IEEE P1667
Authentication-Standard-for-Transient-Storage-Devices

T10 Meeting

Austin, TX

November, 2005

Why Such a Stupid Acronym…

- Dynamically Attached Devices and Device Interfaces Working Group
  - Is developing a “Standard Protocol for Authentication in Host Attachments of Transient Storage Devices”
- So suddenly P1667 doesn’t sound all that bad…☺ (could have been worse 802.11 etc…)

What are Transient Storage Devices?

- TSD's are devices which offer removable mass storage capacities
  - Either as unique personal storage device or
  - Part of another device
- Provide invaluable features for enterprise users
  - Access to corporate data from any communications platform (phone, PDA, PC etc)
- Agnostic to Interface
  - Connection protocol
  - Form factor, connector (UFD, Memory Card, SIM
  - Target host (PC or mobile device)

TSD's are Everywhere

- Huge user acceptance and comfort level
- Users educated about how to use Mass Storage devices
  - Agnostic to form factor
- Users want to transfer their TSD's between hosts and platforms seamlessly
  - Use same TSD in mobile device and PC

Transient Personal Storage Devices Are Great BUT

- Their popularity has security side effects
  - They get lost/stolen along with personal/sensitive information
  - They are an agent for transferring data without proper authorization
  - They enable the transport and execution of malicious software
- These side effects are particularly offensive in the enterprise/corporate world

Industry Reaction to Threat

- Enterprise users and corporate IT departments have increasingly limited access of TSD's to hosts in order to minimize threat
  - USB ports physically disabled by many companies
  - Inhibiting factor for large scale use of TSD's in mobile devices
  - Other ports can be blocked, too
  - Constraint on enterprise use of removable storage
- OS vendors will allow mechanisms for hosts to control mass storage device access
  - IT managers will enable/disable policy

Need for a Standard Authentication Solution

- Many device manufacturers began offering security applications together with their devices
  - Required drivers
  - Executables
  - No transparency on security scheme level or quality
- A Standard security scheme requires host side/OS involvement
- Changes to major OS's (PC, Mobile) can be made **only** for a standard solution

Where IEEE P1667 Began

- P1667 initially spun off from the USB-IF (attempted) Secure-MSC specification
  - USB-IF BoD interested in focusing on access control (password based lock of device)
  - P1667 is lower layer. USB-IF MSC-lock spec (or any other access control scheme) runs on top of P1667 at Application Layer

Authentication for TSD's

- The Core requirement is to associate a TSD to a specific organization, person, device and location
- P1667 enables authentication of TSD to host and vice versa.
- Authentication initiated by host OS
  - Functionality "pulled" by host
  - Driverless
  - No executable

P1667 Use Cases

- Secure Enterprise
  - Authenticate the identity of the device and its ownership
  - Only allow authenticated devices to mount – authentication requires positive identification of the device. Device cannot enumerate before authentication
  - Access control is supplied by the host – device only needs a trusted ID
- Secure Device
  - Device will only mount according to access control rules
  - Device requires positive identification of the host it is attaching to before allowing the host to access it

P1667 Use Cases Cont.

- Secure Content
  - Device and host may not trust each other in the context of some secure data or licensed software
  - DRM system around data needs to authenticate the host, device, and a relationship between them
  - P1667 only focuses on the authentication of the components, not the (content) access control mechanism

P1667 Migration to Mobile Devices

- Mobile devices (other than PC-s) use of TSD/MSC devices growing dramatically
  - Memory cards
  - USB connectors showing up, can connect UFD
  - MegaSIM
- P1667 protocol and command set designed to compliment all of these

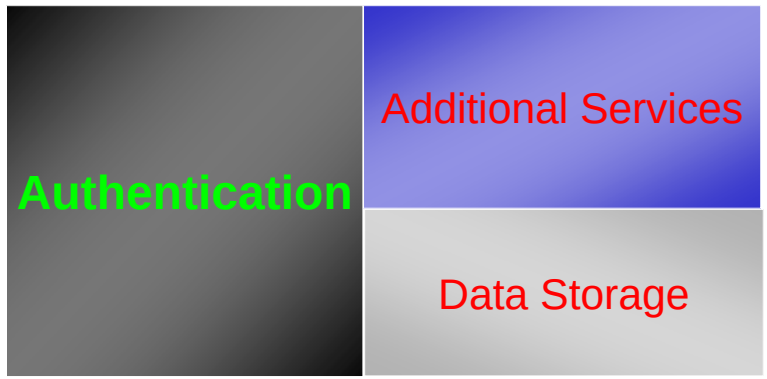
P1667 and TCG

- TCG and P1667 are closely collaborating
  - P1667 is “TCG’s Little Brother”
  - Where dedicated H/W (like TPM) is not available, authentication performed via P1667 channel
  - Consistent with TCG command set and structure to assure all P1667 compliant devices can become TCG/TPM compliant when H/W becomes available on mass level.

Current P1667 Status

- Use case document complete
- Requirements document complete
- Specification draft available to members
- Command set requirements to be coordinated with relevant standards bodies to assure uniformity and conformity:
  - **T10 (SCSI),** T13 (ATA), TCG, USB/DWG
  - Present work to OMA DRM, Security/Smart Cards Group, GSMA/SCaG

IEEE P1667 Area of Responsibility



Host (PC or Mobile device

Transient Storage Device

IEEE P1667

Security Services

Hardware

IEEE

Membership and Meetings

- Checkpoint, Kingston, Microsoft, M-Systems, Lexar Media, U3, Mobey Forum, Seagate, Dell, Aladdin, RSA, Mcafee, TCG
- Meetings every 6-8 weeks
- Next meeting December 14, Helsinki
- “Guest” participation, without voting rights
- To gain voting membership rights, company needs to join IEEE, and the P1667 WG.

THANK YOU!

For Further Information:

Ariel.Sobelman@m-systems.com

or

Avraham.Shimor@m-systems.com