MULTOS 20 YEARS OF SECURITY AND INNOVATION

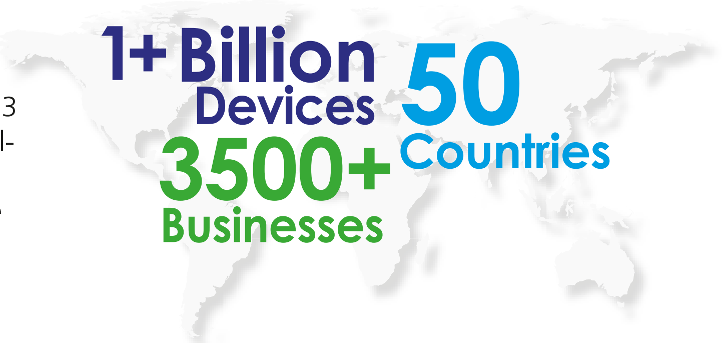
DIGITAL SECURITY INSIGHTS

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

Issue 2, 2017

1 billion+ MULTOS devices and rising

In the past few years we have seen an increasing adoption rate for the issuance of MULTOS cards and devices. 2012 saw the US issuers begin to adopt MULTOS technology for their 1st EMV rollouts with a rapid deployment acceleration from 2014. In 2013 the Latam region started to look increasingly to MULTOS technology to service EMV migrations . In recent years new innovations leveraging real-time enablement, contactless wearables, and the Internet of Things (IoT) have continued to drive growth. Today over 1 Billion MULTOS cards and secure devices have been shipped, in over 45 countries, for over 3,500 businesses. A truly impressive achievement. With new innovative projects now implementing MULTOS technology, the foundations are developing to support continued growth for the coming years.



Fast News

Medical Device Security

A report released by Synopsis (chip design company) and Ponemon (research institute) in May 2017 claims that the medical device industry is “under attack and unprepared to defend”. According to the report “In many cases, budget increases to improve the security of medical devices would occur only after a serious hacking incident occurred” and “Most organizations do not encrypt traffic among IoT devices.” The full report is **here**.

Ukraine CPNI hacks

A recent Wired magazine article highlights the dangers of connecting Critical National Infrastructure to the internet. It makes sobering reading for anyone planning to connect more of our infrastructure without spending the time and the money to do it in a highly secure way. Read more **here**.

Do you really trust your mobile?

According to Zimperium’s Mobile Device Threat Data for Q1 2017, 98% of Android devices do not have the latest software version. For iOS the figure is 35% and there had been no update since March 31st. 13% of Android devices carry malware in their apps and 1% of iOS devices carry malware. More than 19% of apps can access private information and on iOS leaky apps can allow third parties to maintain persistence on the device, decrypt traffic, know your location and potentially siphon data from it. Read more **here**.

We have no affiliation with the companies mentioned above. The links/blogs listed are provided for relevant interest only.

INSIDE:

Fast News - Continued

WOODFOREST NATIONAL BANK

In 2017 our consortium membership is continuing to grow and we are delighted to welcome our newest member, Woodforest National bank. They are the first issuing bank to join the MULTOS consortium and highlight the gradual evolution in our membership. As a highly innovative bank in the US, and an active MULTOS issuer, they are keen to leverage the benefits the technology has to offer and participate as an active stakeholder in the future developments of the open MULTOS standard. Read more **here.**

Technology Briefing – Physically Unclonable Functions (PUFs)

by Chris Torr

Today

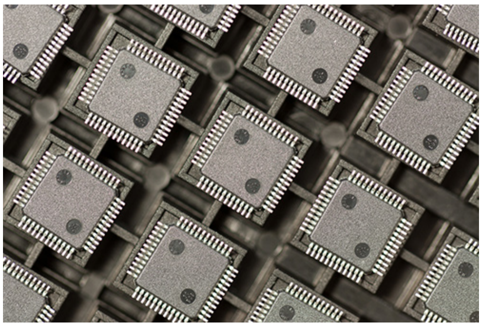
In classical computer-based cryptography, cryptographic keys have to be generated, shared and stored in such a way that the secret parts of a key's value is not generally disclosed. The key generation process always makes use of randomly generated numbers, and the quality of the keys depends on the ability of the circuit (or program) to generate numbers that more likely than not are unique, or at least unique in any population that the key is likely to operate in. This step is surprisingly difficult to achieve.

