Security Validation of Smartcard: MCOS

Saadiah Yahya[1], Nik Azmi Nik Omar[2]

[1]*Department of Computer Technology and Networking,*
Faculty of Computer and Mathematic Sciences,
Universiti Teknologi MARA 40450 Shah Alam, Selangor, MALAYSIA
[1]*saadiah@tmsk.uitm.edu.my,* [2]*nikazmi100@gmail.com*

ABSTRACT

The National Fuel subsidy system planning in Malaysia should it persist would have elevated the Multi-purpose of MyKad. Malaysian government is planning for a new MyID system that can retrieve governmental related documents when dealing with 760 governments and agencies nationwide (The Star, 2010). This move will leverage the existing infrastructure of MyKad. The wider usage of MyKad may raise public concern regarding its security. Thus, there is a need for assessing the security of MyKad by an independent third party. This paper will first discuss vulnerability of smartcard by using the attack potential model (CCDB, 2008), and then the appropriateness of the current methods and tools to test the security of smartcard will be investigated. The study concludes that there is no yet a standard of security testing tool imposed on smartcard in Malaysia. The study promotes the developing of security testing tool for MyKad.

Keywords
Smartcard, MyKad, Attack potential, testing tool.

1.0 INTRODUCTION

There are endless opportunities created by information technology (IT) including embracing a knowledge-based economy. Government multi-purpose card (GMPC) also known as MyKad, is one of the Malaysian government's efforts towards accepting e-government. The main objectives of which are: to support the payment and future government applications on a single MPC platform; to enhance customer service; and to strengthen security on the existing and new applications delivered on the MPC platform. This may spur knowledge sharing between the service providers and the citizens that use the technology. However, the area of preservation of confidentiality, integrity and availability of the information embedded in MyKad should also be considered. Since MyKad is a multi-purpose smartcard, it is subjected to many different types of attacks aiming at tampering the chip or parts of it, in order to retrieve secret information. (Anderson, 2001)

1.1 Smartcard

The main feature of smartcard is it's resistant to attack and tamper resistant computer microprocessor chips. They have the ability to run applications to make computations on data and programs stored in memory. Multi-applications operating system smartcard also need the ability to load card applications side by side and provide the card with a variety of separate functions such as digital identity such as biometric verification, electronic cash, medical records and other applications. The smartcard security should be independent of the applications that are loaded to the card. The internal structure of multi-application operating system smartcard is made up of functionalities as follows:

- operating system which allowing access in a secured and controlled manner to the raw processing power of the chip as well as useful libraries for functionality such as cryptography;
- a virtual machine that allows loaded applications to be interpreted and executed which is conformed to the virtual machine API and are compiled from common high-level language such as C, Java, small language, virtual basic etc; and
- a card manager for controlling the security, including such functions that support loading and deleting of card application.

It is noted that the study by Elliott (2001) has been addressing on the comparison between Java card, Multos, MfSC and open platform but not the comparison between MCOS and any other multi-application smartcard. The brief comparison between the two multi-application operating system of smartcard which is MCOS and Java card is given in the following tables 1-3.

Table 1: Basic Information

	MCOS	**Java card**
Developer	IRIS Corporation, Malaysia.	Sun Microsystems and Java card forum
Design objective	e-passport and ID application	IT- based platform-independent implementations and telecommunication application
Application	MCS	Sun Microsystems
Conformance / Compliance to International standards for smartcard	ISO 7816 ISO 1443	ISO 7816 ISO 1443 Global Platform EMV

