally without any modifications because only the data payload is encrypted [18].

Integrated Data Protection: Processes like replication or backup can be managed by using CardVault solution, but only the authorized users can access to the contents of the encrypted file [18]. NetApp Internet access and NetCache security systems are used at the gateway level [18]. Internet threats from outside of the enterprise can be greatly reduced.

Media Disposal: Since all of the keys are stored in secure hardware, and all of the files are encrypted as well, the data can hardly be revealed even if the relevant media is stolen or lost [18]. Hence, any physically dispose to the media with expired data is unnecessary. To make sure the data and its duplicates (if exist) are destroyed, one can just simply delete the associated key [18].

2) Advantages over Application Level Security Solutions: The Decru DataFort deployment model does not require modifications at the application or the database level. It provides much stronger security than traditional encryption solutions without sacrificing simplicity and efficiency [18].

Wire-Speed Performance: Strong encryption is computationally expensive. Current solutions have bottleneck of performance for round trip latency penalty with every read and write in an application host or a server [18]. The CardVault solution supports a 2Gbps fiber channel and 1Gbps Ethernet networks at wire speed, which allows encryption of all of the data, rather than just limiting it to some specific columns [18].

OS Independence: Major application software, databases, and operating system versions are supported by Decru DataFort and NetApp systems [18]. On the contrary, software-based solutions are OS-dependent such that the installation varies on its runtime environment, as they integrate at the application level [18].

Storage-Optimized Encryption: Being different from many other column-level solutions, the encrypted data do not increase in size when encrypted with Decru DataFort [18]. Since some DataFort appliances use hardware compression, backup windows are not increased either [18].

Easy to Handle: The NetApp storage system and Decru DataFort storage security alliances are easy to use and provide high performance [18]. The installation procedure of CardVault Solution takes only a few hours, and, once installed, it allows the organization to take out a large number of threats to stored data [18]. Moreover, the CardVault solution protects each field of database from unauthorized access, unlike column-level encryption where some fields, like customer name and address, are left in plain text because they are required for billing and customer service [18].

Centralized Enterprise-wide Key Management: The key management is fully automated and centralized, which provides strong security and high availability of data [18]. Keys are always in encrypted form whenever they are copied from Decru's DataFort secure hardware [18]. Keys are never left in a clear text.

Extensibility: CardVault provides a unified secure system across the entire enterprise [18]. It also secures sensitive data

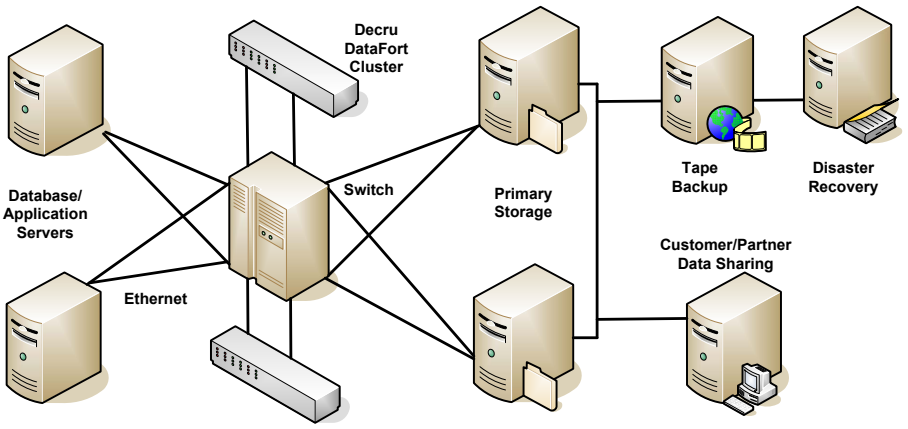


Fig. 5. The end-to-end security designed by Decru DataFort and NetApp in a file based context [18].

across all formats, like from files, to block based data to backup tapes [18].

