Application Security

Katrin Jordan
T-Mobile International

OMTP OMA Workshop
Frankfurt 20 April 2007

Overview

- Why
- Aim
- Activities of the OMTP security group
- Application Security Framework
  - The Principle
  - Status
- Way Forward
- Interaction with OMA

WHY

- Exploring the need for application security

WHY

- Steadily increase of mobile devices with application execution environment

- Increase of malware and consequences
  - Unwanted calls and messages
  - Loss of private information
  - Shutdown of phone
  - Spy out personal data
  - Calls to operator customer services
  - Unhappy customers

AIM

- Limit risk of malware
  - **proactively control** an applications execution on a mobile device **based on its level of trust**
- Ensure usability
- Ensure widespread adoption

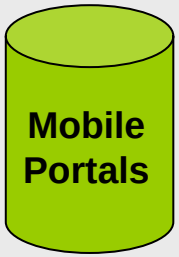
OMTP Security Group

- OMTP Security Project
  - Lead: Tim Haysom,Orange (tim.haysom@orange-ftgroup.com)
  - Strong support by key operators and vendors
- Active tasks
  - Application Security Framework
    - Develop a device based security framework
      - Define different trust levels for applications
      - Define access and prompting conditions
      - Define complemeting device requirements
  - Signing Scheme Requirements
    - Define requirements for 3rd party signing schemes, such that applications signed by these are considered as TRUSTED.

The Principle.

OPEN MOBILE TERMINAL PLATFORM

Device based Application Security



1.Content channels

2. Application Download

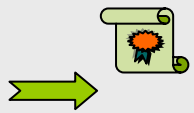
3. Device Security Frameworks

4. Access control

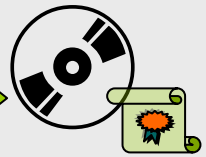
5. Revocation

Signing Process*

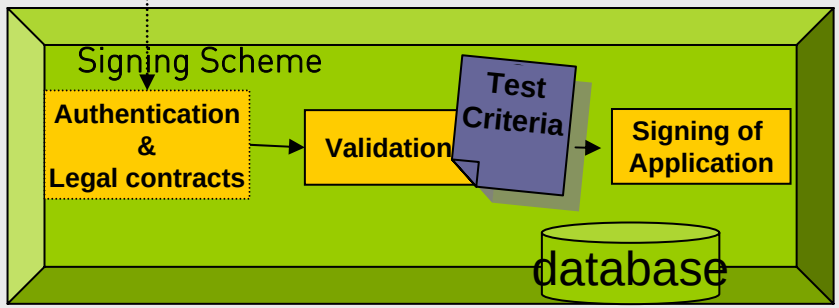
1.Application development

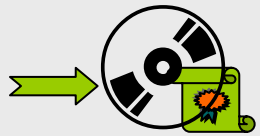


2. Publisher certificate



3.Submission of application





5. Signed application

*The diagram provides an example only. There may be different steps with different proces

Application Security Framework

- Status
  - The conclusion of 18 months work to derive an operator and manufacturer agreed framework to protect customers
  - Released 2nd February 2007
    http://www.omtp.org/docs/OMTP_Application_Security_Framework_v2_0.pdf

OMTP ASF V2.0

- Deliverable includes
  - Definitions of key functional groups
  - Definition of different Trust levels
  - Access and prompting framework
  - Additional device requirements

Security Policies

Functional groupings

Trust levels

Functional groups

- CIRCUIT SWITCHED CONNECTIONS
- PACKET DATA ACCESS
- LOW LEVEL PACKET DATA ACCESS
- MESSAGING (SPECIFICALLY SMS AND MMS)
- SMS – CELL BROADCAST
- LOCAL CONNECTIVITY

Functional groups 2

- READ USER DATA
- WRITE USER DATA
- READ SENSITIVE SIM/UICC DATA
- WRITE SENSITIVE SIM/UICC DATA
- RESTRICTED UICC-ME COMMANDS
- READ/ WRITE APPLICATION DATA
- WRITE GLOBAL NETWORK CONFIGURATION DATA
- WRITE DEVICE CONFIGURATION DATA
- FILE SYSTEM CONTROL AND ACCESS

Functional groups 3

- MULTIMEDIA RECORDING
- GPS (NON NETWORK BASED) LOCATION/ PRESENCE
- NETWORK BASED LOCATION FUNCTIONS
- PROCESS MANAGEMENT
- APPLICATION AUTO INVOCATION
- ACCESS TO AT COMMANDS
- USER INPUT EVENTS
- DRM – ACCESS TO UNENCRYPTED DRM PROTECTED DATA

Trust levels

- Unapproved
- Approved
  - By appropriate signing/ approval schemes
  - At discretion of operator (purchaser)
- Enterprise
  - To support enterprise specific applications
  - Enterprise roots may only be installed by manufacturer or operator
- Operator
- Manufacturer

Installation Requirements

- Terminal SHOULD apply least privilege principle
- Installation prompts
  - Informative of functional groupings
- Revocation of applications (support of OCSP)
- SIM based operator root certificates

Runtime

Access Conditions*

Functional Group / Trust Level	Circuit switched connections	Low level Packet data access	Packet data access	Messaging	SMS-Cell Broadcast	Application auto invocation	Local connectivity	Multimedia recording	Read user data	Write user data	Read Sensitive SIM/UICC data	Write Sensitive SIM/UICC data	Restricted UICC-ME Commands	Write global network config data	Write Device Configuration data	GPS based location/ Presence	Network based location information	DRM - access to unencrypted drm protected data	Read/ Write Application data	Process management	Access to AT commmands	User input events	File system control and access
Unapproved	x	x			x	x				x	x	x	x	x	x	x	x	x		x	x	x	x
Approved											x	x	x	x			x	x		x	x		x
Enterprise Approved											x	x	x	x			x	x			x		x
Operator Approved																		x					
Manufacturer Approved																							

