Merchant Endpoint Review of Shift4's Point To Point Encryption Solution

Report Date
August 27, 2013

PA-QSA Company Information:
Coalfire Systems, Inc – 3 Twin Dolphin Dr - Suite 150 – Redwood Shores - CA - 94065

Table of Contents

Executive Summary

Assessment Overview

Shift4 Corporation engaged Coalfire Systems, Inc. (Coalfire), an IT Audit, Governance, Risk and Compliance (GRC) management firm and a leading Payment Card Industry (PCI) Qualified Security Assessor (QSA) and Payment Application (PA) company to conduct an independent technical security assessment of three specific point-of-interaction (POI) devices. The goal for the assessment is to evaluate the Shift4's Point-To-Point Encryption (P2PE) solution to determine if there is any unencrypted cardholder data in the merchant environment outside of the POI device. While the Shift4 P2PE solution is not a PCI listed P2PE solution, this review is based on relevant PCI P2PE guidance. In addition, a risk based approach was used to justify appropriate scope reduction for a merchant.

Company Business Summary

Shift4 is a privately held, self-funded company that provides high-speed, reliable, and PCI-compliant connectivity to merchants' payment processor of choice. Shift4 is a leading provider of technology that enables electronic payment transactions and value-added services at the point of sale. Shift4 is a Level 1 service provider in the Payment Card Industry and offers a P2PE solution that can reduce both risk and scope for merchants.

Assessment Scope

The objective of this engagement is focused on the forensic analysis of cardholder data at rest and in transit within the merchant environment while utilizing the Shift4 P2PE solution. The assessment does not seek to speculate on PCI DSS compliance nor does it seek to draw conclusions on the security posture of data within Shift4's data decryption and key management facilities. The goals for the assessment are to demonstrate strong encryption of cardholder data from the point of entry on the POI device through the merchant environment until reaching the secured Shift4 decryption facility and to validate that the merchant has no access to any key materials related to the encryption or decryption process.

Assessment Methodology

Coalfire used a multifaceted approach to conduct the assessment:

- Perform an architecture-design review of the proposed implementation of the POIs within the merchant environment in order to better understand the potential deployment test cases
- Review test payment card transactions through Shift4's P2PE solution
- Interview both Shift4 and other relevant third parties on the technical aspects of Shift4's P2PE solution

- Perform forensic test procedures on the controlled network, host computing devices, and applications used in the testing laboratory
- Perform forensic test procedures of the POIs in a controlled laboratory setting

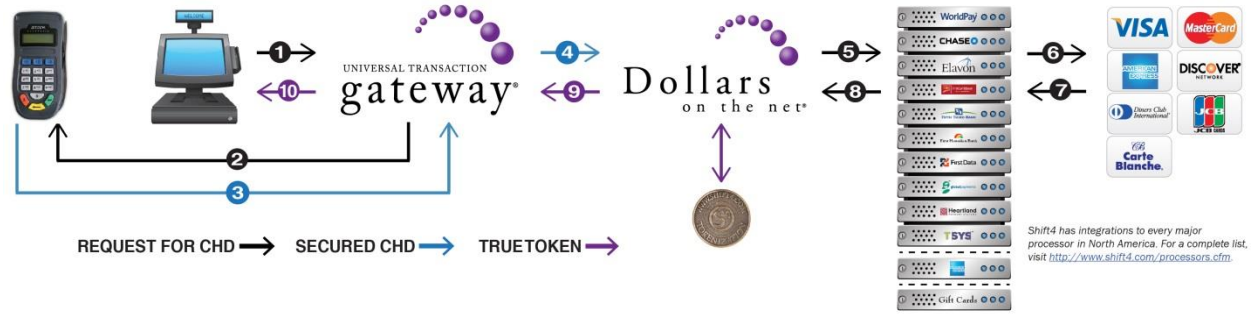
Using a controlled laboratory environment, test transactions were swiped and also manually entered using POI device keypads to validate the encryption process of the internal hardware encryption module within the POI devices. Transaction data was forensically analyzed as the data traversed the USB connection into the connected host system, the network laboratory, until it reached Shift4's data decryption facility. The test environment for this project included the POI devices, host computing devices, and applications, which were contained within an isolated network in order to eliminate any outside variables or network interference, and the data transport connection between the controlled environment and Shift4's decryption facility. The host system leveraged a fully patched Microsoft Windows 7 workstation, Shift4's Universal Transaction Gateway® (UTG®), antivirus software, and was configured with several forensic tools that supported wire-level inspection of the USB traffic between the POIs and the host system and the host system to Shift4's decryption facility.