F. Altiris Solutions

Altiris' SecurityExpressions is a product which can address vulnerability, audit, and compliance problems in various environments [19]. Major security data for network systems, like security status, unauthorized facilities, and configuration settings are all audited by SecurityExpressions [19]. During the security audit, SecurityExpressions will compare the actual settings with the company's defined settings [19]. At the end of this procedure, it will immediately inform a security manager about the instances where the actual settings vary from the company's defined policies [19]. Security managers are responsible to deal with those problems [19]. Quarterly vulnerability scans are required by the PCI, but still has drawbacks. Between two scan jobs, they do not check the vulnerabilities [19]. On contrary, SecurityExpressions can conduct audits on a daily basis and this can help in remediate the non-compliant settings at the very beginning [19].

SecurityExpressions also stores audit logs and sends report to the managers [19]. It stores a record for each audit in the log file [19]. Using a benchmark tool, the reports can reveal the non-compliance in detail, together with the compliance level against the standard [19]. With the help of trending analysis, security managers can examine the company's progress in their compliance project [19].

G. Secure Works Solutions

Secure Works is a PCI certificated security scanning vendor and a leading provider of managed security services [20]. It can help an organization secure the cardholder data in accordance with the PCI DSS [20].

To fulfill the first requirement of the PCI DSS, Secure Works provides several solutions: 1) *Professional Services*, which can examine the state of current network architecture and firewalls, check the gaps, and recommend feasible solutions, and if necessary, make corresponding changes [20]; 2) *Managed Firewall*, whose setting should be checked by authorized specialists to align with the PCI DSS to prevent any possible attacks; 3) *Security Monitoring*, which takes real-time surveillance on the firewall infrastructure, which helps the local employees perform security monitoring internally [20].

For compliance with the second requirement of the standard, Secure Works also provides professional services and vulnerability scanning [20]. The professional services team conducts a vulnerability assessment of a company's environment to find out any configuration weakness, including weak passwords, rouge web servers, and unnecessary services [20]. The vulnerability scanning service can be utilized to carry on fully vulnerability scans to secure company's infrastructure [20]. The vulnerability reports can be generated from the Secure Works portal [20]. Any movement taken to eliminate them can be determined [20].

The managed intrusion prevention and detection service of Secure Works can be used for compliance with the third requirement of the PCI DSS [20]. The service provides prevention and detection controls to protect unencrypted data [20]. It involves either Secure Works iSensor IPS or IPS/IDS technology to protect data in a cost-effective manner [20]. After the implementation, the professional services team of Secure Works will manage these devices, including ongoing tuning and monitoring them to locate and eliminate any weakness [20].

Secure Works Managed Firewall and Email encryption service provide compliance with the fourth requirement of the PCI DSS [20]. The managed firewall service provides a team of experts to handle site to site Virtual Private Network (VPN) management by administering all of the devices [20]. Malicious activities on the VPN's are quickly reported to the security managers so that they can respond before the damage can be done [20]. All of the outgoing and incoming emails containing cardholder data are encrypted using the email encryption service [20]. Lexicons are used to determine that a particular email has cardholder data and that, if found, the email is automatically encrypted [20].

Secure Works provides managed IPS/IDS, security monitoring, and security information management services for compliance with the fifth requirement of the PCI DSS [20]. The iSensor IPS appliance of the Secure Works contains antivirus and anti-spyware to block malicious codes in order to protect critical systems [20]. The security monitoring ser-

vice team monitors the infrastructure to find attacks quickly [20]. The security information management service allows the company's internal employees to perform the same work as provided by the security monitoring team and to analyze any threats that may occur [20].

The threat intelligence service, in association with professional services and vulnerability scanning, can take care of the sixth requirement of the PCI DSS [20]. It can provide new vulnerability and threat alerts tailored to the company's environment [20]. This helps the employees of the company to be updated about new patches relevant to the company's system [20].

Similarly, professional services, security monitoring, and security information management services of Secure Works take care of compliance for the seventh, eighth, ninth, and tenth requirements of the PCI DSS [20].

Moreover, Secure Works maintains compliance with the eleventh requirement of the PCI DSS with the help of managed IPS/IDS, managed host intrusion prevention, security monitoring services, the professional services, vulnerability scanning, and security information management [20]. The managed host IPS provides technology to manage this infrastructure and a group of specialists to monitor this infrastructure to operate at peak performance [20]. The real-time security monitoring service of Secure Works will identify and respond to any unauthorized activity occurring [20].

Finally, professional services and security monitoring services of Secure Works provide compliance for the twelfth requirement of the PCI DSS [20]. The professional services help the company to set an effective and robust information security policy by working with the company's team [20]. The security monitoring service provides incident response plans which can be used to address threats before any damage is done [20].

