MCMC MTSFB TC G013:2018

TECHNICAL CODE

INTERNET OF THINGS (IoT) - SECURITY MANAGEMENT

Developed by

MTSFB org.my
Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date:

15 October 2018

Development of technical codes

The Communications and Multimedia Act 1998 (‘the Act’) provides for Technical Standards Forum designated under section 184 of the Act or the Malaysian Communications and Multimedia Commission (‘the Commission’) to prepare a technical code. The technical code prepared pursuant to section 185 of the Act shall consist of, at least, the requirement for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd (‘MTSFB’) as a Technical Standards Forum, which is obligated, among others, to prepare the technical code under section 185 of the Act.

A technical code prepared in accordance with section 185 shall not be effective until the Commission pursuant to section 95 of the Act registers it.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8688 8000
Fax: +60 3 8688 1000
http://www.skmm.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Malaysian Communications & Multimedia Commission (MCMC)
Off Persiaran Multimedia
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel: +60 3 8320 0300
Fax: +60 3 8322 0115
http://www.mtsfb.org.my

Contents

Committee representation

This Technical code was developed by Internet of Things Security Sub Working Group which supervised by Internet of Things Working Group under the Malaysian Technical Standards Forum Bhd (MTSFB) consists of representatives from the following organisations:

Al Hijrah Media Corporation

Altel Communications Sdn Bhd

Celcom Axiata Berhad

Digi Telecommunication Sdn Bhd

Kolej WIT Sdn Bhd

Maxis Communications Sdn Bhd

Multimedia University

Provintell Technologies Sdn Bhd

Telekom Applied Business Sdn Bhd

Telekom Malaysia Bhd

TIME dotCom Berhad

Universiti Kuala Lumpur

Universiti Tenaga Nasional

webe digital sdn bhd

Xiamen University Malaysia

Foreword

This technical code for Internet of Things (IoT) - Security Management (‘Technical Code’) was developed pursuant to section 185 of the Act 588 by the Malaysian Technical Standards Forum Bhd (‘MTSFB’) via its IoT Security Sub Working Group.

This Technical Code is developed in reference to International Standards such as ITU-T Y.4000, ITU-T Y.4100, ITU-T Y.4401 and other best practices on IoT security.

This Technical Code shall continue to be valid and effective until reviewed or cancelled.

INTERNET OF THINGS (IoT) - SECURITY MANAGEMENT

0. Introduction

The Internet of Things (IoT) is the current state of the art technology that revolutionised the world. It networks the physical devices, vehicles, home appliances, embedded items, software, sensors, actuators and data exchanges. From the perspective of technical standardisation, the IoT can be viewed as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (ICT). Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of "things" to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

The IoT is expected to greatly integrate leading technologies, such as technologies related to advanced machine-to-machine (M2M) communication, autonomic networking, data mining and decision-making, security and privacy protection and cloud computing, with technologies for advanced sensing and actuation.

The dependency on IoT is imminent and so are the challenges and threat it will inevitably bring to security and privacy. A strong commitment to provide a secure and resilient IoT network, protecting sensitive information, is necessary to mitigate the potential risk in IoT.

1. Scope

This Technical Code provides an overview of the IoT security management framework and defines the general requirements for security and privacy protection in the IoT ecosystem as an extension to the document ‘MCMC MTSFB TC G009:2016 - *Requirements for information and network security*’.

2. Normative reference

The following normative reference is indispensables for the application of this document. For dated reference, only the edition cited applies. For undated reference, the latest edition of the normative reference (including any amendment) applies.

ITU-T Y.4100/Y.2066 (06/2014), *Common requirements of the Internet of Things*

3. Abbreviations

For this Technical Code, the following abbreviations apply.

AAA	Authorisation and Accounting
API	Application Programming Interface
FCAPS	Fault, Configuration, Accounting, Performance and Security
ICT	Information and Communication Technologies
IoT	Internet of Things
M2M	Machine-to-Machine
OWASP	Open Web Application Security Project
XSS	Cross Site Scripting

4. IoT security threats

IoT devices and systems with weak configurations are potentially exposed to security threats. The vulnerabilities appear in all software codes from time to time which leads to compromised device, system, infrastructure, network and interface.

