PROTECTION PROFILE DEVELOPMENT

FOR CARD ACCEPTANCE DEVICE (CAD) WITH BIOMETRIC

Norahana Salimin
norahana@cybersecurity.my
ICCC 2013 Sept 10-12 Orlando

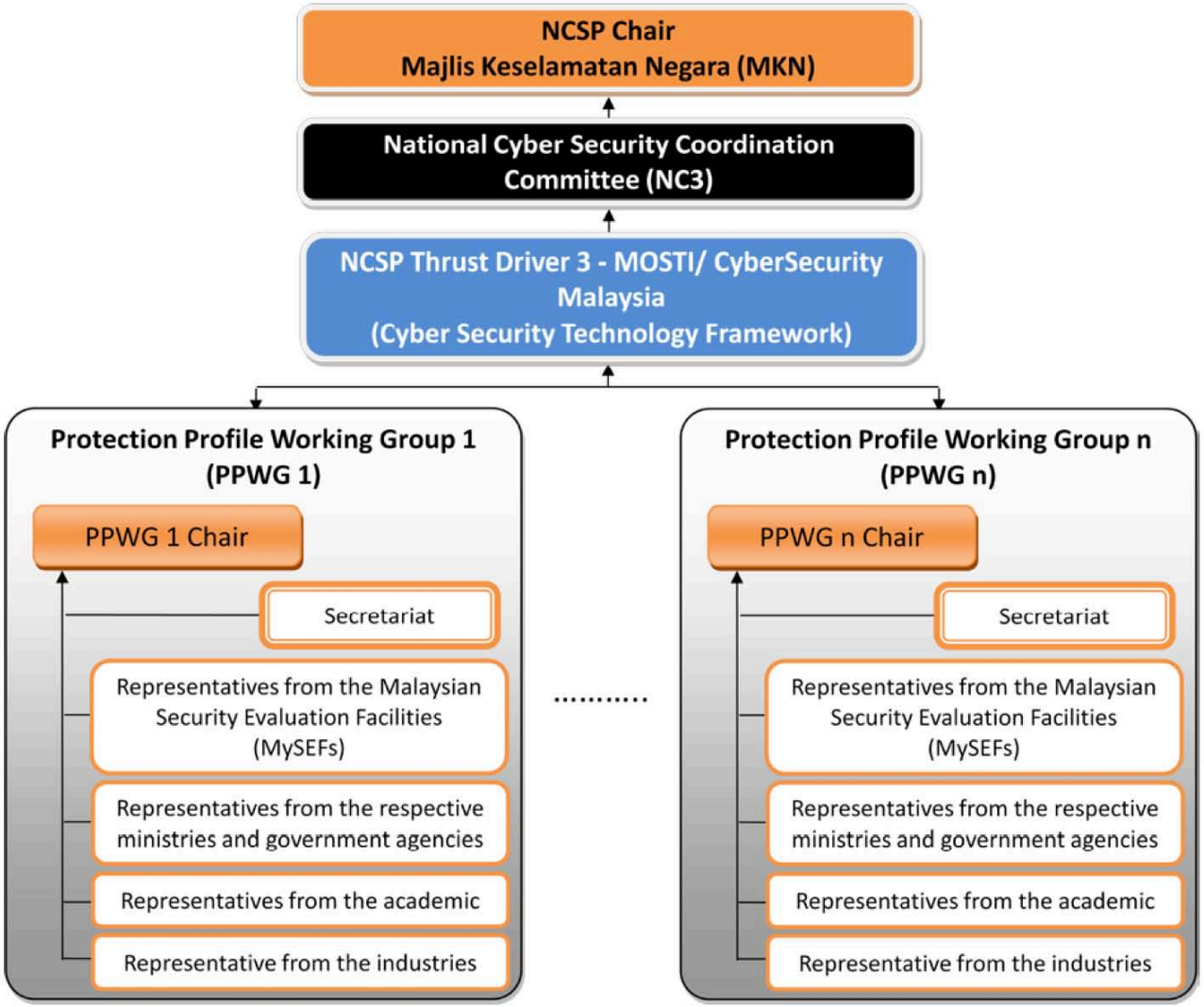
Content

- PPWG Background
- Challenge
- Lesson Learn
- Sneak Peak on the Tech Part…..
- Current Progress & Way Forward
- Q&A

PPWG4 Background

- Definition: Protection Profile Working Group
- Four (4) PPWGs established:
  1. Data Protection
  2. Network Devices
  3. Application
  4. Smart Card and its related device
- Initiative under ‘Thrust 3: Cyber Security Technology Framework’ of the National Cyber Security Policy (NCSP)