VII. PCI Qualified Security Assessor Requirements

Visa and MasterCard require the use of the PCI Qualified Data Security Companies (QDSC) to perform online compliance validation assessments using the Security Audit Procedures derived from the PCI DSS [21], [22]. The PCI SSC now publishes the Payment Card Industry Data Security Standard Validation Requirements for Qualified Security Assessors (QSA) [29]. The later was developed from the former, and the requirements to become a QDSC or QSA are essentially the same. The qualification process consists of two parts: qualification of the security company itself and qualification of the company's employees that will be serving as qualified data security professionals [21]. These requirements are grouped in the following 6 subsections.

A. QSA Business Requirements

The QSA business requirements outline that the information must be provided to prove the company's business stability, independence, and minimum insurance coverage [22].

1) Business Stability: The QSA will be examined in credit history and business stability. Firstly, the company should be accepted as legitimate one [29]. Thus, the qualified company should follow the regulations and have no criminal or fraudulent activities. The QSA should submit a copy of its business license that mentions the year of incorporation to the PCI SSC in order to show business stability [29]. Also, the qualified company should mention the total number of employees and its number of employees that can perform technical security assessment [29]. It should also provide a written statement of any past or present allegations or convictions of any fraudulent or criminal activity involving the security company [29].

2) Independence Requirement: The QSA must be able to make independent judgments while performing assessments, and it must limit sources of influence that might compromise its judgments [29]. Therefore, to begin with, it must provide the resumes and backgrounds of the company's directors [29]. Then the company should sign a written agreement known as the QSA Agreement [21]. This agreement requires that a QSA will not undertake to perform an assessment of any entities controlled by the QSA that is under common control, or of an entity in which the QSA holds any investment [21]. In addition, the QSA has not offered any gift, gratuity, service, or other inducement to any PCI SSC employees, any subjects, or agency involved in retaining the QSA to enter into the agreement with the PCI SSC or to provide QSA-related services [22]. The QSA must agree not to use its status as a "listed QSA" to market services unnecessary to bring subjects into compliance [22]. It should not represent requirements of the PCI DSS and/or the Payment Application Best Practices in connection with promotion or sales of services to the client [29]. It also should not state or imply that the PCI DSS and/or Payment Application Best Practices require usage of QSA's products or services [29].

3) Insurance Coverage: A QSA should have a minimum insurance coverage to support the indemnity clause [29]. The QSA should provide proof of coverage of statutory workers' compensation, commercial general liability, crime/fidelity bond, and automobile insurance [29]. The QSA should also have cyber risk liability covering liabilities for financial loss resulting or arising from acts, errors or omissions in rendering computer, or information technology services from data damage/destruction/corruption, including without-limitation unauthorized access, unauthorized use, virus transmission, denial of service, and loss of income from network security failures in connection with the services provided under this agreement [29]. These requirements are the minimum requirements for a company to have in order to be a QSA [29].

B. QSA Skill Requirements

This is required to prove that the employees of the QSA have skill levels necessary to serve as the QSA employees. A company must provide information and documentation to demonstrate that it has necessary information security audit service expertise, work history, and industry experience to serve as a QSA [22].

1) QSA Services and Experience: For a company to become a QSA, it should have security assessment experience

[29]. The company should also have a proper staff that can support the data security practice, and there should be a proper data security practice in place [29]. Additionally, the company should provide high level documentation with a description of the security company's experience and knowledge of information security audit engagements [29]. The description should include an explanation of relevant areas of specializations within information security, such as network security, vulnerability assessments, and/or applications security audits [29]. Moreover, the company should provide the size and the industry of the organizations which it has worked with. The qualified company should also provide the number and specific roles of the information security employees on staff and the percentage of their time dedicated to the company's security practice. At least two client references from recent security engagements are required [22], [29].

2) QSA Employee Skills and Experience: Each QSA employee who will perform the PCI data security assessment must also be qualified [22], [29]. The employees are responsible for the performance of the PCI data security assessment [22], [29], as well as being on-site for the duration of the assessment and reviewing the work product that supports the audit procedures [22], [29]. They should make sure that all of the processes adhere to the PCI security audit procedures [22], [29]. Meanwhile, the employees are also responsible for the selection of systems and system components, evaluation of compensating controls, and final report production [22], [29]. In the following we simply refer such an employee as "a QSA employee" for the ease of discussion.