The current state of IoT security seems to take all the vulnerabilities from existing space, such as network security, application security, mobile security, internet connected devices and combine them into a new or even more insecure space. Furthermore, a study[1] shows:

a) 90 % of IoT devices collected at least contains one personal information;

b) 80 % of devices along with their cloud and mobile application components failed to require password of a sufficient complexity and length;

c) 70 % of IoT devices did not encrypt communications to the Internet and local network;

d) 70 % of IoT devices along with their cloud and mobile application enable an attacker to identify valid user account through account enumeration techniques; and

e) 6 out of 10 IoT devices that provide user interfaces were vulnerable to a range of issues such as persistent Cross Site Scripting (XSS).

Additionally, Open Web Application Security Project (OWASP) IoT Top 10 project listed the security issues and impacts which are related to IoT include:

a) insecure web interface;

b) insufficient authentication/authorisation;

c) insecure network services;

d) lack of transport encryption;

e) privacy concerns;

f) insecure cloud interface;

g) insecure mobile interface;

h) insufficient security configurability;

i) insecure software/firmware; and

j) poor physical security.

5. Principles of IoT security

The principles of IoT security are as listed below.

a) Assume a hostile device

Devices are likely to fall into the wrong hands. Assume attackers will have physical access to devices and are able to manipulate and launch malicious attacks.

[1] Internet of things research study 2015 report

b) Test for scale

The potential limitless of IoT deployment means that every design and security consideration should also take into account of the scale. Simple bootstrapping into an ecosystem can create a self-denial of service condition on IoT infrastructure. Security countermeasures should scale to perform based on the huge traffic volume of IoT.

c) Internet of lies

IoT systems should always verify data from the device in order to prevent autonomous misinformation from tainting a system.

d) Exploit autonomy

Automated systems are capable of complex, monotonous and tedious operations that human users would never tolerate. IoT systems should seek to apply this advantage for security purpose.

e) Expect isolation

The advantage of autonomy should also extend to situations where a component is isolated. Security countermeasures shall never degrade in the absence of connectivity.

f) Protect uniformly

Careful consideration should be given to full data lifecycle to ensure that encryption is applied uniformly and appropriately to guarantee protections. Data that is transmitted over an encrypted link is still exposed at any point it is unencrypted, such as prior to encryption, after decryption and along any communications pathways that do not enforce encryption.

Encryption is not total, be aware that metadata of encrypted data might also provide valuable information to attackers.

g) Encryption

It is very easy for developers to make mistakes when applying data encryption. Below are the common pitfalls during deploying the encryption:

i) failing to validate certificates;

ii) failing to validate intermediate certificates; and

iii) failing to encrypt traffic with a strong key or using a uniform seed or exposing private key material.

Developers should ensure a thorough review of any encryption capability to avoid these mistakes.

h) Device and system hardening

Developers should ensure that IoT components are stripped down to the minimum viable feature set to reduce attack surface. Unused ports and protocols should be disabled and unnecessary supporting software shall be uninstalled or turned off.

Developers should ensure to track third party components and update the software where possible. Secured element should be embedded in hardware to additional hardware layer security protection.

i) Limit what you can

Developers should limit access based on acceptable use criteria to the extent possible and taking into account appropriate whitelists rules.

