Trusted Computing Group

• Open industry specifications
• 170+ members
• www.trustedcomputinggroup.org

• Mobile Phone Work Group
  – Mobile Trusted Module
  – Reference Architecture

• Storage Work Group
  – Trusted Storage Specifications
TCG: The “BIG” Picture

Applications
- Software Stack
  - Operating Systems
  - Web Services
  - Authentication
  - Data Protection

Security Infrastructure

Security Hardware

Desktops & Notebooks

Mobile Phones

Networking Applications & Gear

Servers

Storage

TCG Confidential
Copyright © 2007 Trusted Computing Group. - Other names and brands are properties of TCG.

TCG
Standards

ARM Developers’ Conference & Design Pavilion 2007
Why the Time is Right for Mobile Security Standardization… ?

“IDC agrees that there is unlikely to be a major outbreak until the start of 2008”

"Despite this intense vendor - and media-driven speculation - the necessary conditions required for viruses or worms to pose a real rapidly spreading threat to more than 30 percent of enterprise mobile devices will not converge until year-end 2007“ (Gartner)

"A lot of this (cell phone attacks) is hyped to create a market that doesn't exist," said Neil MacDonald, group vice president and research director at Gartner Inc. "The market will exist eventually because the devices are becoming more powerful, but the threat today is minimal and overblown."

Source: Eweek.com, News.com
Mobile Trusted Module Ecosystem

- Mobile Trusted Module embedded in its user environment
- MTM is not an isolated entity inside the mobile device. It communicates externally, protecting both users’ and service providers’ interests.
- Software downloads, mBanking and user privacy are good examples of integrated ecosystem use cases.
Mobile Trusted Module Use Cases

Mobile Trusted Module
IN OPERATION

- PLATFORM INTEGRITY
- USER DATA PROTECTION & PRIVACY
- PROVE INTEGRITY TO END USERS
- SOFTWARE USE
- MOBILE PAYMENT
- MOBILE TICKETING
- DEVICE AUTHENTICATION
- ROBUST DRM IMPLEMENTATION
- SIM LOCK/DEVICE PERSONALIZATION
- SECURE SOFTWARE DOWNLOAD
- SECURE CHANNEL BETWEEN DEVICE & UICC
Mobile Trusted Module (MTM) – Supporting Multiple Stakeholders

**Consumers**
- Enables the protection of user’s personal information
- Better protection against physical theft, remote attacks and malware
- Safer content downloads, mobile ticketing, mBanking transactions, etc.

**Enterprises**
- Open standard: reduced costs compared to non-standard point solutions
- Losses through fraud and theft decreased
- Enables better integration between leisure time and work

**Mobile**
- Reduced in-house R&D costs
- Increased interoperability with other vendors’ products
- Enables advanced, high value services
- Helps to expand supplier base

**Networks**
- Enables more robust platform integrity
- Increased customer confidence and better image
- Common network security infrastructure across devices
- Enables developing more sophisticated services

Source: Nokia & Trusted Computing Group
Allowing Tailored Implementation

One potential implementation model among others

Source: Nokia & Trusted Computing Group
MTM Specification – Collection of Engines

1. Trusted Resources
   - Measurement
   - Storage
   - Reporting
   - Enforcement
   - Protected resources

2. Generic Engine

3. INTERNAL TRUSTED SERVICES

4. Normal Services
   - Service definition
   - Normal resources

5. TRUSTED SERVICES

6. NORMAL SERVICES

ARM Developers’ Conference & Design Pavilion 2007
Different ownership models

PC
- Single party owns outright and expects to control it.
- e.g. User can choose/ hide/vary device identity

Mobile Phone
- Mixed control via regulation, network contract, subsidy etc.
- e.g. User may be legally banned from changing device identity
MTM Options in ARM TrustZone

- MTM as a Native Service
- MTM as a STIP Service
- MTM as a hardware element
- TCG Software Stack (TSS) for libraries and drivers. APIs for applications.
Supporters of the Mobile Trusted Module (MTM)

For more information, please visit:
www.trustedcomputinggroup.org/groups/mobile

Contact:
admin@trustedcomputinggroup.org
TCG Storage Work Group

Mission:

• Open specification for building trust and security into storage devices

• Support infrastructure for trusted storage devices such as key management, tools, commands and APIs
Why Security in STORAGE (Hard Drive)?