78BCD27B8F E23412F2B9DB05D5F066FCAC43DE3BC 8D133DB82955ED85D82CE
BFB206561DE 3D7F72CF75961734648FE48782B7A634 DC1DED33051887BE43F37
C9E936E68E3 0F62CD9F6044A4A2ABF74A1B391B426 BD3C56864E8EE3C6D556E
82B3E18F3E9 60D95046F2B11A7BC3DC628CF298C02 7CA5C6A82C4C6637D0721
3FC1B1171EA A465D40C2280B942F2FB1DD900EF7B8 4698B7BFA112D79FC7B38
04CB9125BA AE675AEF6351AB7DC17E4A25064AD51 C4FEF6F4A46E2045DE6A2
609B7978D8 51CE1951A91F7E280B88716036740304 011C20EDC3817B2C47846
02B73A66DB B88DABE7C540601B981D46A6C3C62D7 36B00B6DD0FB7E2F74D13
F8FFC18C4B 44E672F09486365F0C0844B2C0CD3812 42D8AB81FD74905196E98
44CB528A65 04DD2D17C5E62C5521891B4F18066A5 F2B538D660DC930F99569
C2A35FE26E6 F265C0BC77589C5325691FB3A243D866 FE7F62E125D3F9661582D5
2C158D3CE07 75D91B12915CFFCA758DE4AB93FA173 2B50DCCF396584A27B136
BCA1695007 E172A02E837CE040B76EC5B5F48B5E6D 9445C333135ABC7CE0E364
917457F5600 C8924823D3AB072C527A3AAB47E8270 D2E6F8DCBB37138BFB378
E213F51DE0C 7DADD2C6044AEF8A9A48DC0242E2E7 E14DD53920A40BFC77D37
4C8F02094D8 4B5C70EC3F710B5D2849364CCD1B633 4697F46B2C5E9D1952FCD

The failure to generate sufficiently random values has led to attacks on SSL, Windows 2000/XP, MIFARE Crypto-1 and the Playstation 3 to name but a few. Unsurprisingly then the random number generators used throughout the payments industry are subject to strict testing and certification.

PUF basics

The idea behind a PUF is that identically manufactured electronic devices can be made to output unique streams of data when stimulated with the same input signal. This stream of unique data can then be used for key generation, memoryless key storage and device authentication.



The PUF process usually exploits unavoidable physical variations in materials and processes and in some cases even quantum effects. The cheapest, and most often talked about type of PUF is the SRAM PUF, which exploits the tiny variations in the physical structure of memory cell circuits. PUF technology can, therefore, in theory do away with existing RNG hardware and secure memory. In theory it can also do away with the need for key management and key loading during manufacture.

As always, it's not that simple.

An individual PUFs response to a given stimulus has to be repeatable. Herein lies the first problem. The effects relied upon by PUFs may not be intrinsically stable; for example the process may be sensitive to environment effects or physical aging. To get around this, PUF devices contain "helper data" which is used to correct the data being output by the PUF. An obvious attack then is to attack this "helper data" or the processing of the PUF output with the helper data. For protection, the "helper data" may be signed, the irony perhaps being that the only key to sign it with will be a key derived from the PUF data – at least in a pure PUF.

A PUF's response value is effectively its root key, no matter what mechanisms are used to derive symmetric or asymmetric keys based on its value. A simple attack on a device would be to stimulate the device directly and measure its response. Therefore PUFs have to be physically and logically packaged to prevent this – difficult if it is a discrete component. Another approach used is for a PUF to have many challenge-response behaviours which are then chosen at random. This though then requires responses to be harvested at manufacture, securely stored and then distributed. Essentially this is just key management by another name.

The thought that you can somehow just attach a PUF to a regular microcontroller and achieve totally security leaves out a vital element. Even assuming that you have used the PUF to verify application signatures the actual running application is still prone to physical attacks.

Where might a PUF be useful?

One possible use for a PUF as part of a MULTOS secure element could be to provide the unique identifier (MCD-ID) and manufacturing symmetric key (tkv) without the need for MISA data injection at

Technology Briefing - Continued

manufacturing time. However, you would then lose the cryptographic chain of provenance between a manufactured device and the associated KMA. Also a response gathering mechanism would need to be put in place at some other stage in manufacturing to harvest the identifiers and keys for loading into a KMA to support the rest of the process.

A more radical approach could be to use the PUF to provide each device's unique asymmetric key pair, removing the key generation work from the KMA, though of course the public keys would need certifying (which introduces other issues such as man-in-the-middle attacks).

Summary

Basic PUFs are reportedly cheap, but potentially not any cheaper than much more functional and proven secure elements. Attacks on different kinds of PUFs are known, especially on those based on PFGA or SRAM devices. However, they may find uses where cost is an issue and more basic security is all that is required. As the technology matures it is worth considering how they may be exploited by MULTOS.

Tech Tip – Using Smart Cards with Arduino

ARDUINO

The incredibly popular Arduino family of microcontroller prototyping boards is a great way to experiment with using smart cards for device security.

External reader approach

http://www.elettroinnova.altervista.org/english.htm

This shield generates all the ISO7816 signals using a PIC. APDU commands and responses are transmitted from/to the Arduino via the SPI bus. The benefit of this approach is that it minimizes the resources used in the Arduino's own microcontroller.

The shield is, however, let down by the way it appears to only exchange one byte at a time over SPI, which makes the whole process relatively slow. Still, it enabled us to build our first smart meter demo and the car security demo first shown at Cartes in 2012.

