TCG OPAL Design and Testing

FMS Session 103-A, Security

by

Joseph Chen, ULINK Technology
Why TCG OPAL SED

- Industrial standard
- Supported by major HDD/SSD vendors
- Supported by major SW vendors such as Microsoft
- HW based encryption, no performance impact
- Instant provision and erase
- Strong key management for end user & corporation applications
Introduction of the TCG SWG (Storage Work Group)

SWG builds upon existing TCG technologies and philosophy.

SWG focuses on standards for security services on dedicated storage systems.

SWG defines a common security services for SATA, SCSI, SAS, FibreChannel, USB, IEEE 1394, NAS and iSCSI.

Storage includes HDD, SSD, Removable Drive, Storage Server.

Source: TrustedComputingGroup

Flash Memory Summit 2012
Santa Clara, CA
OPAL AES Encryption Diagram
OPAL TPer and Storage Device

Host Interface

- SATA/SAS/USB/MMC

OPAL TPer

Security Protected Storage
OPAL Credentials/Authorities

- **MSID**
  - Manufacture PIN (C_PIN_MSID)

- **SID**
  - TPer Owner SID (C_PIN_SID)

- **Admin**
  - Admin PIN (C_PIN_Admin1 – C_PIN_AdminXX)

- **User**
  - User PIN (C_PIN_User1 – C_PIN_UserMM)

- **PSID**
  - Physical ID PIN (C_PIN_PSID)
  - Physical Drive Owner
OPAL TPer, SP and Authority

Admin SP
(Security Provider)

TPer
(Trusted Peripheral)

Locking SP
(Security Provider)

TPer Owner

TPer Owner

Anybody

Admins

Actors/Authorities

Users

Admin SP
(Trusted Peripheral)
OPAL Configuration Example

1. Get MSID
2. Authenticate SID
3. Activate Locking SP (SingleUserMode)
4. Enable TPer_Reset
5. Assign Anybody Erase on all Ranges
6. Authenticate Admin1
7. Get Ranges and Users Info
8. Check K_AES and Protect Mechanism
9. Assign Anybody Read Access on Datastore
10. Clear Admin1 Authority (Enable=0)
11. Authenticate User_X
12. Setup LBA Range for User_X
13. Configuration Completed
14. Setup User_X PIN
15. Setup R/W Lock for the LBA Range
OPAL Unlocking Example

1. Power UP OPAL
2. Level 0 Discovery
3. Get Host and TPer Properties
4. Check OPAL Life Cycle
   - Check K_AES, Protect Mechanism
5. Unlock LBA Range for USER_X Read/Write
6. Authenticate User_X
7. Check Locking/Authority Table
8. Continue Boot from Unlocked LBA Range
9. Ready to Use
10. Boot from Unlocked LBA Range
11. Ready to Use
LBA Range Assignments Example

- No LBA Range Assigned
- LBA Range 1 and 2 Assigned

User 1: Assign LBA Ranges
User 2: Assign LBA Ranges
User 3
User N

Global Range
Max LBA

0

LBA Range 1
LBA Range 2
Max LBA
OPAL Commands for SATA/SAS/USB/eMMC/NVMe

- **SATA/ATA/CFA**
  - TRUSTED SEND (5Eh/5Fh) PIO/DMA
  - TRUSTED RECEIVE (5Ch/5Dh) PIO/DMA

- **SAS/SCSI, USB, UAS, UFS**
  - SECURITY PROTOCOL OUT (B5h)
  - SECURITY PROTOCOL IN (A2h)

- **eMMC**
  - SET BLOCK COUNT (CMD23)
  - PROTOCOL WR (CMD54)
  - PROTOCOL RD (CMD53)

- **NVMe**
  - SECURITY SEND (81h)
  - SECURITY RECEIVE (82h)
Microsoft eDrive Requirements

What is an eDrive?

• A regular storage subsystem (Embedded MultiMediaCard, solid-state drive, hard disk drive, usb) that comes with hardware offload to accelerate crypto processing

How is it different from SEDs?

• Self-encrypting drive: Trusted Computing Group (TCG) standards
• Encrypted drive: TCG standards (OPAL v2.0) + IEEE 1667

Why should the ecosystem care?

• Initial-time hardware-based encryption is negligible
• Faster than software-based encryption during standard operation
• Removes initial and on-going performance hit
• Standardized in-box support can enable broad adoption

Source from Microsoft
DriveMaster
OPAL Test for Multiple Interfaces

One Test Script
OPAL Test Scripts
... ...
IEEE 1667 Option

ULINK
DriveMaster
OPAL Test Station

HBA

SATA OPAL Device
SAS OPAL Device
USB OPAL Device
eMMC OPAL Device

Test on Multiple Storage Interfaces

Test Results
DriveMaster Testing Applications

1. On Screen GUI
   - GUI to Retrieve Device Information
   - GUI to Control Device State, i.e. Reset, Activate

2. User Defined Scripts
   - Create OPAL Command Sequence
   - Create Exceptional Cases for Error Handling Test

3. Turnkey Test Suites
   - OPAL Test Case Suites
   - IEEE 1667/eDrive Specific Test Suites

Disclaimer:
This OPAL Test Suites is developed and managed by ULINK and not TCG
ULINK Technology OPAL Testing Tutorial Workshop -
September 11 & 12, 2012