NOTE. A whitelist is a list of items or entities that are granted access to a certain system or protocol. When a whitelist is used, all items or entities are denied access, except those included in the whitelist. The opposite of a whitelist is a blacklist, which allows access from all items or entities, except those included in the list.

j) Lifecycle support

IoT systems should be able to quickly onboard new components but should also be capable of re-credentialing existing components and de-provisioning components for a full device lifecycle. This capability should include all components in the ecosystem from devices to users.

k) Data in aggregate

IoT systems are capable of collecting vast quantities of data that may seem innocuous at first, but complex data analysis may reveal very sensitive patterns or information hidden in data. IoT systems should prepare for the data stewardship responsibilities of unexpected information sensitivity that may only be revealed after an ecosystem is deployed.

l) Plan for the worst

IoT systems should have capabilities to respond to compromises, hostile participants, malware, or other adverse events. There should be features in place to re-issue credentials, exclude participants, distribute security patches and updates before they are ever necessary.

m) The long haul

IoT system designers should recognise that extended lifespan of devices will require forward compatible security features. IoT ecosystems should be capable of aging in place and still addressing evolving security concerns. New encryption, advances in protocols, new attack methods and techniques, and changing topology all necessitate that IoT systems be capable of addressing emerging security concerns for years after they are deployed.

n) Attackers target weakness

Ensure that security controls are equivalent across interfaces in an ecosystem. Attackers will identify the weakest component and attempt to exploit it. Mobile interfaces, hidden Application Programming Interface (API)'s, or resource constrained environments should enforce security in the same way as more robust or feature rich interfaces. Using multi-factor authentication for a web interface is useless if a mobile application allows access to the same API's with a four-digit Personal Identification Number (PIN).

o) Transitive ownership and disposal

IoT components are often sold, transferred or disposed. Plan for this eventuality and be sure IoT systems can protect, isolate and sanitise overwrite data with audit report to enable safe transfer of ownership or disposal to the third party.

p) N:N Authentication

Realise that IoT does not follow a traditional 1:1 model of users to applications. Each component may have more than one user and a user may interact with multiple components. Several users might access different data or capabilities on a single device and one user might have varying rights to multiple devices. Multiple devices may need to broker permissions on behalf of a single user account and so on. Be sure the IoT system can handle these complex trust and authentication schemes.

q) IoT value chain obligation (Software and firmware update hardened with security requirements)

The software and firmware of all IoT devices, application systems and network elements software and firmware throughout its entire operational lifecycle shall always be hardened and up to date with last version to address the latest and future malware and update hardened with all security vulnerabilities requirements.

i) IoT device manufacturers

As IoT devices are marketed towards the mass market, the IoT device manufacturer’s provider shall need to ensure that all its supplied devices software is always running at the latest software version. The IoT device manufacturer shall provide software/patch updates to its customers in order to earn the right to place a security certification label on the package to denote that they are trusted manufacturers. If any IoT devices are going to be made obsolete in their roadmap and cannot be patched, they shall inform its customers in advance so that there is sufficient time to replace the devices with the latest version, which does not have any security vulnerabilities.

ii) IoT application systems provider

The application system providers need to ensure that all its systems software is always running at the latest version to ensure that there will be no security vulnerabilities.

iii) IoT network provider

The network provider need to ensure that all its network elements software is always running at the latest version to ensure that there will be no security vulnerabilities.

r) Transparency across IoT providers

IoT service provider need to know their supply chain, namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organisation. Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

6. IoT reference model

The IoT reference model as shown in Figure 1 consists of management and security capabilities which are associated with the four layers as follows.

a) application layer;

b) service support and application support layer;

c) network layer; and

d) device layer.