Table 2: Security comparison

	MCOS	Java card
Cryptographic support	RSA, DES, ECC, AES and SHA1 (Device dependent)	RSA, DES, ECC, AES and SHA1 (Device dependent)
RSA and ECC (Asymmetric)	Device dependent 2.048- bit RSA, 256-bit ECC	Device dependent 2.048- bit RSA, 256-bit ECC
DES/DES3 & AEC (Symmetric)	Device dépendent, 64-bit DES, DES3	Device dependent, 64-bit DES, DES3
Application segregation on card	Strict segregation	Strict based on application packages with some level of code sharing
Certification	In the process of certification of Common Criteria, EAL4+	Some versions have been certified for Common Criteria, EAL4+
Secure Application Load and delete	Supported by asymmetric and symmetric cryptography	Available with global platform card manager only
Cryptographic support	RSA, DES, ECC, AES and SHA1 (Device dependent)	RSA, DES, ECC, AES and SHA1 (Device dependent)

Table 3: General comparison

	MCOS	Java card
Multi-Application support	Available	Available
Global Platform Standard	Architecture designed for National multi-application and line with standard	Java card specifications evolved to support multi-application through dramatic change
Silicon/Chip support	Atmel, My-MS, Renassas, ST	Atmel, Infineon, NXP, Renassas, Samsung, ST
Multi-Application support	Available	Available

1.1 MyKad Overview

MCOS (Figure 1) was first introduced in 1996 for e-passport project. It's was introduced for its smartcard on 5th September 2001, which is called MyKad. It was developed by IRIS Corporation for ID application. It is based on 32 Kbytes or 64 Kbytes EEPROM contact smartcards chip from ATMEL and ST Microelectronic respectively and embedded together into the hybrid card is 1 Kbyte MIFARE Classic contact less chip from NXP (Phillip). Each of the three chips is having its own separate operating system and there is no sharing of data (Meor, 2002). MCOS is a smartcard operating system purpose-designed for national ID applications. MyKad incorporates nine applications i.e. national identity card, driving license, passport information, transit card (which is called Touch 'n Go), automated teller machine (ATM) card, e-cash card (which is called MEPS Cash), electronic health information, public key infrastructure (PKI), and frequent traveler card (FTC) (RFID News, 2005). An important feature of MyKad is the usage of biometrics verification, chip technology such as the digital photo and basic data in chip, encryption and decryption and mutual authentication (challenge and response). A multi-application operating system, MCOS simultaneously supports multiple custom applets with custom instruction sets and data structures from several agencies on a single smartcard, limited only by the IC specifications. The internal structure of MyKad is made up of operating system (OS), native code, small machine language, API and the applet. In term of the standard, it is conform to the ISO 7816 and ISO 1443.

The basic structure of MCOS is shown in Figure 1.

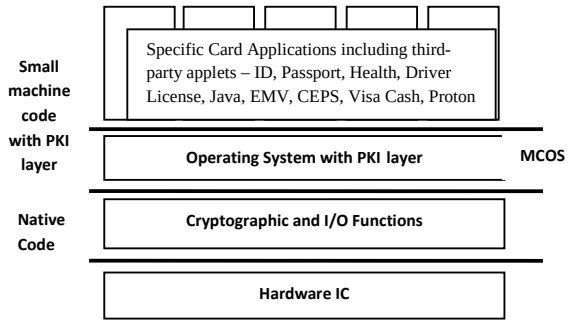
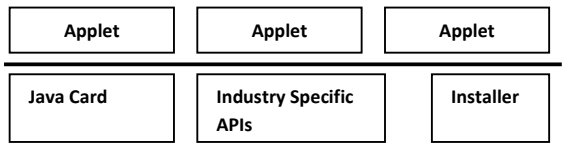


Figure 1: Basic structure of MCOS

1.2 Java Card Overview

Java card (Figure 2) was launched in 1995-1996. Java smartcard is a CPU card based on the Java language. It's a subset of a standard Java language, like a small computer which is fully operational and its hardware that ensure the need of run time environment of Java card. The internal structure of Java card is made up of operating system (OS), Java virtual machine language, API and the applets. The Java card forum (www.javacardforum.org) develop and recommended the specification to Sun Micro system and have had their most success in mobile telecommunication sectors. In term of the standard, it is also conform to the ISO 7816, ISO 1443 and global platform.