This workshop consists of 2 sessions conducted on 2 separate days. Each session include a 2 hour lecture and a 1 hour practice. The tutorial topics are:

- Explanation of OPAL technology
- Explanation of Trusted Storage Architecture, the roles of Trusted Peripheral and Security Provider
- Testing / Validation methodology for OPAL devices
- Practice OPAL commands using Drivemaster tool

Where: Tuesday Sept 11 from 1pm to 4pm (PST) AND Wednesday Sept 12 from 1pm to 4pm (PST)

Fee: $895 per person (Register by August 14 to be eligible for a $100 discount)

***Each registrant will receive a FREE Testing Service in confidence of TCG Storage OPAL test cases v1.0 for one device. (This Testing Service is regularly priced at $2,000)

Seating is limited. So please register early. (We reserve the right to cancel the class if the number of registrants does not meet our target)

Click in this block to add your text and images to promote your event. You can add more blocks to this Event Homepage by selecting Add Blocks above.

Register Now!
For more information please contact
Joseph.chen@ulinktech.com
Edwin.kuo@ulinktech.com

Visit our Booth #701
In the Exhibition Hall
THANK YOU!

THANK YOU!

Flash Memory Summit 2012
Santa Clara, CA
DriveMaster ControlPanel GUI

- **Device Capabilities**
- **Level 0 Discovery**
- **COMID/MSID**
- **K_AES/PSID Support**
- **Stack/TPer Reset**
- **Get/Set Properties**
- **Activate/Revert/RevertSP**
- **Get Current State**
- **IEEE1667 Probe**
- **IEEE1667 TCG Get Silo Capabilities**

**GUI Functions**

**Device Capabilities**

**Level 0 Discovery**

**COMID/MSID**

**K_AES/PSID Support**

**Stack/TPer Reset**

**Get/Set Properties**

**Activate/Revert/RevertSP**

**Get Current State**

**IEEE1667 Probe**

**IEEE1667 TCG Get Silo Capabilities**
DriveMaster ControlPanel GUI (Cont.)

GUI Functions (Cont.)

Table Contents
- AdminSP/LockingSP
- ALL Object Tables over SP
- Individual Table

Get/Set Byte Table
- MBR Byte Table
- DataStore Byte Table

Methods
- Random
- Authenticate
Security Protocol 1 – Generic
- LEVEL 0 DISCOVERY
- PROPERTIES
- START SESSION
- SYNC SESSION
- START TRUSTED SESSION/
- SYNC TRUSTED SESSION
- ENDSESSION/CLOSESESSION
- GET ACL
- NEXT
- AUTHENTICATE
- GENKEY
- GET
- SET
- START TRANSACTION
- END TRANSACTION

Security Protocol 1 – FeatureSet
- ACTIVATE/REACTIVATE (OPAL)
- REVERT/REVERTSP (OPAL)
- ERASE (ENT/OPAL FeatureSet)
- RANDOM (ENT/OPAL v2.0)

Security Protocol 2
- GET_COMID
- HANDLE_COMID_REQUEST
- GET_COMID_RESPONSE
- VERIFY_COMID_VALID
- STACK_RESET/TPer_RESET

IEEE1667 - Security Protocol 0xEE
- PROBE Silo
- TCG Silo
  - Get Silo Capabilities
  - Transfer/Get Transfer Result
  - Stack Reset/TPer Reset
## DriveMaster OPAL Command Examples

<table>
<thead>
<tr>
<th>DriveMaster Commands</th>
<th>Purposes</th>
<th>Examples</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCG_Discovery</td>
<td>Get Level 0 Discovery Information</td>
<td>TCG_Discovery</td>
<td></td>
</tr>
<tr>
<td>TCG_SetHostProperties</td>
<td>Set Host Property</td>
<td>TCG_SetHostProperties</td>
<td></td>
</tr>
<tr>
<td>TCG_GetTPerProperties</td>
<td>Get Host &amp; TPer Properties</td>
<td>TCG_GetTPerProperties</td>
<td></td>
</tr>
<tr>
<td>TCG_StartSession</td>
<td>Start Session</td>
<td>TCG_StartSession 1, 000000205000000001h, 1</td>
<td>HostSID = 1, SPUID = Admin SP, Write = 1</td>
</tr>
<tr>
<td>TCG_SyncSession</td>
<td>Sync Session</td>
<td>TCG_SyncSession</td>
<td></td>
</tr>
<tr>
<td>TCG_HostEndSession</td>
<td>End Session</td>
<td>TCG_HostEndSession</td>
<td></td>
</tr>
<tr>
<td>TCG_TPerEndSession</td>
<td></td>
<td>TCG_TPerEndSession</td>
<td></td>
</tr>
<tr>
<td>TCG_Get_Rqs</td>
<td>Fetch the values of selected table cells</td>
<td>TCG_Get_Rqs 1, v0</td>
<td>Define the scope of the data to be retrieved</td>
</tr>
<tr>
<td>TCG_Get_Rsp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCG_Set_Rqs</td>
<td>Change the values of selected table cells</td>
<td>TCG_Set_Rqs</td>
<td>Define location and values to be changed</td>
</tr>
<tr>
<td>TCG_Set_Rsp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TCG_Activate_Rqs</td>
<td>Manage the life cycle of manufactured SPs</td>
<td>TCG_Activate_Rqs 00000205000000002h</td>
<td>SPUID = LockingSP</td>
</tr>
<tr>
<td>TCG_Activate_Rsp</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ULINK Test Suites