Coalfire conducted interviews of technical engineers for Shift4 and the hardware manufacturer of the POIs and captured important operational and technical details for the devices. These interviews and subsequent discoveries of command interfaces and command functions positioned Coalfire to conduct a more thorough analysis of the core communications and operations of Shift4's P2PE solution. Details regarding the encryption key injection processes, the firmware interface commands and overall configuration of the POIs were reviewed with the hardware manufacturers.

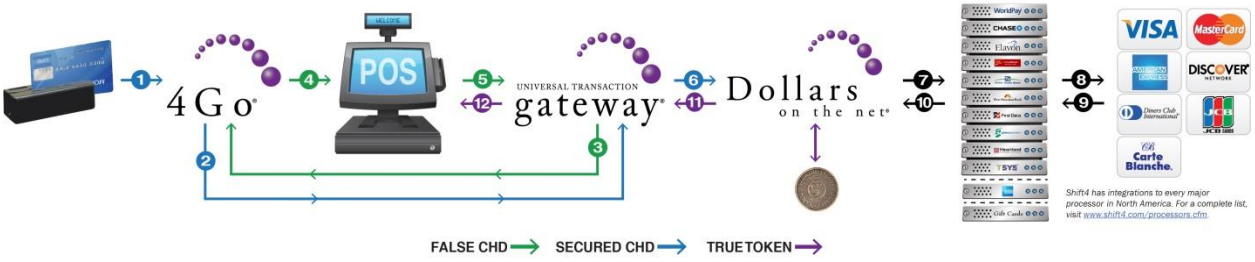
In the merchant environment, a wide range of point-of-sale (POS) applications on the host system may be used to initiate the transport of encrypted cardholder data to the decryption environment. While the POS and subsequent merchant network environment were not part of the scope of this assessment, it is important to understand that cardholder data will not be decrypted until it is received at Shift4's secure decryption facility. The data is subsequently sent to the appropriate acquirer/processor for authorization. The POI devices are injected with encryption keys prior to delivery to the merchant, and the encryption keys may not be changed outside of the key injection facility. Interviews with the hardware manufacturer technical support personnel confirm that the firmware on the POIs is designed to be "locked" following key injection. Re-keying of the POI requires a reload of the firmware by specialized tools and processes at the key injection facility.

Coalfire met with the Shift4 P2PE technical team to understand the proposed payment environment. While the payment environment discovery was not part of the assessment, it did help Coalfire better understand the context for the assessment of Shift4's P2PE solution. The diagrams below show the basic connectivity between the POI devices and Shift4's data decryption facility.

Shift4 P2PE Flow (UTG)



Shift4 P2PE Flow (4Go)



Summary Findings

The Coalfire laboratory environment included the IDTech SecuRED MagStripe Reader (SCR – currently in beta mode), the IDTechSecureKey M130 Encrypted Keypad with Secure MagStripe Reader (SCR+Keypad), and the Ingenico iSC250. All three POI devices were included in the security assessment, and following a detailed, forensic analysis of the POIs devices, no unencrypted cardholder data was found outside the POI devices. Furthermore, an attempt to extract encryption key and encryption configuration data from the POI devices was not successful. Leveraging the command language from the vendor, commands were sent to the POI devices in an effort to try and find vulnerabilities. These commands included known commands and random streams of input data. The random commands attempted to find undocumented or backdoor access points into the POI devices. No vulnerabilities were discovered during this process.

- No cardholder data was discovered during the transparent monitoring of the USB data stream

- No cardholder data was discovered during the direct capture of data from the POI by the simulated POS application
- No cardholder data was discovered in the controlled network
- No cardholder data was discovered during data transport operations by the UTG
- No ability to read sensitive configuration or encryption key data was discovered
- No ability to execute commands against the POI were successful

List of devices evaluated:

Manufacturer	Model	Input Mechanism	Interface	Cardholder Data
IDTech	SecuRED MagStripe Reader*	magnetic card swipe reader	USB	Track
IDTech	SecureKey M130**	magnetic card swipe reader, keypad and LCD display	USB	Track
Ingenico	iSC250	magnetic card swipe reader, keypad and LCD display	USB	Track

*The device tested is currently undergoing PTS validation.