A QSA employee must have sufficient information security knowledge and experience to conduct a technically complex enterprise security assessment [22], [29]. The company should provide detailed information of the employee regarding the education (subjects, degrees and certificates, institutions), area(s) of expertise (network security, application security and consultancy, system integration, auditing, special skills), years of working experience and roles, tenure with the company-specify for different roles, years of working experience related to the payment card industry, and role within the present company [22], [29].

A QSA employee should possess industry-recognized security certifications or have equivalent experience [22]. All of the QSA employees must have at least one of the following certifications CISSP (Certified Information System Security Professional), CISA (Certified Information Systems Auditor), and CISM (Certified Information Security Manager). If a QSA employee does not have any of the above certificates, he or she must provide a description of a minimum of five years' information security experience [29].

C. QSA Administrative Requirements

This subsection covers the requirements for the administrative staff of a QSA. The QSA must provide the PCI SSC with a primary and secondary contact person, including his or her name, title, address, phone, fax, email, and a defined manner of secure communication [29]. A QSA employee must have been assessed against the QSA's personnel background check policies and procedures [29]. A QSA employee is required to give a written consent to the PCI SCC to perform a background check before attending the PCI SSC-sponsored training, and most also to provide consent for additional background checks as may be requested by the PCI SCC for subsequent re-qualification process [29].

1) Adherence to PCI Procedures: The QSA report must follow the report on compliance (ROC) structure as outlined in the PCI security audit procedures [22]. The ROC must be prepared by the QSA based on the evidence obtained from the PCI security audit procedures, and this ROC should be submitted in a manner that is secure and acceptable to the PCI SSC. The QSA must submit an ROC accompanied by a signed "Summary of Findings" cover letter that summarizes whether the entity is in compliance [21], [29]. The QSA should also submit any other findings found during the assessment [21].

2) Quality Assurances: To outline the steps and review process for the ROC before it is submitted to the PCI SCC, the QSA must have a quality assurance procedure [22]. Only a QSA employee that has been qualified can perform the quality assurance procedure [21]. This includes a review of the ROC in areas such as the appropriate selection of system components, sampling procedures, compensating controls, and proper use of payment terminology and consistent findings [22], [29]. The QSA must retain case logs, notes, and any technical information that was provided to the QSA by the merchant or service provider during the PCI data security assessment for a minimum of three years [22], [29]. Digital and/or hard copies of the case logs, notes, and technical information provided to the QSA must be available upon request by the PCI SSC for a minimum of three years [21], [29].

Additionally, the security company must provide a description of the quality assurance procedure that will be used to review the ROC and "Summary of Findings" letter before they are submitted to the PCI SSC [29]. The description should outline the security company's review process for ensuring ROC accuracy and PCI security audit procedures adherence [22], [29].

3) Protection of Confidential and Sensitive Information: To avoid any unauthorized access or threats, the QSA must have sufficient physical, electronic, and procedural safeguards to protect sensitive and confidential information [22], [29]. Thus, the security company should provide a detailed description of its sensitive data protection handling practices, including physical, electronic, and procedural safeguards [22], [29].

D. QSA Qualification Maintenance

Each QSA must be re-qualified by the PCI SSC on an annual basis. The PCI SSC conducts this re-qualification during or prior to the QSA's year-end. Re-qualification is based on satisfactory feedback from the clients (i.e., the merchants or service providers that were assessed) and by the PCI SSC [29]. The QSA is responsible for sending the clients an electronic copy of a QSA Feedback form at the end of each project [22]. The client will be asked to send the completed form back to the PCI SSC. Then, the PCI SSC will base its QSA re-qualification decision on its own evaluation of the compliance validation work completed throughout the year [22], [29]. The

PCI SSC also reserves the right to conduct on-site visits during a PCI data security assessment conducted by a QSA [22], [29].

