20 YEARS OF MULTOS SECURITY AND INNOVATION

DIGITAL SECURITY INSIGHTS

Concise news, information and know-how from the MULTOS Consortium

Issue 4, 2018

Contactless is the future

The industry has seen some significant announcements in the past few months from the global payment brands who are now taking some firm decisions to mandate contactless EMV cards and acceptance devices across most regions. This will start from 2018 and by 2023 all card transactions in those regions will be contactless. The basic premise being that ***contactless is the future***: it removes cash from the system; provides obvious advantages for cardholders, issuers and merchants; and enables a wider array of consumer devices and enhancing other experiences, such as transit and IoT.

Many of the MULTOS consortium members are already well-placed to address the trend for this shift to contactless.

We will take a deeper dive into contactless in the next edition of DSI and discuss the technologies available and how contactless impacts all kinds of interesting use -cases.

Consortium News

Collaboration is a core ethos within the MULTOS Consortium, an approach that has proven valuable for 20 years and continues to open doors to new opportunities for businesses seeking to leverage the MULTOS benefits. In recent months we have welcomed yet more dynamic new members to the MULTOS Consortium. Many of the new members are agile businesses seeking to leverage innovation and implement new technology.

In 2017, Trusted Renewables implemented MULTOS in a smart energy management solution that incorporated a Smart Solar Panel design, winning an industry award. In 2018 DigiSEq extended their advanced provisioning services to support MULTOS devices, Universal Smart Cards extended their IoT product offerings with MULTOS Trust Anchors, and IoT Horizon and Device Authority recently joined the Consortium to expand their IoT product and service offers. Our most recent member, StyloPay, brings expertise in mobile payments solutions offering open platform technology for contactless payments and mobile wallets.

DEVICE AUTHORITY IoT Horizon StyloPay

INSIDE:

Consortium News - Continued

These diverse and forward thinking technology companies are helping to shape the future of the MULTOS community. We are seeing evermore member participation at MULTOS events on our exhibition stands, and with their passion, drive, and enthusiasm it is clear to see the future is bright - the future is MULTOS.

Fast News

Mexico: lawsuits for cyber fraud doubled according to Condusef

Last year more than 700 thousand people in Mexico were victims of a possible fraud in eCommerce representing 50% of all complaints to the banking system. This article (original in Spanish) discusses the most common methods used by fraudsters. Read more…

School video footage appears online

The danger of connecting devices to the internet without adequate security continues to be highlighted in a stream of news articles. This BBC article reports on school security cameras who's feeds were viewable from a US website. Read more…

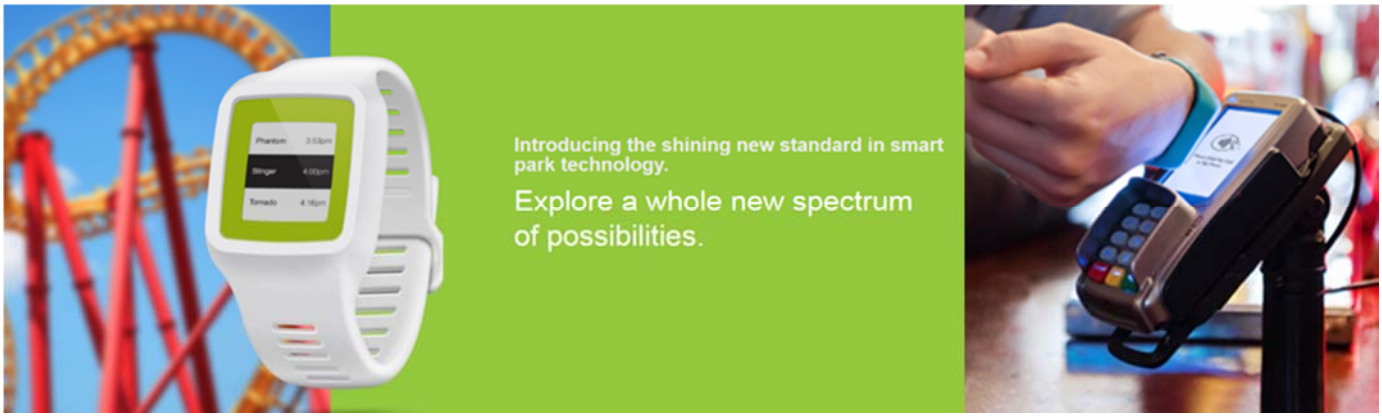
'GrayKey' Promises To Unlock iPhone X For The Feds