• **3 Simple reasons**
  - Storage for secrets with strong access control
    - Inaccessible using traditional storage access
    - Arbitrarily large memory space
    - Gated by access control
  - **Unobservable cryptographic processing of secrets**
    - Processing unit “welded” to storage unit
    - “Closed”, controlled environment
  - **Custom logic for faster, more secure operations**
    - Inexpensive implementation of modern cryptographic functions
    - Complex security operations are feasible
General Risk Model: Storage

Trust = systems operate as intended

Objective: Exercise control over operations that might violate trust

Needed: Trusted Storage commands
Joint Work with
ISO T10 (SCSI) and T13 (ATA)

TRUSTED SEND/IN

(Protocol ID = xxxx …..)

TRUSTED RECEIVE/OUT

T10/T13 defined the “container commands”
TCG/Storage defining the “TCG payload”

Protocol IDs assigned to TCG, T10/T13, or reserved
Implementation Overview

TRUSTED DRIVE

TCG/T10/T13

ATA or SCSI

Firmware

Hidden Storage

Security Providers

Firmware/hardware enhancements for security and cryptography

TRUSTED

Assign Hidden Memory to Applications

• (Partitioned) Hidden Memory
• Security firmware/hardware
• Trusted Send/Receive Commands
• Assign Hidden Memory to Applications

Enterprise Support

ISV Application (on the Host)

Controller

Storage

TCG Confidential
Copyright© 2007 Trusted Computing Group. - Other names and brands are properties of.

Trusted Send and Receive

ISV Application (on the Host)

ARM Developers’ Conference & Design Pavilion 2007
Root of Trust

- Hardware that cannot change can digitally sign and therefore initiate a **chain of trust**
- TPM is a tiny processor on the motherboard that can sign and whose firmware cannot be modified
- Storage devices can be **roots of trust**
Extending Trust to Peripherals

TPer = Trusted Peripheral

Ability to interact with the Platform

Authentication/Attestation

Capability Level

LOW

HIGH

ARM Developers’ Conference & Design Pavilion 2007
Is this a term we are going to use? It's a bit odd.
Trusted Storage with Trusted Platform

Trusted Storage

Secure Communications

Root
Of
Trust

TPM
OR
Trusted
Element

Life Cycle: Manufacture, Own, Enroll, PowerUp, Connect, Use, …
TCG Storage Use Cases (examples)

Full Disc Encryption
- Laptop Loss or Theft
- Re-Purposing
- End of Life
- Rapid Erase

DriveLocking

Forensic Logging

Crypto Key Management
- Crypto Chip
- Personal Video Recorders

DRM Building Blocks

TCG Confidential
Copyright© 2007 Trusted Computing Group. - Other names and brands are properties of.
TCG Storage WG Specification

- **SPs** (Security Providers)
  - Logical Groupings of Features
  - SP = Tables + Methods + Access Controls
- **Tables**
  - Like “registers”, primitive storage and control
- **Methods**
  - Get, Set – Commands kept simple with many possible functions
- **Access Control** over Methods on Tables
Enterprise Management of Full Disk Encryption (FDE) Drives

- **Enterprise Server:**
  - Key generation and distribution
  - Key/Password archive, backup and recovery

- **Laptop (Application):**
  - Master/User passwords, multi-factor authentication, TPM support
  - Secure log-in, “Rapid Erase”

- **FDE Trusted Drive:**
  - Disk or sector encryption, sensitive credential store, drive locking
Next Steps - Storage

• Trusted Storage Specification publicly available 19 June 2007 (www.trustedcomputinggroup.org)
• Seagate has been demo’ing Spec capabilities and has an FDE that is shipping
• Hitachi has announced plans to incorporate FDE capabilities across its product line for PCs
• Workgroup pursuing role in key management issues
• Enterprise-class storage covered by Spec

Storage industry can begin NOW
Summary

- TCG has published open industry security specifications for devices based on ARM processors
  - Mobile Phones
    - https://www.trustedcomputinggroup.org/specs/mobilephone
  - Storage
    - https://www.trustedcomputinggroup.org/specs/Storage/

- ARM Developers should plan to put the TCG Security features into their hardware and software