The PCI SSC's QSA qualification process focuses on four key areas: skills and knowledge, accuracy of ROC completion, remediation activity, and communications [22], [29]. In skills and knowledge, a QSA employee must demonstrate sufficient security experience, an understanding of entity environment, and payment card industry-related knowledge [22], [29]. She or he should also have shown sufficient execution and comprehension of the PCI security audit procedures [22], [29]. All of the testing procedures should be executed or verified in the manner requested in the PCI QSA Agreement. The QSA employee should have accurately completed "In Place" and "Out of Place" details in the ROC, and the applicable comments should fit into the appropriate area as requested by the PCI SSC [22], [29]. The QSA employee should have considered the appropriate compensating controls, and those controls should have fulfilled the intended requirement. She or he also should have followed up and revalidated in order for the client to be compliant [22]. A central QSA representative should enable efficient and consistent communication between the PCI SSC and the QSA during the assessment and revalidation periods [22], [29].

The qualification of a QSA can be revoked if it is found in breach of the PCI QSA agreement [22], [29]. Examples of such breaches include using PCI security audit procedures that are modified without the approval of the PCI SSC, or not validating the compliance according to the PCI audit procedures, or violating the terms of non-disclosure provisions [21], [29]. The qualification can also be revoked if it is found that the company does not maintain enough safeguards to protect the entities' "sensitive information" and/or fails to report unauthorized access to systems that are storing "personal information" [23], [29]. The QSA should also adhere to advertising and promotional restrictions and review processes specified in the PCI QSA agreement in order to avoid any revocation [23], [29]. The QSA should always display professional and ethical business conduct to all of the entities that are being assessed [23], [29]. The QSA qualification can also be revoked if it uses an employee who is not qualified as a qualified QSA employee to conduct the PCI data security assessment [23], [29]. Any breach of the PCI QSA agreement will be grounds for revocation, as well as termination of the agreement [23]. If the PCI SSC believes that the QSA has breached the agreement, the PCI SSC will notify the QSA of the conduct that the PCI SSC deems to be a breach, and the QSA will have 15 days within which to remedy such breach. If the breach is not remedied to the PCI SSC's satisfaction within this 15-day period, the QSA's qualification will be revoked and its name will be removed from the approved on-site PCI QSA list [23], [29].

E. QSA Opting to Conduct Payment Application Assessments

A security company may choose to qualify to perform payment application security assessments according to the payment application best practices procedures [22]. If a company chooses to become a Payment Application Qualified Security Accessor (PA-QSA), it should fulfill all requirements of a QSA to perform PCI data security assessments. In addition, the company should also use the testing procedures and adhere to all PA-QSA requirements [22], [30].

VIII. VISA Europe Security Scanning Procedures

In this section, we will discuss the network security scanning procedures and guidelines in accordance with the PCI DSS. According to the VISA Europe regulations [23], a vulnerability management program should include network security scanning on a regular basis, since these scans help identify vulnerabilities of network or system infrastructures [23]. The result of the scan can be used to design a corresponding patch file or other security solutions [23]. These scans should be applied to all of the merchants and service providers that have external IP addresses, and store or process cardholder data [23]. The scan should be performed by a PCI Qualified Security Assessors (QSAs) [23]. All scans should be compliance with a set of predefined procedures. Thereby, the customers' normal operations will not be affected [23]. If application or network changes have been made in production environment, then additional scans should be done for eliminating any possible new vulnerability in this system [23]. In addition, the list of all vendors' devices and external facing IP addresses are required [23]. The scan vendors should use network probing to get the external IP range to identify the active services and IP [23].

These scans are required to be done on a periodic basis. Firewalls, external routers, or any other filtering devices, irrespective of its use, either for DMZ network or for filtering normal traffic, should be scanned for vulnerabilities [23]. Scanning web servers is critical since they are fully accessible from the public Internet [23]. If application servers are present in the network, then they should be scanned for vulnerabilities, since these application servers are used as middle men for transporting shared cardholder data which is normally shared between the cardholder and the merchant for managing accounts [23]. Additionally, customer-facing web applications of a merchant should also be scanned for vulnerabilities [23]. If the service provider or the merchant is using its own DNS servers or it is using DNS servers provided by its Internet service provider, then these DNS servers should also be scanned for vulnerabilities because anybody can spoof the web servers and collect credit card information if these DNS servers are vulnerable [23]. DMZ networks may contain mail servers and they can serve as easy paths for hackers, and therefore these mail servers should also be scanned for possible vulnerabilities [23]. Moreover, due to the fact that merchants and service providers normally use load balancers for balancing loads on their physical servers, these servers should be scanned and tested individually behind the load balancer since failure to do so could leave possible vulnerabilities undetected [23]. If the merchants' websites are hosted by third parties, then the third parties' entire externally facing infrastructures also should be scanned to show compliance with the PCI DSS, because they may host other clients' web sites on the same server, and those web servers could have vulnerabilities [23]. Likewise, all of the wireless access points in a merchant's wireless LANs must be scanned, as wireless LANs introduce new data security risks [23]. IDS/IPS should be configured in a way that they

