



IEEE 1667 and Portable Device Authentication

James Borden

Senior Technical Evangelist

Microsoft Corporation

IEEE 1667 – Standard Protocol for Authentication in Host Attachments of *Transient Storage Devices*

- What are they?
 - Storage Devices which offer removable mass storage capabilities
 - Unique personal storage device (e.g., UFD, USB Hard drives)
 - Part of another device (e.g., media players, cell phones)
 - Interface Agnostic
 - Connection Protocol
 - Form factor, connector
 - Target Host

Transient Storage Devices

Current Landscape

- Broad User Acceptance
- Expectation of Ease of Use
 - Form factor independence
 - Seamless use between Hosts and Platforms (e.g., same TSD in mobile device and PC)
- Popularity has Highlighted Significant Gaps in Security
 - Lost/Stolen Data
 - Malicious Software
 - Corporate Banishment

Transient Storage Devices – Security

- There has been Progress
 - Device-level password support on UFD (“MSC-Lock”) for “Lost UFD” scenario
 - Enterprise Security Applications bundled with hardware
 - Custom Drivers
 - Executables
 - Inconsistent Implementation (e.g., “faux” encryption)
- A Comprehensive Security Solution requires host/OS involvement
- OS changes require standard hardware solutions

- Need for a device/bus agnostic approach for security
 - Lightweight
 - Timely to Market
 - Complementary to existing Specs and Initiatives (MSC-Lock (USB-DWG) and TCG)
 - Two-way authentication
 - Functionality “pulled” by host
 - Host-provided drivers
 - Host-provided Executables
- Extensible

IEEE 1667 – Status

- V1.0 Specification Complete (December 2006)
- Broadly supported Working Group
 - Fifteen (plus) Participating companies
- Spec-based hardware and software development actively ongoing
- Soliciting Companies to apply for 1667 Silo Identifiers