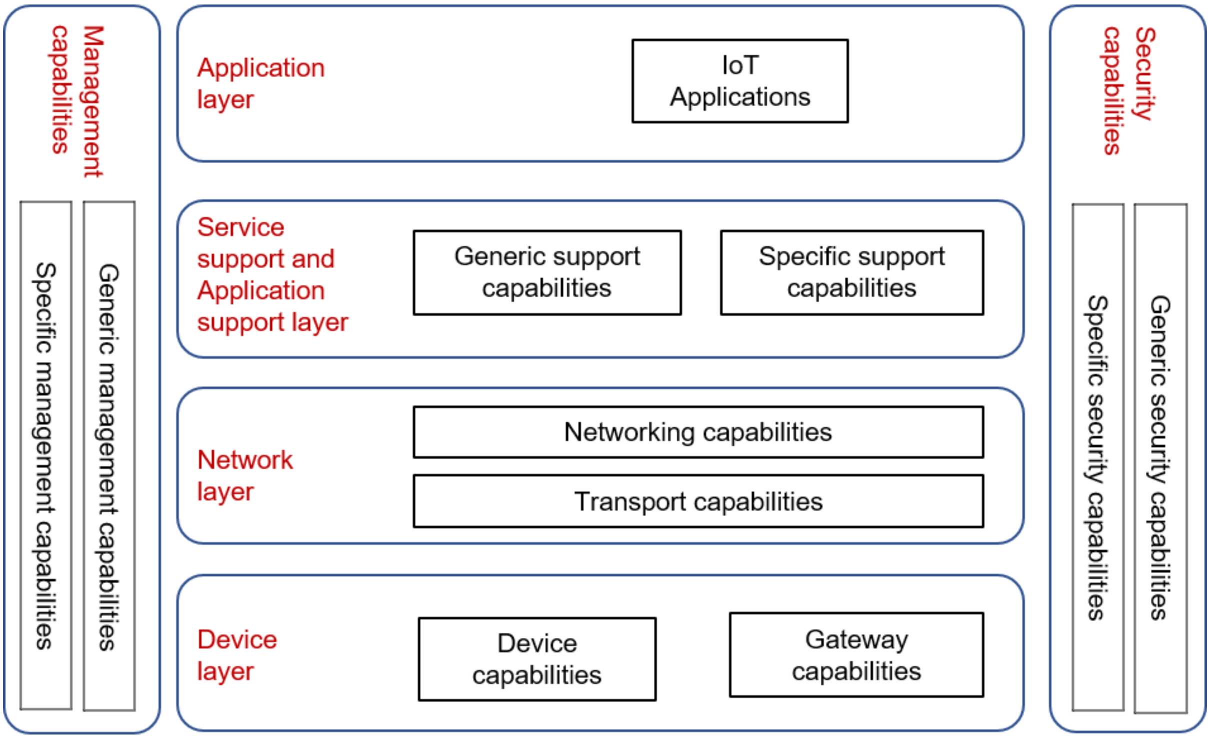
Management capabilities
Specific management capabilities
Generic management capabilities
Application layer
IoT Applications
Service support and Application support layer
Generic support capabilities
Specific support capabilities
Network layer
Networking capabilities
Transport capabilities
Device layer
Device capabilities
Gateway capabilities
Security capabilities
Specific security capabilities
Generic security capabilities

Figure 1. IoT reference model

6.1 Application layer

The application layer is the layer that interact with the user and it contains IoT applications. It can be in the form of mobile apps, software application or web.

6.2 Service support and application support layer

The service support and application support layer consist of the following two capability groupings:

a) Generic support capabilities

The generic support capabilities are common capabilities which can be used by different IoT applications, such as data processing or data storage. These capabilities may be also invoked by specific support capabilities, e.g. to build other specific support capabilities.

b) Specific support capabilities

The specific support capabilities are particular capabilities which cater for the requirements of diversified applications. In fact, they may consist of various detailed capability groupings, in order to provide different support functions to different IoT applications.

6.3 Network layer

This consists of the following two types of capabilities:

a) Networking capabilities

Provide relevant control functions of network connectivity, such as access and transport resource control functions, mobility management or Authentication, Authorisation and Accounting (AAA).

b) Transport capabilities

Focus on providing connectivity for the transport of IoT service and application specific data information, as well as the transport of IoT related control and management information.

6.4 Device layer

Device layer capabilities can be logically categorised into two kinds of capabilities:

a) Device capabilities

The device capabilities include but are not limited to:

i) direct interaction with the communication network;

ii) indirect interaction with the communication network;

iii) ad-hoc networking; and

iv) sleeping and waking up.

b) Gateway capabilities.

The gateway capabilities include but are not limited to:

i) multiple interfaces support; and

ii) protocol conversion.

6.5 Management capabilities

In a similar way to traditional communication networks, IoT management capabilities cover the traditional Fault, Configuration, Accounting, Performance and Security (FCAPS) classes.