should admit the original IP address of the scan vendor, or the scan should be originated in a location to prevent them from interfering with their behaviors [23].

IX. Conclusion

The PCI DSS is the very first industry-wide standard that aims at achieving a strong protection of sensitive consumer and cardholder data, and prevents major security issues. It is the result of a collaborative effort of the major payment card networks and issuers. The standard sets force requirements in many aspects, including secure networks, cardholder data protection, access control, vulnerability management, security assessments, and reporting. The benefits of the standard are the definition of the standard set of security tools, practices, and measurements for stakeholder information protection, increased confidentiality and integrity, and a strong infrastructure to prevent security attacks. Through a continuous process of assessment, remediation, and reporting, a compliant merchant or service provider would significantly reduce the risk of security breaches [26].

Major card networks such as Visa, MasterCard, Discover, American Express, and JCB mandate that merchants and service providers achieve certain levels of compliance [26]. However, its 12 requirements are non-trivial to implement due to its complexity in both technical and organizational terms. For example, it is widely acknowledged that security key management is difficult to maintain. In addition, the standard calls for continuous assessments of their security programs, which is often regarded as a burden to many merchants. Furthermore, some of the unclear requirements especially those which do not have any recommended implementation lead to ambiguity. It has been observed that many merchants, acquirers, and service providers have difficulties to adapt the standards. Nevertheless, a high-level of PCI-compliance has not been achieved. As reported by Visa, only 22% percent of its largest merchants were PCI-compliant, not to mention smaller merchants with tight budgets and resources [27].

As implementing all of these requirements requires a significant amount of effort and technical competence, there are a number of companies that provide compliance solutions for the PCI DSS. Those solutions share certain similarities. However, to evaluate and compare their efficiencies properly, we need the complete implementation details of the vendors and survey reviews from the corresponding client companies.

Due to the challenges of the standard compliance, we have seen many development opportunities. For example, merchants and banks maintain direct customer relationships [27], and customer data is pervasive in their business to provide high-quality customer service. It is difficult to track and assess data exposures. The pervasiveness of "data" is clearly a challenge for security protection. Another example is the key management. This issue is complicated by frequent keying and re-keying. Nevertheless, technical advances in many of these aspects can eventually lead to a reassessment and revision of the current standard, which may essentially improve penetration of the security standard, and may reduce the risks of security breaches.

Acknowledgment

The work is supported in part by the U.S. National Science Foundation (NSF) under Grant Nos. CNS-0716211, CNS-0737325, and CCF-0829827.

References

[1] XRamp. (2006, March 13). "SecureTrust PCI Compliance" [Online]. Available: http://www.securetrust.com/pdf/securetrust_datasheet.pdf.

[2] Endava. (2007, January 30). "Assessing & Implementing Compliance Management for PCI DSS" [Online]. Available: http://www.endava.com/resources/Endava Whitepaper - Assessing and Implementing Compliance Management for PCI DSS.pdf.

[3] IT Compliance Institute. (2007). "IT Audit Checklist Series" [Online]. Available: http://www.itcinstitute.com/display.aspx?id=2499.

[4] PCI Security Standards Council. (2006). "Organizational Structure" [Online]. Available: http://www.pcisecuritystandards.org.

[5] Choicepoint. (2007). "Choicepoint Corporation" [Online]. Available: http://en.wikipedia.org/wiki/Choicepoint.

[6] Identity Theft. (2006). "Identity Theft Categories" [Online]. Available: http://idtheft.about.com/od/.

[7] Msnbc.com. (2007, March 30). "TJ Maxx theft believed largest hack ever" [Online]. Available: http://www.msnbc.msn.com/id/17871485/.

