Heartland Payment Systems completes End-to-End Encryption network with support from Uniform Industrial Corporation

A global payment company, Heartland Payments Systems found a need for improvement in how payment procedures were conducted. The company started to implement a safer and more robust encryption design for the payment network. Developed together with Voltage Security and cooperated with Uniform Industrial Corporation (UIC), Heartland is due to this offering a unique End-to-End Encryption (E3) which revolutionizes the way payments are done, treating the payments system as a chain of potential vulnerabilities that must be addressed as a whole. Reaching all the way from when the payment card is swapped, passing the gateway and processor, still having the data encrypted. When using payment cards, the E3 delivers a robust approach to security and the card holder can now make purchases in a more secure way and business can go on as usual, but with minimized risk of fraud.

Customer : Heartland
Business Focus : End-to-End Encryption
Location : United States
UIC Solution : Terminal : TS900
Pinpad : PP790
MSR : MSR reader 215E

Challenge :

There is always a need for protection from hackers

Skimming, carding, fishing, BIN attacking, and now also packet sniffing, a form of cardholder data theft where computer hackers use malicious software to compromise data while it is in transit, are some of the methods thieves use to get hold of credit card information. Many times, the card holders are putting themselves at unnecessary risk, and thus easily become a victim of fraud. Paying attention to where you use your card, where you store it and how to keep your PIN safe are becoming commonly known by card users, since payment cards today are frequently used.

In later times EMV (a chip on the payment card, developed by Europay, MasterCard and Visa), also know as chip and PIN, has been a spread-out technology in major parts of the world where skimming, and other fraud methods needed to be prevented. Also to prevent fraud, the CVV code, a 3 digit code that's often printed on the back of the card, would make online shopping with cards more safe, since it hinders others from using the credit card number to complete a purchase.

More to this, when using only magnetic stripe on the card, there is not much protection that prevents hackers from sniffing your card data when the PIN is entered and the only thing remaining is a confirmation, one button click away. An improvement is needed, to get hold of this situation.

Solution :

In the payment process, there are many places where data is transferred; starting at the payment terminal, continuing thought the gateway and later on to the processor, each point is a zone where data needs to be encrypted and thus is considered to be potentially vulnerable. To mitigate against an attack, there are some official recommendations that includes data encryption protocols.

Heartland Payment Systems, a payments processor has, by using Voltage Security, a market leader in encryption technology, managed to implement E3 in their payment devices. Together with UIC – a payment solution provider, they manufacture and deliver point-of-sale equipment as a part of the Heartland network, to ensure that the card data remains encrypted through-out the whole payment process and thus minimizing the risk for packet sniffing and other attacks from malware where someone snatches the card data.

"While EMV technology is said to give a high protection, the E3 delivers an even higher level of security, hence this method is better for the card holder, the merchants, and in the end also for the society", Winson Fong, V.P. at UIC explains. He further continues, "Using E3 in the device makes the whole payment process safer, and that is what card payment is all about". From a classical Point-to-Point Encryption, where the encryption took place at each instance, the system can be considered to be at risk, but with the new E3, when the encrypted data is passing the whole network, the system never stores usable cardholder information.

Result :

Using the highest protection for the most valuable belongings

Compare to other technologies, such as chip and PIN, E3 is not a competitor, it is a complement. "Even if the chip technology is being more commonly used, and is a more secure environment for card users, the payment industry should always continue to create safer methods for payments, in that way hackers will have a hard time catching up" Fong explains. For cards without chip, E3 is important, but even for cards with chip, E3 delivers a comprehensive protection. Since a payment with chip that fails often uses the magnetic stripe as a back-up.

So far UIC has supported Heartland with three devices that are using E3 technology, a Terminal, a Pinpad and an MSR-reader. "It is a blessing to have this technology implemented, Heartland has a unique advantage in that it can protect data through its own network", says Fong at UIC. "When we offer a product to our customer we want them to know that this product is the state of the art in the industry, both when it comes to which cards that can be used, and that the data is protected all the way to the bank, and that the purchase is done without risk" he continues. Heartland Payment Systems is cooperating with Voltage Security to develop the E3 technology, Voltage is an encryption innovator and global leader in enterprise data protection for data residing both inside and outside the cloud. Voltage Security works by encoding cardholder data so it can not be read by unauthorized users. This approach is particularly effective because by encoding the data across the complete flow of a transaction, it renders the data useless to anyone who might succeed in penetrating a network or system.

UIC
Uniform Industrial Corp.

www.uicworld.com

UIC Headquarters
1FL.,No.1,Ln.15, Ziqiang St.,Tucheng Dist., New Taipei City 236,Taiwan, R.O.C.
TEL : +886-2-2268-7075
FAX : +886-2-2269-5686
Email : salessupport@uniform.com.tw

UIC USA
47436 Fremont Blvd., Fremont, CA 94538, USA
TEL : +1-510-438-6799
FAX : +1-510-438-6790
Email : info@uicusa.com

UIC Europe GmbH
Daimlerstraβe 6, 61449 Steinbach am Taunus, Germany
TEL : +49 6171 2088 404
FAX : +49 6171 2088 413
Email : info@uiceurope.com