Shipping Products

- OPAL Test Cases Suite
- Enterprise Application Notes Suite
- OPAL Application Notes Suite

Developing Products

ULINK Protocol Suite
Including OPAL v2.0, eDrive, more
### Section A: Basic Grammar - Generic

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>ULINK Test Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>A0: Identify Device</td>
<td>IdentifyDevice</td>
</tr>
<tr>
<td>A1: Trusted Send/Receive</td>
<td>TCGSend_Recv</td>
</tr>
<tr>
<td>A2: Protocol ID = 0 related</td>
<td>ProtocolID_0</td>
</tr>
<tr>
<td>A3: Level 0 Discovery</td>
<td>Discovery0</td>
</tr>
<tr>
<td>A4: Synchronous Communication Protocol</td>
<td>SynchroPtc</td>
</tr>
<tr>
<td>A5: ComPacket/Packet/SubPacket</td>
<td>ComSubPacket</td>
</tr>
<tr>
<td>A7: Transaction</td>
<td>Transaction</td>
</tr>
<tr>
<td>A8: Ending Session</td>
<td>EndSession</td>
</tr>
<tr>
<td>A9: Empty Atom</td>
<td>EmptyAtom</td>
</tr>
<tr>
<td>A10: Properties</td>
<td>PropertiesSet PropertiesGet</td>
</tr>
<tr>
<td>A11: Start/SyncSession()</td>
<td>StartSyncSession StartSyncSession_OptParams</td>
</tr>
</tbody>
</table>

### Section A: Basic Grammar - Method

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>ULINK Test Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>A6: Method invocation/response</td>
<td>Method_RegSession Method_CtrlSession</td>
</tr>
<tr>
<td>A12: Get()</td>
<td>Get_Byte_GramChk Get_ObjAdminSP_GramChk</td>
</tr>
<tr>
<td>A13: Set()</td>
<td>Set_Byte_GramChk Set_ObjLKSP_GramChk</td>
</tr>
<tr>
<td>A14: Next()</td>
<td>Next_AdminSP_GramChk</td>
</tr>
<tr>
<td>A15: GetACL()</td>
<td>GetACL_AdminSP_GramChk</td>
</tr>
<tr>
<td>A19: RevertSP()</td>
<td>RevertSP_GramChk</td>
</tr>
</tbody>
</table>

### Section C: Table Contents

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>ULINK Test Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1: Level 0 Discovery contents</td>
<td>DiscoveryTable</td>
</tr>
<tr>
<td>C2: Properties() contents</td>
<td>PropertiesTable</td>
</tr>
<tr>
<td>C3: Get() contents</td>
<td>Get_ByteTable_All Get_ObjTable_AdminSP_All Get_ObjTable_LockSP_All</td>
</tr>
<tr>
<td>C4: Next() contents</td>
<td>Next_Table_AdminSP Next_Table_LockSP</td>
</tr>
<tr>
<td>C5: GetACL() contents</td>
<td>GetACL_Table_AdminSP_All GetACL_Table_LockSP_All</td>
</tr>
</tbody>
</table>

### Section D: Grammar and Effect

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>ULINK Test Scripts</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1: ACE.Set()</td>
<td>ACESet</td>
</tr>
<tr>
<td>D2: Authority.Set()</td>
<td>AuthoritySet</td>
</tr>
<tr>
<td>D3: C_PIN.Set()</td>
<td>C_PinSet</td>
</tr>
<tr>
<td>D4: Locking.Set()</td>
<td>LockingSet_RangeStartLength LockingSet_ReadLock / LockingSet_WriteLock</td>
</tr>
<tr>
<td>D5: MBRControl.Set()</td>
<td>MBRControlSet</td>
</tr>
<tr>
<td>D6: MBR.Set()</td>
<td>MBRSet</td>
</tr>
<tr>
<td>D7: DataStore.Set()</td>
<td>DataStoreSet</td>
</tr>
<tr>
<td>D8: K_AES_*.GenKey()</td>
<td>GenKey_Effect</td>
</tr>
<tr>
<td>D9: Activate()</td>
<td>Activate_Effect</td>
</tr>
<tr>
<td>D10: Revert()/RevertSP()</td>
<td>Revert_AdminSP_Effect Revert_LockSP_Effect / RevertSP_Effect Act_Revert_RstrCmds</td>
</tr>
<tr>
<td>D11: Power Cycle</td>
<td>PowerCycle</td>
</tr>
</tbody>
</table>