[8] Identity Theft. (2007). "Data breaches 2007" [Online]. Available: http://idtheft.about.com/od/databreaches2007/a/Databreaches07.htm.

[9] Ann Kjos, "The Merchant-Acquiring Side of the Payment Card Industry: Structure, Operations, and Challenges," Payment Card Center, Federal Reserve Bank of Philadelphia, 2007, Available: http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2007/D2007OctoberMerchantAcquiring.pdf.

[10] PCI Security Standard Council. (2006, September). "Payment Card Industry Data Security Standard" [Online]. Available: https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html.

[11] Configure Soft. (2006, September). "Payment Card Industry Data Security Standard 1.1/1.0 Comparison" [Online]. Available: http://www.configuresoft.com/webparts/CMS/ViewDocument.aspx?ItemID=d61356d9-cde2-4236-a6e1-36b8fd3be195.

[12] Vormetric Inc. (2005). "Vormetric White Paper: Protecting 'Data at Rest' with CoreGuard" [Online]. Available: http://www.randtronics.com/pdf/CoreGuardOverviewWhitePaperv1_P02.pdf.

[13] Min-Hank Ho. (2006). "Don't Let It Happen to You: Encrypt Sensitive Information in Your Oracle Database" [Online]. Available: http://www.oracle.com/technology/deploy/security/database-security/pdf/oow2006_TDE.pdf.

[14] Arup Nanda. (2005, September). "Transparency Data Encryption" [Online]. Available: http://www.oracle.com/technology/oramag/oracle/05-sep/o55security.html.

[15] Stephen Kost and Jack Kanter. (2007, January). "Oracle Applications 11i: Credit Cards and PCI Compliance Issues" [Online]. Available: http://www.integrigy.com/security-resources/whitepapers/Integrigy_Oracle_11i_Credit_Cards_PCI.pdf.

[16] Motorola. (2003). "Specification sheet for Key Management Facility" [Online]. Available: http://www.vsp.state.va.us/downloads/ STARSContract/Appendix 05 - 32 - Encryption Info 2 KMF.pdf.

[17] Motorola. (2007, August 10). "Security Policy Key Management Facility Crypto Card (KMF CC); Version 2.17" [Online]. Available: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp864.pdf.

[18] Decru and NetApp. (2005, October). "Compliance Solution for the Payment Card Industry Security Standard (PCI)" [Online]. Available: http://www.bareapp.se/PDF/PCI Compliance solution.pdf.

[19] Altiris Inc. (2005, September). "Achieving and Maintaining Compliance with the Payment Card Industry Data Security Standard" [Online]. Available: http://whitepapers.techrepublic.com.com/ abstract.aspx?docid=353195.

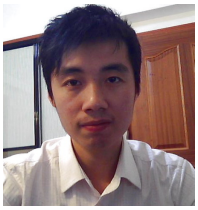
[20] Secure Works Inc. (2006). "Achieving PCI Compliance with Managed Security Services" [Online]. Available: http://www.secureworks.com/assets/print/brochure_pci.pdf.

[21] Pci.org. (2008). "PCI Certification" [Online]. Available: http://www.pci.org/about/certification/index.html.

[22] Visa U.S.A. Inc. (2005, June 7). "Payment Card Industry Qualified Data Security Company Requirements" [Online]. Available: https://www.etsms.com/ASP/CISPDocs/8.pdf.

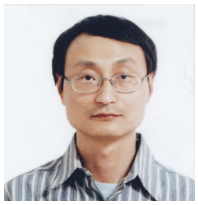
[23] Visa Europe. (2006, June 1). "Account Information Security: PCI Security Scanning Procedures" [Online]. Available http://www.visaeurope.com/documents/ais/appendix_c.pdf