The basic structure of Java card is shown in Figure 2.



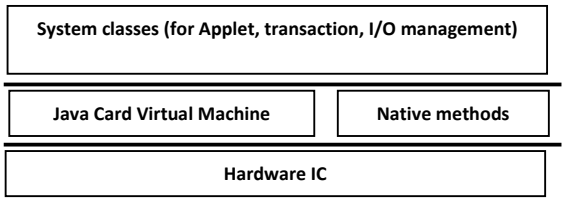


Figure 2: Basic structure of Java card

2.0 VULNERABILITY OF SMARTCARD

The implementation of secure applications on smartcard is different to the development on other platforms. Smartcard have limited computing power, small amounts of memory and are reliant on a smartcard reader to provide power and a clock. There are security considerations that are specific to smartcard that need to be taken into account when developing a secure smartcard based application.

2.1 The Taxonomy of Attackers

The adoption of the taxonomy of attackers is proposed by IBM that characterizes some extent of tamper resistant (Mead, 2006). The taxonomy of attacker is as shown in table 4 below:

Table 4: Taxonomy of attacker and their goal

Attackers	
Class 1: Clever outsiders	They are often very intelligent but may have insufficient knowledge of the system. They may have access to only moderately sophisticated equipment. They often try to take advantage of an existing weakness in the system, rather than try to create one.
Class II: Knowledgeable Insiders	They have substantial specialized technical education and experience. They have varying degrees of understanding of parts of the system but potential access to most of it. They often have highly sophisticated tools and instruments for analysis
Class III: Funded Organization	They are able to assemble teams of specialists with related and complementary skills backed by great funding resources. They are capable of in-depth analysis of the system, designing sophisticated attacks, and using the most advanced analysis tools. They may use Class II adversaries as part of the attack team.
	Attacker goals i) To get the crypto keys in RAM or ROM ii) To learn the secret crypto algorithm used iii) To obtain other information stored into the chip (PINs) iv) To modify information on the card(calling card balance)

Attackers are assumed to have a various level of expertise, resources and motivation. Motivation of the attacker can also include economic rewards or the satisfaction and notoriety of defeating expert security. Relevant expertise may be in semiconductor technology, software engineering, hacking technique, or in the specific smartcard applications.

2.2 Methods of Attacks on Smartcard

According to Adam (2006), there are four methods of attacks on smartcard which are physical, environmental, side channel and software. Besides Adam (2006), studies have been carried out by Aderson and Kuhn (1996), Kommerling and Kuhn (1999) on physical attacks. In addition, Gamdolfi, Mourtel and Oliver (2001), Quisquater and Samyde(2001), Skorobogatov and Anderson(2002), Skorobogatov(2005) and Bar-E, Choukri, Naccache, Turtall and Whelan(2006) have named environmental attacks as one of the attacks on smartcard. Meanwhile, Aderson and Kuhn (1996), Kocher, Jaffe and Jun (1999), Skorobogatov(2005) and Mangard,Oswald and Popp(2007) confirmed that side channel attacks is one of the smartcard attacks. Leroy (2003) stressed that smartcard can also be attack through software attacks. The methods of attacks that are specific to smartcard are as shown in table 5 below:

Table 5: The four methods of attacks

Type of Attacks	**Methods**
Physical	Rewiring circuit on the chip (adding tracks to the chip in order to restore circuitry during the production process to test the chip before it has been finalized). Cutting the track on the chip in order to damage circuitry and interfere with random number generation, which will make it easier to break encryption. Insert probe pins into the chip to monitor data on the chip's buses.
Environmental	Require the surface of the chip to be exposed. Altering the physical environment around the card to induce the faults. This include altering temperature, UV radiation, light, or x-ray, and resulting the chip to behave abnormally and sometimes allow an attacker to bypass security measures, or gain extra information from the behavior of the card which may infer secrets.
Side Channel	Derive information without modifying a smartcards i.e. both the secure microprocessor and plastic card remain unaffected. Exploit information leaked by the physical characteristics of the card during execution of the algorithm. Exploitation of information allows infer secrets in the form of timing power or radiation. Three types of side channel attacks: -A timing attack: the time it takes for the card to execute the cryptographic algorithm depends on the value of the secret data. -Power analysis attack: use information leaked by a card's power consumption: -Simple Power Analysis (SPA): attacks rely on detailed knowledge of the cryptographic