** The device tested is scheduled to undergo PTS validation in 2014.

Summary PCI DSS Scope Reduction

The following summary chart provides Coalfire's opinion of the impact to PCI DSS control requirements on a merchant's cardholder data environment (CDE) assuming the Shift4 P2PE solution has been properly implemented. Merchant environments or payment processes can differ, and it is important to work with your QSA and or MSP to validate in-scope PCI DSS control requirements before making any assumptions on scope reduction.

If a merchant has deployed the Shift4 P2PE solution in their environment, it is assumed that it is the only payment channel within the merchant's CDE, including corporate environments. Paper based processes discussed within the justifications below would be in support of the Shift4 payment channel only. All recommended risk reductions are based on the assumption that a QSA has fully validated that the Shift4 P2PE solution has been properly implemented in the merchant's environment.

Shift4 can support multiple POI devices, therefore a merchant should check with Shift4 for POI options. The PCI SSC website should be consulted to confirm a device's PTS status: https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Summary Chart of Merchant PCI DSS Scope Reduction – PTS validated POI

PCI DSS Area	Major Scope Reduction	Moderate Scope Reduction	Minor/No Scope Reduction
Section 1	**X**		
Section 2	**X**		
Section 3	**X**		
Section 4	**X**		
Section 5	**X**		
Section 6	**X**		
Section 7	**X**		
Section 8	**X**		
Section 9			**X**
Section 10	**X**		
Section 11	**X**		
Section 12			**X**

Legend:

- **Major** – A significant number of controls are either removed from scope or a reduction in the number of IT assets requiring the controls
- **Moderate** – A reduced number of controls are required and a significant reduction in the number of IT assets requiring the controls
- **Minor** – Either no controls are removed from scope or minor impact to the scope of IT assets requiring the controls

The analysis of Shift4's P2PE solution confirmed the encryption of cardholder data prior to leaving the POI. It is Coalfire's professional opinion that this design strategy positions Shift4's P2PE solution well for maintaining high levels of security and data integrity throughout the communication network until reaching Shift4's decryption facility.

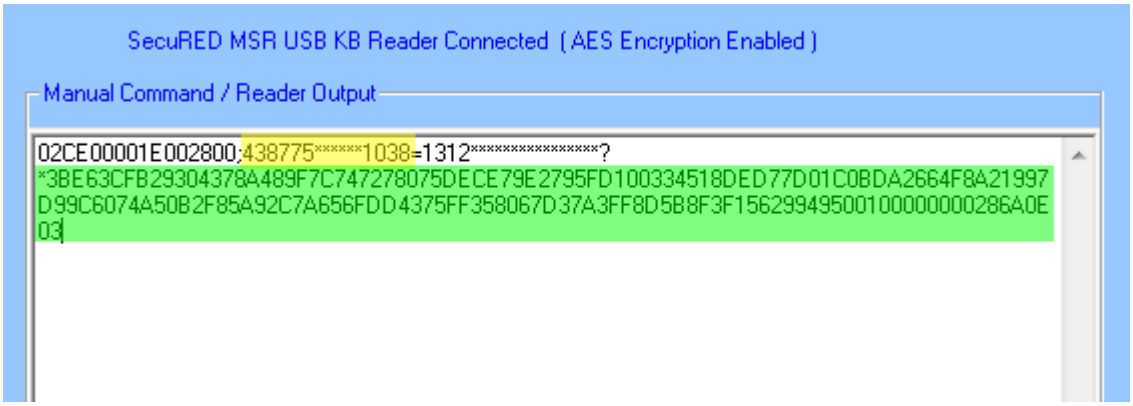
Further, Coalfire attests that a properly implemented Shift4 P2PE solution can afford the above scope reduction reflected in the tables. Coalfire confirmed the absence of cardholder data within the merchant environment when solely leveraging the Shift4 P2PE solution.