A second company starts up promising to unlock iOS devices for law enforcement agencies. The article describes how it is probable that the company is using undisclosed vulnerabilities to enable it to gain access to devices. However, as they appear to be offering software for sale the possibility exists for it to be reverse engineered to reveal the relied upon vulnerabilities. Read more…

Technology Briefing

Wearable NFC Consumer Device – MULTOS Inside

Recently the **accesso Technology Group plc**, the premier technology solutions provider to leisure, entertainment and cultural markets, launched a new smart wearable device incorporating MULTOS technology – the **accesso Prism**[SM]. This advanced wearable device is part of a range of award-winning solutions to drive increased revenue for attraction operators while improving the guest experience. More than 1,000 attractions and venues worldwide currently employ **accesso** technology - from theme parks, water parks, cultural attractions, live performance venues and sporting events to ski and snow parks.



Incorporating the renowned secure MULTOS technology with the MULTOS M5 chip product, allowed the design company contracted by accesso to build in a robust secure element and multi-function micro-controller, thus protecting the device and supporting a variety of features such as NFC payment, Physical Access Control, Push Information Feeds, and a Que Busting Application.

POS Fraud in Mexico

When Mexico began their EMV migration back in 2003, fraud reduction, the liability shift rules and chip mandates were the three key driving forces for EMV adoption. 15 years on, Mexico is still facing some issues with fraud at the Point of Sale despite the increase of EMV cards in the field. Here's a look at some of the reasons why and what is being done to address them.

Despite the strong drive for EMV migration over the years, Mexico still has a huge population that uses **magnetic stripe** cards and there are many merchants still accepting these cards **with signatures** as the cardholder identity verification method; quite different to most other regions that have shifted to EMV. So without strong liability mandates or penalties for merchants to enforce EMV card acceptance at the POS during the payment transaction, there remains a clear opportunity for fraud to take place at the point of sale.

Then there are also the EMV chip cards that use **chip and signature** as the identity verification method. Many chip cards in Mexico are not PIN enabled and therefore, some cards are stolen before they even reach the rightful cardholders. Activation is rarely an issue as the fraudsters will most likely have pre-gained enough personal details of the cardholder required for activation. This undermines the layered security model that relies on multiple factors to verify a cardholder (valid card in possession, PIN) - fraudsters only need to have the card in their possession.

There are also cases where unscrupulous merchants enter **incorrect values for the transaction**. The customer may unwittingly authorise a payment by signing the receipt only to realise the fraud much later, by which point no claims can be made due to the time lapse in raising the alarm and the cardholder's actual signature being on the receipt. Issuers will only be able to refund transactions that cardholders can validly prove they did not make.

Finally, there is the potential for some **cloned chip cards** in circulation that are **Static Data Authentication (SDA)** EMV cards. The payment schemes no longer allow SDA cards to be issued,

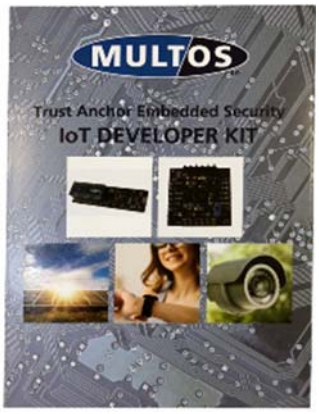
rather mandating that issuers either use online authentication (ODA) or if approved off-line that cards must support Dynamic Data Authentication (DDA) or for contactless cards, Combined Data Authentication (CDA). Although online issuer authentication has reduced fraudulent transactions overall, some smaller issuers are still issuing chip cards that do not have cryptogram validation and therefore, the cloned SDA chip cards are continuing to be accepted at the point of sale.

There are some clear causes that are contributing to the level of fraud that still exists here in Mexico particularly at the point of sale. As a positive step, all the major banks are now operating in "**partial grade**" mode until such time full issuer and acquirer host upgrades can be implemented; this has certainly helped to reduce fraud. Adoption of new technology by issuers and merchants has been a challenging factor but it is clear that **communication and education** to cardholders, merchants, acquirers and issuers alike are fundamental in combating fraud. Increasing the adoption of **DDA EMV cards**, implementing **cryptogram validations** and increasing **security awareness** through communication and education will undoubtedly help to reduce fraud at the point of sale. We also expect to see an increase in contactless card issuance across the region, thanks in part to the payment schemes announcements, but also with some innovative issuers already launching programs to bring benefits to their customers.