	algorithm being implemented, and visual inspection of the power consumption curve, to extract the cryptographic key -Differential Power Analysis (DPA): more powerful attack based on SPA. Adds the power of statistical techniques to separate signal from noise and require less detailed knowledge of the implementation of the cryptographic algorithm on the card -Electromagnetic analysis (EMA): similar to DPA but exploit the information leaked in the electromagnetic emanation from the card while it is running.
Software	-Exploit implementation vulnerabilities in the card through its own communication interface. -Exploiting buffer overflow and using Trojan horse programs to deliberately inject malicious code into the card.

3.0 THE MODEL OF POTENTIAL ATTACK

According to Boswell (2009), in order to evaluate smartcard security, we need a framework of parameters with which to model an attack and to make statements about its difficulty. Rating vulnerabilities has historically proven difficult. In many cases, the precise details of vulnerability and the method of potential exploitation can both be significant. But of course this information may not be known at the time of rating, so that it proves difficult to give a single rating value that is suitably meaningful for all of its evaluation testing. The Common Criteria defines a model for calculating the difficulty of an attack, which it calls 'attack potential'. (CCDB, 2008) The model parameters are described in table 6 below.

Table 6: Parameters of attack potential to smartcard

Parameter	Description
Elapsed time	This is the time taken for the attack. It's unlikely to spend more than 3 months attacking TOE.(Target of evaluation)
Expertise	This level of general attack knowledge and skill that an attacker must possess in order to carry out the attack.
Knowledge of the TOE	The knowledge that an attacker needs about the design of the target card (or chip).
Access to the TOE	The number of samples that an attacker requires in order to carry out an attack. More than one sample may be required because some attacks require card samples to be destroyed in order to find out information about the chip before the attack can be carried out. Other attacks may be prone to damaging the card when the attack is carried out, or may be likely to activate countermeasures that will shut down a card after a certain threshold is reached. The number of samples is measured against the thresholds 10, 100, more than 100.
Equipment	The type of equipment needed for attacks on smart cards can vary widely from a PC and card reader, through optical microscopes, digital oscilloscopes and lasers, to electron microscopes and focused ion beams workstations.
Open sample	The use of the samples that are deliberately weaker in some way than the real cards that an attacker would face. The weakness might be in the form of knowing keys or other secret values, in having the ability to load test applications onto the card, or it might be that certain countermeasures are deactivated on the test samples.

The model parameter which is depicted above has contributed a number of points such as the attack potential, and the relationship between them. It also describes assurance levels in Common Criteria (Common Criteria, 2007).

4. THE CURRENT TESTING METHODS AND TOOLS TO ASSESS SMARTCARD

In managing the security risks of the potential attack of the smartcard, there are two smartcard test security that can be applied and proposed the methods and tools to test the security of smartcard (Yachuan and Yaqin, 2009). They proposed:-

4.1 JACARTA

JACARTA is a security assessment to the Java card. It has a tool that facilitate the testing, the analysis and the validation of the security and functionality of Java Card products. It was researched by Brightsight Company. It will permit the validation of the different components implemented on a Java card through the open standard of smartcards. The test suit is made up of the test that are based on runtime environment specifications which include API of Java card, global platform card and test program of Java virtual machine actions. It applies the test suit by iterating the following phases. Firstly, the tool is authenticated to the card by an authenticated protocol. Secondly, the test applet is loaded onto the card and the appropriate test functionality that is incorporated in the applet is invoked. The applet will then responds to the loading, the installation and the removal processes, which will be specified by the Java card. After the entire test is complete, the test tool will generate a report for the tested result. Finally, the applet is deleted from the card. Therefore, the JACARTA tool can not only deal with the smartcard of unified standard, but also be used with some modification of code of the application program specified by the supplier.