The IoT management capabilities can be categorised into generic management capabilities and specific management capabilities.

Essential generic management capabilities in the IoT include:

a) device management;

b) local network topology management; and

c) Traffic and congestion management.

Specific management capabilities are closely coupled with application specific requirements such as smart grid power transmission line monitoring requirements.

6.6 Security capabilities

There are two types of security capabilities which are generic security capabilities and specific security capabilities.

a) Generic security capabilities are independent of applications which include:

i) the application layer

Authorisation, authentication, application data confidentiality and integrity protection, privacy protection, security audit and anti-virus.

ii) the network layer

Authorisation, authentication, use data and signalling data confidentiality, and signalling integrity protection.

iii) the device layer

Authentication, authorisation, device integrity validation, access control, data confidentiality and integrity protection.

b) Specific security capabilities are closely coupled with application specific requirements such as mobile payment, security requirements.

7. IoT functional reference model

The IoT functional framework shown in Figure 2 is to describe the IoT capabilities at the functional level in order to guarantee that the IoT capabilities can fulfil all common requirements of the IoT. A practical way is to describe the IoT capabilities in groups corresponding to all categories of common requirements of the IoT. The IoT functional framework consists of groups of the IoT capabilities and their relationships.

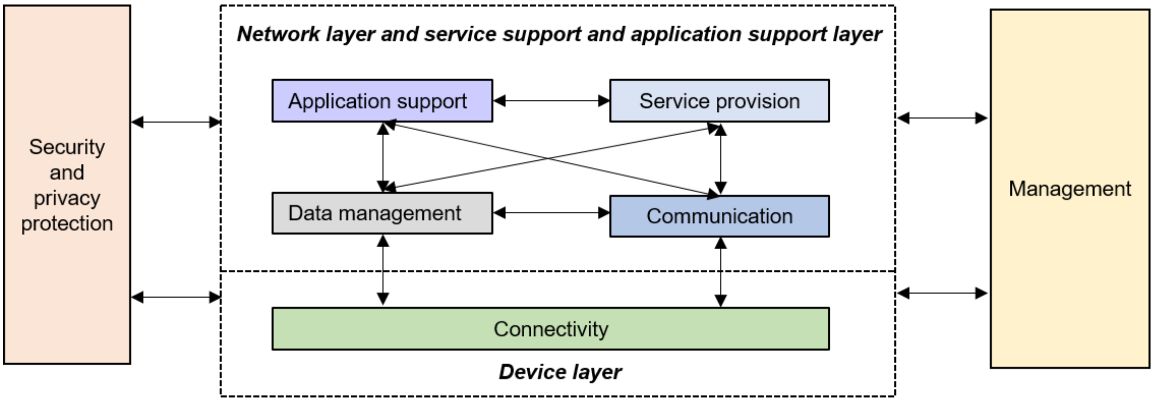

Figure 2. IoT functional framework

The connectivity group provides services to the data management group and communication group. It can provide services to the communication group and data management group triggered by requests. The security and privacy protection group configure and manage the security and privacy protection aspects of connectivity capabilities, and the management group configures and manages the other aspects of connectivity capabilities.

The communication group provides communication services to the other functional group. The other functional groups use the communication services. The management group configures and manages the communication capabilities. The security and privacy protection group configure and manages the security and privacy protection aspects of communication capabilities.

The data management group provides services to the other functional groups. The other functional groups request and configure the data management services. The management group configures and manages the data management capabilities. The security and privacy protection group configure and manages the security and privacy protection aspects of data management capabilities.

The application support group requests services from the data management group and communication group, and these two groups can provide services to the application support group. The management group configures and manages the application support capabilities. The security and privacy protection group configure and manages the security and privacy protection aspects of application support capabilities.

The service provision group requests services from the data management group and communication group, and these two groups can provide services to the service provision group. The management group configures and manages the service provision capabilities. The security and privacy protection group configure and manages the security and privacy protection aspects of the service provision capabilities.