[24] Americans Bankers Association and Dove Consulting, "2005/2006 Study of Consumer Payment Preferences", 2006. Available: http://www.aba.com/Surveys+and+Statistics/SS_CPPS_05.htm.
[25] Fred Katayama, "Hacker hits up to 8M credit cards," CNNMoney.com February 27, 2003, Available: http://money.cnn.com/2003/02/18/technology/creditcards/index.htm
[26] PCI Security Council, "PCI Quick Reference Guide," Oct, 2008, Available: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf
[27] James C. McGrath and Ann Kjos, "Information Security, Data Breaches, and Protecting Cardholder Information: Facing Up to the Challenges," September 13-14, 2006, Available: http://www.philadelphiafed.org/payment-cards-center/events/conferences/2007/C2006SeptInfoSecuritySummary.pdf
[28] PCI Security Council, "Summary of Changes of PCI DSS Version 1.1 to 1.2," Oct, 2008, Available: https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf
[29] PCI Security Council, "Payment Card Industry Data Security Standard Validation Requirements for Qualified Security Assessors," April 2008, Available: https://www.pcisecuritystandards.org/pdfs/pci_dss_validation_requirements_for_qualified_security_assessors_QSAs_v1-1.pdf
[30] PCI Security Council, "Payment Card Industry (PCI) Data Security Standard QSA Validation Requirements: Supplement for Payment Application Qualified Security Assessors (PA-QSA)," April 2008, Available: https://www.pcisecuritystandards.org/pdfs/pci_qsa_validation_requirements_pa-qsa_supplement.pdf



Jing Liu is a PhD student in the Department of Computer Science at The University of Alabama. He is an active researcher in the area of network security, bio-inspired network and telemedicine, including botnet issues, visual attention, anonymous communication and accountability in telemedicine. He received his BSc and MSc degrees from the Hunan University (China) in 2005 and 2008, respectively.

Yang Xiao worked in industry as a MAC (Medium Access Control) architect involving the IEEE 802.11 standard enhancement work before he joined Department of Computer Science at The University of Memphis in 2002. Dr. Xiao is currently with Department of Computer Science at The University of Alabama. He was a voting member of IEEE 802.11 Working Group from 2001 to 2004. He is an IEEE Senior Member. He is a member of American Telemedicine Association. He currently serves as Editor-in-Chief for *International Journal of Security and Networks (IJSN)*, *International Journal of Sensor Networks (IJSNet)*, and *International Journal of Telemedicine and Applications (IJTA)*. He serves as a panelist for the US National Science Foundation (NSF), Canada Foundation for Innovation (CFI)'s Telecommunications expert committee, and the American Institute of Biological Sciences (AIBS), as well as a referee/reviewer for many national and international funding agencies. He serves on TPC for more than 100 conferences such as INFOCOM, ICDCS, MOBIHOC, ICC, GLOBECOM, WCNC, etc. He serves as an associate editor for several journals, e.g., *IEEE Transactions on Vehicular Technology*. His research areas are security, telemedicine, robot, sensor networks, and wireless networks. He has published more than 300 papers in major journals, refereed conference proceedings, book chapters related to these research areas. Dr. Xiao's research has been supported by the US National Science Foundation (NSF), U.S. Army Research, Fleet & Industrial Supply Center San Diego (FISCSD), and The University of Alabama's Research Grants Committee. Dr. Xiao is a Guest Professor of Jilin University (2007-2012), and was an Adjunct Professor of Zhejiang University (2007-2009).



Hui Chen studied geophysics and computer science, and worked in industry. He is currently with Department of Mathematics and Computer Science, Virginia State University. He primarily works on computer systems, networking, and security areas such as design and analysis wireless networks, sensor networks, caching for wireless systems, operating system and network security as well as applied computing. He served as journal guest editors and various IEEE conference program committees, and publishes frequently. He is a member of IEEE and ACM.

Suat Ozdemir has been with the Computer Engineering Department at Gazi University, Ankara, Turkey since March 2007. He received his MSc degree in Computer Science from Syracuse University (August 2001) and PhD degree in Computer Science from Arizona State University (December 2006). Dr. Ozdemir's main research interests include broad areas of wireless networks and network security. He is currently working on concealed data aggregation in wireless sensor networks and reputation based trust development systems. Dr. Ozdemir serves on TPC for several conferences such as ICC, GLOBECOM, etc. He also serves as reviewer for several IEEE Transactions journals.

Srinivas Dodle used to be a graduate student at Department of Computer Science, The University of Alabama. Currently Srinivas Dodle works in a company in USA.

Vikas Singh used to be a graduate student at Department of Computer Science, The University of Alabama. Currently Vikas Singh works in a company in USA.