THE NILSON REPORT

FOR 45 YEARS, THE LEADING PUBLICATION COVERING PAYMENT SYSTEMS WORLDWIDE JULY 2016 / ISSUE 1090

HPE Security in Payment Systems

When Hewlett-Packard split into two companies last year, storage, servers, and software became Hewlett Packard Enterprise (HPE). HPE's Data Security business has four segments that impact payment systems. All deal with the encryption and tokenization of data either through hardware security modules (HSM) or software. HSMs are vaults that hold encryption keys. They are installed behind firewalls at data centers and connect to card networks. HSMs perform multiple functions triggered by a discrete command for each function. Sending minimal information in a command and receiving minimal information in response is a built-in security feature. That model of communication is used when verifying a payment card's CVV number, a chip card's ARQC for tokenization and 3D Secure, and when PINs are sent to card issuers from ATMs and POS terminals.

Hewlett Packard Enterprise

HP gained hardware security module technology in the acquisition of Compaq in 2001. Compaq owned Atalla Corp., which invented HSMs 40 years ago, and HPE has continued to invest in the Atalla product line.

Multiple HSMs can be combined to handle growing transaction volume, and higher speed HSMs are available for higher value transactions such as PIN translations and verifications. HPE Atalla devices are tamper resistant. The derived keys will be destroyed or the whole device will shut down depending on the degree of attack.

HPE also offers a software development kit (SDK) to acquirers, processors, and large merchants to encrypt payment card data immediately when the card is swiped or dipped in a POS terminal. The technology protects even EMV-compliant chip card data as part of the point-to-point encryption (P2PE) process. Of the nine largest U.S. merchant acquirers, eight use the HPE SecureData Payments Host SDK. That technology came to HPE in last year's acquisition of Voltage Security. Other customers include POS terminal manufacturers such as Ingenico and Verifone, which integrate HPE's encryption software into their devices.

Eight of the largest U.S. acquirers use the SDK to encrypt card data.

Other HPE software uses format-preserving encryption (FPE) and secure stateless tokenization (SST) to secure data as it moves through the payment process to a protected back-end server. FPE is a National Institute of Standards & Technology approved security standard. SST uses stateless technology that eliminates a token database. This significantly improves speed, scalability, security, and manageability versus conventional tokenization. HPE software generates simple tokens using random data. The tokens are for internal use only and are never sent into a network. They are issued after a card authorization has been conducted with the networks. Adding tokens to internal applications

> see p. 2

HPE Security in Payment Systems

from page 1...

reduces a merchant's PCI compliance requirement. Additionally, they support consumer privacy protections such as those in the European Union.

HPE SecureData Web uses patented technology called page-integrated encryption (PIE) to protect ecommerce data before it is sent to the web and as it passes through web servers and intermediaries before reaching a back-end host. HPE SecureData Mobile protects sensitive data in native mobile applications.

Smrithi Konanur is Senior Manager, Global Product Management — Payments at HPE Data Security in Cupertino, California, (408) 886-3253, smrithi.konanur@hpe.com, www.hpe.com.