The security and privacy protection group configure and manages the security and privacy protection aspects of the capabilities in other functional groups.

The management group configures and manages the capabilities, except the security and privacy protection aspects of these capabilities, in other functional groups.

8. Security and privacy protection requirements

The security and privacy protection requirements shall be in accordance with 8.8 of ITU-T Y.4100/Y.2066 (06/2014).

Security and privacy protection requirements refer to the functional requirements during capturing, storing, transferring, aggregating and processing the data of things, as well as to the provision of services which involve things.

Matching analysis results between security and privacy protection requirements of the IoT and the supported capabilities of the IoT are shown in Table 1.

Table 1. IoT common requirements related to security and privacy protection

No	Security and Privacy protection	Description
1	Communication security	Secure, trusted and privacy protected communication capability shall be required, so that unauthorised access to the content of data can be prohibited, integrity of data can be guaranteed and privacy related content of data can be protected during data transmission or transfer in IoT.
2	Data management security	Secure, trusted and privacy protected data management capability shall be required, so that unauthorised access to the content of data can be prohibited, integrity of data can be guaranteed and privacy related content of data can be protected when storing or processing data in IoT.

Table 1. IoT common requirements related to security and privacy protection *(continued)*

No	Security and Privacy protection	Description
3	Service provision security	Secure, trusted and privacy protected service provision capability shall be required, so that unauthorised access to service and fraudulent service provision can be prohibited and privacy information related to IoT users can be protected.
4	Integration of security policies and techniques	The ability to integrate different security policies and techniques shall be required, so as to ensure a consistent security control over the variety of devices and user networks in IoT.
5	Mutual authentication and authorisation	Before a device (or an IoT user) can access the IoT, mutual authentication and authorisation between the device (or the IoT user) and IoT shall be required to be performed according to predefined security policies.
6	Security audit	Security audit shall be required to be supported in IoT. Any data access or attempt to access IoT applications shall be required to be fully transparent, traceable and reproducible according to appropriate regulation and laws. In particular, IoT shall be required to support security audit for data transmission, storage, processing and application access.

Bibliography

[1] ITU-T Y.4000/Y.2060 *Overview of the Internet of Things*

[2] ITU-T Y.4401/Y.2068 *Functional framework and capabilities of the Internet of Things*

[3] OWASP Internet of Things Project
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[4] OWASP - https://www.owasp.org/index.php/Top_IoT_Vulnerabilities

[5] Internet of things research study 2015 report - Hewlett Packard Enterprise http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-4759enw

Acknowledgements

Members of the IoT Security Sub Working Group

Prof Dr Shahrulniza Musa (Chairman)	Universiti Kuala Lumpur
Ms Norkhadhra Nawawi (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohd Fairos Ibrahim	Al Hijrah Media Corporation
Mr Mohd Rashidi Mohamad Awal	Altel Communications Sdn Bhd
Mr Azlan Mohamed Ghazali	Celcom Axiata Berhad
Mr Hanaffy Goeffery Ramli	Digi Telecommunication Sdn Bhd
Mr Muhammad Syamsi Mohd Taufik	Kolej WIT Sdn Bhd
Mr Wong Chup Woh	Maxis Communications Sdn Bhd
Dr Khazaimatol Shima Subari	Multimedia University
Mr Nicholas Ng/ Mr Yew Seng Ong	Provintell Technologies Sdn Bhd
Mr Thaib Mustafa	Telekom Applied Business Sdn Bhd
Mr Muhamad Hasyimi Shaharuddin/ Ms Rafeah Omar	Telekom Malaysia Bhd
Mr Imran Zulkifli/ Mr Tahirul Amran Tahirul Arifin	TIME dotcom Berhad
Assoc Prof Dr Mohd Ezanee Rusli	Universiti Tenaga Nasional
Mr Mohd Fadzwan Japar/ Mr Mohd Nadzree Karim	webe digital sdn bhd
Assoc Prof Dr Yau Wei Chuen	Xiamen University Malaysia