*Note – the framework will be updated with new maintenance

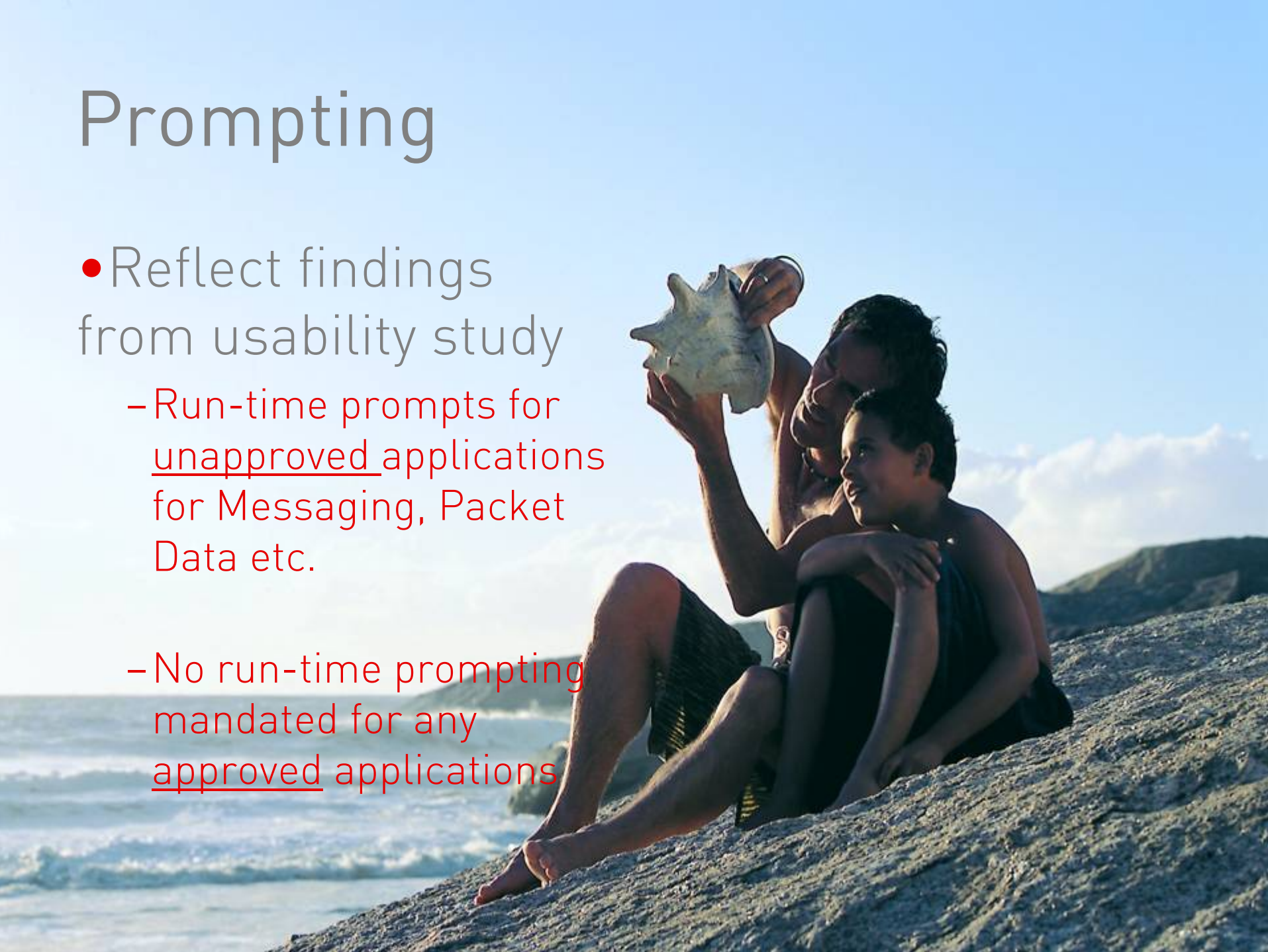
Prompting - less is more

Recap of usability study

- Overuse of prompting will lead users to lose faith in their effectiveness and to ignore them in future
- Security decisions are jarring to the user experience and often cryptic and poorly understood
- Prompts are especially frustrating when they ask users to authorise actions that the user has already authorised implicitly

Prompting

- Reflect findings from usability study
  - Run-time prompts for unapproved applications for Messaging, Packet Data etc.
  - No run-time prompting mandated for any approved applications



Additional requirements

- Users and applications cannot install root certificates
- Local connectivity cannot be switched on by unapproved applications
- No access by low trust applications to authentication data
- No sending of recognised installation files by unapproved applications using device messaging APIs
- Unapproved and approved applications cannot intercept SMS targeted at well known ports
- Any received executable cannot be executed without the user taking deliberate action

Way forward in OMTP

- Continuous improvement, current focus on
  - Prompting and Access Conditions
  - User and Application Data
  - Support of SIM based UICC root
  - Revocation

- Anticipated mid year release of maintenance update
  [see website]

Interaction with OMA

- Any input from OMA is welcome
- Further promotion of the outcome