4.2 JCAT

JCAT is developed by LaBRI, Laboratoire Bordelais de Recherche en Informatique (Sauveron, 2003). JCAT will run in a different runtime environments. It is not only simulating attacking to hardware but also to the software. JCAT can also simulate the electromagnetic radiation to modify the content of the smartcard's memory cell, and then modify some value of the target system. The simulator can test and run the program of the target card and check same malicious act. The work flow of the JCAT is shown in figure 3.

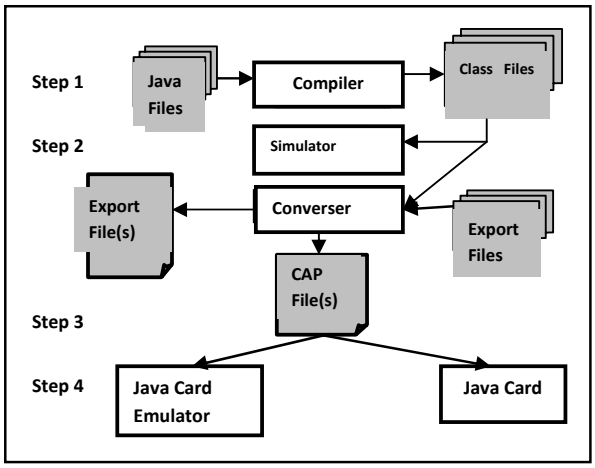


Figure 3: The work flow of JCAT

JCAT will simulate the attack or test the executable program. It is characterized by the completion of the mission step by step, the observation of memory, the buffer, stack and etc. The provision of the state of analysis during the process of implementation and will perform the execution of the laser attack. The converter of JCAT converts the CAP file format into another form. Subsidiary tool of JCAT can help to modify the byte code.

5.0 ANALYSIS OF FEASIBILITY OF ADOPTING THE TOOLS FOR MYKAD SECURITY

This paper concludes the following:

5.1 Attack Potential Model

Most types of attack on smartcards cannot be completely explored during a commercially feasible evaluation period since new attacks appear over time, and known attacks may be improved and enhanced as targets are studied over time. This requires monitoring and 'recalibration' of attack ratings over time, as well as some sort of agreement on a baseline set of attacks that should be covered in the limited evaluation time. Boswell (2009), recommends the use of the attack potential calculations as a guidance metrics to calculate the attack potential when there is no known specific vulnerability can be ascertained. For example, the 'bounding calculations' can be used to estimate 'if a vulnerability exists then it has an attack potential of at least x'.

5.2 Test Tool

The basic principle of the two test tools JCARTA and JCAT is uniform to most of the smartcard, including MyKad, as they have an industry specific extension such as global platform API, the GSM API or proprietary extension. The tools that were proposed will be able to cope with the card proprietary schemes as well as vendor specific coding of applications.

If independent third party is used, it would require sharing of the test methods and information about vulnerabilities between private companies and independent institutions (Jesang, 1995). The validation tools and method should be further investigated into different tools and method available in the market. It will require expertise in different domain of knowledge and require time and investment.

6.0 CONCLUSION

CyberSecurity, Malaysia (CSM), the agency under MOSTI is in the midst of carrying out a security certification to the next generation of MyKad. With all these measures, we hope that Malaysian citizens will have a full confidence on using MyKad applications. The validation tools and methods of MyKad certification should be considered and investigated by various Malaysian authorities. Furthermore, there isn't yet a security testing tool on smartcard in Malaysian though Malaysian government was the first to claim the use of multi-application smartcard in the world. The only way to gain citizens trust is to prove that the usage of MyKad is highly secured in its area of access service and system delivery.