PPWG Governance Structure



PPWG Governance Structure

- PPWG members should have the knowledge and experience in ICT technologies, policy or decision making.
- **MySEF**: CSM MySEF & BAE Daetica
- **Academician**: Multimedia University, University Putra Malaysia
- **Gov. Agencies**: National Registration Department of Malaysia (JPN)

PPWG4 Objectives

- Procurement guideline on minimum requirement
- Product development reference
- Security enhancement on of Malaysian information infrastructure
- Increased assurance in the ICT product implemented security features

Challenge

- Lacking of Common Criteria knowledge to user & vendor.
- Transforming requirements into PP language and content
- Keep up with latest technology, but not forgetting the practicality
- Harmonizing the security function to meet capability of vendor and user requirement

Lesson Learn

- Combine Functional and Security Requirements in PP. Functional requirements to be put in OSP/Security Objective for Operational environment.
- Essential Security Requirements (ESR) need to be mapped to PP content. Inexperience member could not get the bigger picture.
- Timeline must be clear.

Lesson Learn

- Way forward of PP implementation must be clear to avoid unused PP
- Chairperson must be clear of the objective
- The potential organization must be clear that they will be the potential user of the PP (at least)

Sneak Peak on the Tech Part…

- PP security features will compliment:
  - Malaysian Standard (MS) 2287: Interface Device for Malaysia Multipurpose Smart Card that defines the functionality of CAD
    - **Electrical, Mechanical/Physical, Communication Protocol**
  - Malaysian Standard (MS) 1960: Multipurpose Smart Card

TOE

- Smart card reader with Biometric function
- Most of the counter in JPN/banking sector using CAD with Biometric function for user verification with their fingerprint
- JPN's procurement requirement for CAD inclusive of Biometric function
- Make sense to integrate Card Reader and Biometric in a PP

PP Scope

- **Smart card reader or card acceptance device (CAD)**
  - Contact or Contactless chip
  - Able to read smart card issued by JPN, such as MyKad, MyPR and MyKAS.
  - Whether to generalize the smart card inclusive of bank card is still in discussion.
  - Smart card can run multi applications such as national ID and health application.

PP Scope

- **Smart card reader or card acceptance device (CAD)**
  - Standalone (with network interface) or non-stand alone (without network interface)

    (Still in debate whether to choose stand alone or non-stand alone)

PP Scope

- **Biometric**
  - Verification process only
  - Gets the biometric reference associated with this identity from the smart card and captures the biometric characteristic of the user
  - Compare Biometric Live Record (BLR) and extracted characteristic of user from smart card
  - If within the threshold, successful verification

CAD Major Security Functions

- User identification, authentication, and authorization
- Enforcement of the encryption of communication
- Firmware update
- Access to one or more slots for smart cards

Biometric Major Security Functions

- Spoofing detection
- Residual Information Protection (Biometric miniature, data)

SFRs

- **Class FCS :Cryptographic Support**
  - FCS_CKM.1
  - FCS_CKM.4
  - FCS_COP.1
- **Class FDP : User data protection**
  - FDP_ACC.1
  - FDP_ACF.1
  - FDP_IFC.1 (not confirm)
  - FDP_IFF.1 (not confirm)
  - FDP_RIP.1

SFRs

- **Class FMT :Security Management**
  - FMT_SMF.1
  - FMT_SMR.1
- **Class FPT :Protection of the TSF (not confirmed)**
  - FPT_FLS
  - FPT_PHP
  - FPT_TST

SFRs

- **Class FTP :Trusted path/channels (FTP)**
  - FTP_ITC.1

- **For Biometric, no SFRs have been discussed yet**

Current Progress & Way Forward….

- Drafting PP
- Sorting SFRs (lots of good argument)
- Finalizing SFRs (more good argument)
- Expected to finalizing PP on December 2013

Q & A

CyberSecurity MALAYSIA

People First, Performance Now

MOSTI Ministry of Science, Technology and Innovation

Thank you

Corporate Office
CyberSecurity Malaysia,
Level 5, Sapura@Mines
No. 7 Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan, Malaysia.

T : +603 8992 6888
F : +603 8992 6841
H : +61 300 88 2999

www.cybersecurity.my
info@cybersecurity.my

Northern Regional Office
Level 19, Perak Techno-Trade Centre
Bandar Meru Raya, Off Jalan Jelapang
30020 Ipoh, Perak Darul Ridzuan, Malaysia

T: +605 528 2088
F: +605 528 1905

www.facebook.com/CyberSecurityMalaysia
twitter.com/cybersecuritymy
www.youtube.com/cybersecuritymy