Direct approach

Another problem with the shield was that it implied to the casual observer that to use a smart card you need to include lots of additional circuitry. In fact that isn't at all true if you are happy to use some of the resources on your microcontroller to implement the ISO7816 interface directly.

The only real issue is that because the ISO-CLK signal has to be generated it does use up one of the timers of the Arduino's micro. This can lead to problems doing other timer related functions in a program, so care has to be taken with this.

We used the open source arduinosclib implementation. After fixing a couple of minor issues in the library it worked very well and was much faster to process APDUs than the shield. The other benefit was that power consumption was much reduced so demos were able to run for longer on a single battery.

https://sourceforge.net/projects/arduinosclib/

A demo showing how the MULTOS provisioning model could be used to secure ownership of car access systems

**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!).

MULTOS Q&A

Question: How can I easily build smart card access into my Windows applications?

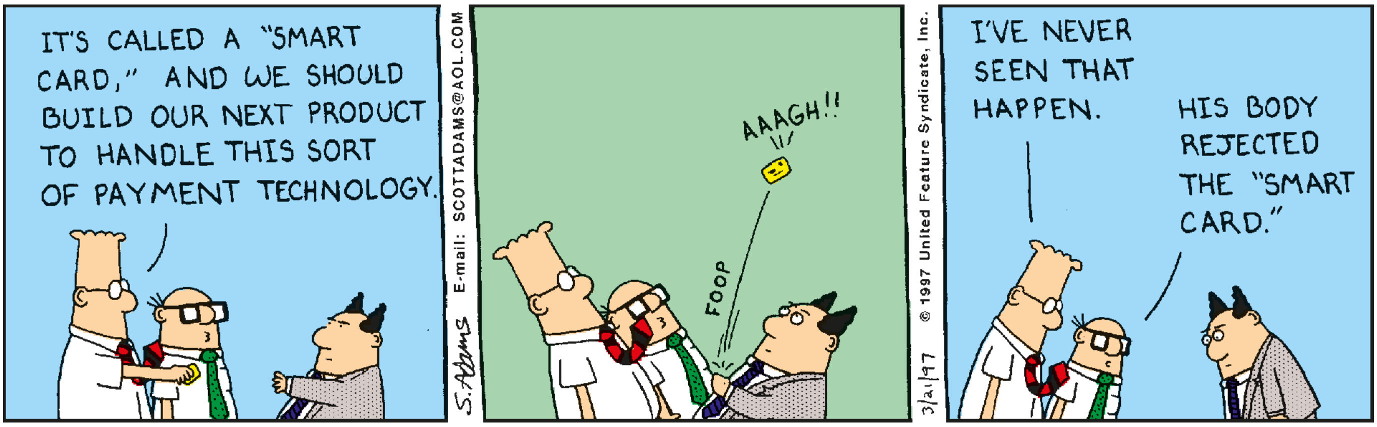
Answer: The SmartDeck SDK includes a COM component that provides both generic, low-level smart card functionality (such as listing PCSC readers present, connecting to a reader, resetting a card, sending an APDU, read directory) and MULTOS specific commands (such as load application and delete application). Being a COM component, it can be used with many different application development environments, including .NET. Full details are available in the SmartDeck Manual.

Question: What programming languages can I write MULTOS applications in?

Answer: There are two main supported options. The most commonly used option is C as this is industry standard for embedded programming. For those who wish to have low level control of exactly the code that is generated then MULTOS has a native assembly language called MEL. MEL code and C code can be mixed together in one application where required. Finally, there is the option to use Java using legacy versions of the SDK, but note that support is limited since most developers use the more suitable "C" or MEL options.

Digital Doodle

First published in 1997, the year MULTOS was born! For those who don't follow Dilbert, Pointy Haired Boss is not at all smart…


IT'S CALLED A "SMART CARD," AND WE SHOULD BUILD OUR NEXT PRODUCT TO HANDLE THIS SORT OF PAYMENT TECHNOLOGY.
S. Adams
E-mail: SCOTTADAMS@AOL.COM
AAAGH!!
FOOP
© 1997 United Feature Syndicate, Inc.
3/21/97
I'VE NEVER SEEN THAT HAPPEN.
HIS BODY REJECTED THE "SMART CARD."

Prize Puzzle

Solution to last issue's puzzle:
Marge and Homer are going to Rio de Janeiro. Each word in the message is the anagram of the name of a famous city with the initial letter missing. The missing letters, when re-arranged, give the solution.

This issue's puzzle:

Who has won "Best Actor" at the Oscars according to this cryptic message?

"Last Tango in Paris" is showing at the Oscars retro slot. Mike will be staying at the Hotel Alpha again, like he did in November. Listen to 519 kHz Radio Sierra Nevada for the latest news.

Email your solution to dev.support@multos.com. The first correct answer **wins a US$100 Amazon voucher.**

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.

www.multos.com

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