Detailed Technical Analysis

Forensic Data Capture

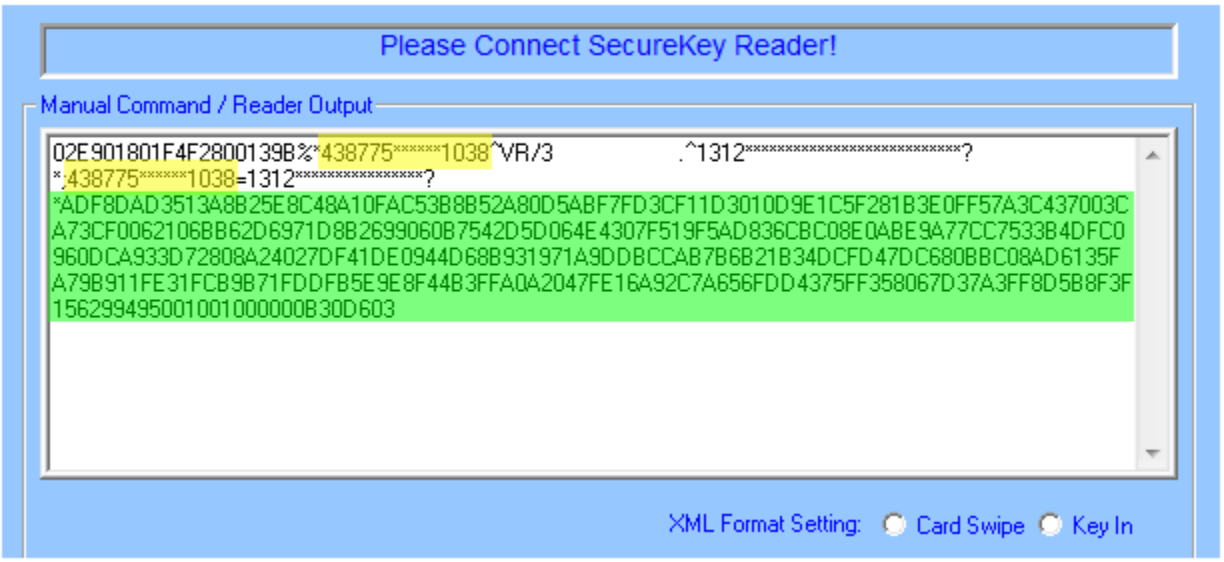
As part of a detailed forensic analysis of the POI devices, a wire level "sniffer" data capture was performed. In addition, input applications, such as simulated POS applications, that interface with USB Human Interface Devices (HID) were used to further analyze the data from the POI devices. The HID bit-stream readers are able to act as the recipient of all data communications and extract the raw data stream coming from the POI device. As a third level of USB data traffic analysis, client applications that were provided by the hardware vendor were used to inspect traffic from the POI, as well as to send commands and "brute force" data to the POI. In all test cases, no more than the first six and last four digits of the payment account number (PAN) were displayed. No sensitive authentication data (SAD) was discovered during the evaluation. Source data from the POI was also evaluated against ASCII hex values to determine if PAN data would be revealed. No PAN or SAD data was discovered. Screen shots of the data captures are provided below:

Figure 1: Hardware Manufacturer Communication Application for SCR (SecuRED beta device)



From the image above, the truncated payment account number (PAN) is shown in yellow. The PAN used for this test was 4387 – 7511 – 1111 – 1038. The data shown in green represents the encrypted payload from the POI device.

Figure 2: Hardware Manufacturer Communication Application for SCR+Keypad (SecureKey M130)



From the image above, the truncated payment account number (PAN) is shown in yellow. The PAN used for this test was 4387 – 7511 – 1111 – 1038. The data shown in green represents the encrypted payload from the POI device. Note that both swipe and manually-entry test were performed on the SecureKey M130 device.

Figure 3: Standard HID Input

From the image above, the truncated payment account number (PAN) is shown in yellow. The PAN used for this test was 4387 – 7522 – 2222 – 2227. The data shown in green represents the encrypted payload from the POI device.

Conclusion

Shift4's P2PE solution provides merchants with a much more economical alternative to a validated and listed P2PE solution and offers dramatic risk reduction as well as dramatic scope reduction. Shift4 does not charge extra for its security products, providing it to merchants as part of the DOLLARS ON THE NET® payments gateway service.

When correctly implemented, using POI devices that encrypt cardholder data as the card is swiped or manually entered, Shift4's P2PE solution will dramatically improve overall data security posture in merchant environments and render cardholder data inaccessible from point of interaction at merchant end-points until journey's end at Shift4's decryption facilities in the DOLLARS ON THE NET data centers. Finally, acquiring banks with merchants running Shift4's P2PE solution will enjoy a dramatic reduction in operating risk because their merchants' cardholder data environments have virtually disappeared.