Above all, the government will have to ensure that a fool-proof system will be in place to safeguard the personal information embedded in MyKad, prior to introducing any projects that involves the public interest. It is hope that this research would stimulate development of the security testing tools. More research should be carried out on the security evaluation of MyKad for the benefit all Malaysian citizens.

REFERENCES

Anderson, R. & Kuhn, M. (1996) Tamper resistance-a cautionary note. In The Second *USENIX Workshop on Electronic Commerce Proceedings*, pp. 1-11

Application of Attack Potential to Smartcards, V2.5 Revision 1, April 2008, CCDB-004-001

Anderson, R. (2001*). Security Engineering.* New York, NY: Wiley.

Bar-E, H., Choukri, H., Naccache, D., Tunstall, M., & Whelan, C. (2006). The sorcerer's apprentice guide to fault attacks. *Proceeding of the IEEE*, 94(2), pp. 370-382.

Boswell, T.(2009). *Smart card security evaluation: Community solutions to intractable problems. Information Technical Report*, pp. 57-69. Retrieved from ScienceDirect Database.

Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007

Elliott, J. (2001) *The MAOS trap in Computing & Control Engineering*. Retrieved December 2009, from IEEE database

Gamdolfi, K., Mourtel, C., and Olivier, F. (2001). Electromagnetic analysis: Concrete results. *In CHES Workshop Proceedings, 2162*, pp. 251-261. Retrieved January 2010, from Springer-Verlag database.

Jesang, A. (1995). The difficulty of standardizing smartcard security evaluation. *Computer Standards and Interface Journal*, 333-341. Retrieved from IEEE database.

Kommerling, O. and Kuhn, M. (1999). Design principles for tamper resistant smartcard processors. In *USENIX Workshop on Smartcard Technology proceedings*, pp. 9-20.

Kocher, P., Jaffe. J., and Jun, B. (1999*). Differential power analysis.* In Wiener, M.J., editor, Advance in Cryptology – CRYPTO '99, volume 1666 of Lecture Notes in Computer Science, pp 388-397. Retrieved from Springer-Verlag database.

Mead, N.R., (2006). *Security requirements engineering Build Security in 2006-08-10*, Retrieved January 10, 2010, from http:/ buildsecurityin.us-cert.gov/daisy/bsi/articles/bestpractices/requirements/234.htm.

Mangard, S., Oswald, E., E., and Popp, T. (2007). *Power Analysis Attacks* – Revealing the Secrets of Smartcards, Retrieved from Springer-Verlag database.

"Security of MyKad" (Meor, F., personal communication, December (2009).

Skorobogatov, S and R. Anderson,(2002) Optical Fault Induction Attacks, *4thWorkshop on Cryptographic Hardware and Embedded Systems* pp. 2-12. Retrieved from Springer-Verlag database.

Skorobogatov, S. P. (2005). *Semi-Invasive Attacks – A new Approach to Hardware Security Analysis.* PhD thesis, University of Cambridge. Available at http://www.cl.cam.ac.uk/TechReports/.

Sauveron, D. (2003). JCAT Laboratoire Bordelais deRecherche en Informatique 02.08.2003

The Star, (2010). New MyID system for retrieving document. *The Star*, January 19, Star Publication (Malaysia) Bhd.

Quisquater, J.J. and Samyde, D. (2001). Electro Magnetic Analysis (EMA): Measures and counter-measures for smartcards. *International Conference on Research in Smartcards, E-smart 2001*, Cannes, France, pp 200-210. Retrieved from Springer-Verlag database.

Xavier Leroy (2003*)* Computer security from a programming language and static analysis perspective. Programming Languages and Systems: *12th European Symposium on Programming, (ESOP) 2003*, pp. 1-9. Retrieved from Springer database.

Yuchuan,W. and Yaqin, S. (2009). Analysis and Research to security Testing of Smartcards. *Proceeding of International Conference on Electronic Commerce and Business Intelligence*, pp. 99-101. Retrieved from IEEE Explore database.