*Article contributed by **Edison Alonso***
Multos International

Tech Tip - MULTOS Trust Anchor Development Kit Launched

In the last issue we talked about plans for a new MULTOS development kit to help those designing secure embedded devices. We are pleased to announce that the kit is now available to buy via our Consortium partner, Universal Smart Cards.



The development kit has a supporting website which can be found at http://www.multos.com/trust_anchor/ .

The supporting website provides more information on the kit contents, getting started, API documentation, tutorials and much more.

Demand for the kit is expected to be high having attracted much positive attention at the various IoT events attended by the MAOSCO in 2017 and 2018. The topic of security is thankfully increasingly in the minds of system designers today.

MULTOS Q&A

Question: What is causing the error "Nothing to build" when trying to compile a MULTOS application using Eclipse?

Answer: This error can occur when the Windows PATH environment variable does not include the Smartdeck "bin" folder (which contains the compiler tools). To correct this, modify the System Path variable from Control Panel -> System -> Advance system settings -> Environment Variables…

Alternatively, you can run the SmartDeck "super installer" which sets up this and the rest of the environment.

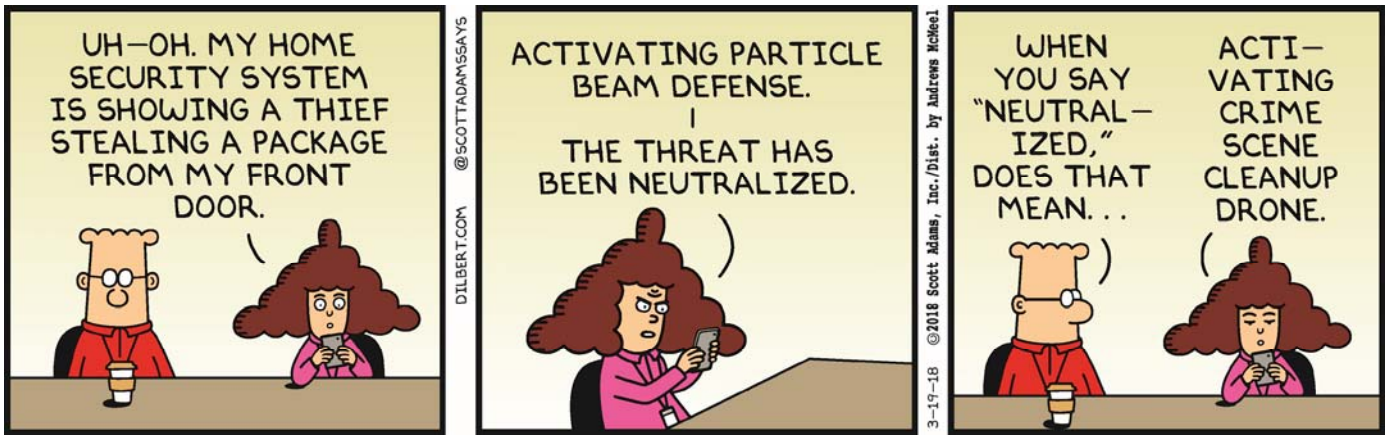
Question: Do the Meltdown and Spectre attacks impact MULTOS?

Answer: These attacks rely on microprocessors that use a cache-based architecture and "speculative execution". The microprocessors used in MULTOS devices do not have these features and therefore they are not vulnerable.

Don't forget that there is a MULTOS developer forum at http://www.multos.com/forums/viewforum/5
To join e-mail: dev.support@multos.com

The MULTOS SDK, SmartDeck, is fully integrated with the Eclipse CDT development environment. Applications can be developed in 'C' or the MULTOS assembly language, MEL (or both!).

Digital Doodle



Prize Puzzle

Solution to last issue's puzzle:

George's message was "Hungry. Give me Bananas". In the code vowels were substituted for their opposite vowel (A->E, B->D, C->C, D->B, E->A) and consonants were numbered from 21 down to 1 (B=21, Z=1).

This issue's puzzle:

The results of a "Best Ever Song" vote are encoded below. What is the song? Please send your solution to dev.support@multos.com. The first correct answer received wins a **US$100 Amazon voucher**.

LIEWDO UNSIIN
CTKTAD YHYHMS

Something to say? If you would like to contribute a short article or have a question you would like answered we'd like to hear from you.

Please e-mail us on **info@multos.com.**

www.multos.com