PC Platforms and High Assurance Implementation

Michael Thompson
mft@netpipe.com

Strong Access Controls on PCs Require a Secure Initial State

- PC Manufacturers Recognize Security Need
- Weak Solutions Exacerbate the Problem
- Trusted Subsystem for Secure Initial State
- Distributed Dynamic Labels & Global Root
- TCB Extension Achieves SAC With COTS
PC Platform Manufacturers Recognize Security Need

- Endpoint Security Critical to E-Commerce
- Trusted Computing Platform Alliance
  - Mainstream PC Manufacturers (IBM, HP, etc.)
  - Core Hardware Module and Boot Block
  - Specification Targeted at Business Customers
  - Signing Up to “Trusted Computing”
- Strength of Security as Vendor Distinctive
  - Commercial Platforms as High Assurance

Weak Solutions Exacerbate the Problem

- Soldered Boot Proms
  - Modifiable by Software (e.g., Flash RAM)
  - “Protected” by Global Passwords
  - Cannot Boot to Strong Access Controls
- Traditional Replacement of Boot Proms
  - Swap With High Assurance Boot Proms
  - Result in Non-standard Hardware Platform
- Flexibility Via a High Assurance Subsystem
  - High Assurance Immutable Boot Block
  - Trusted Platform Subsystem Controls Boot
**Trusted Subsystem for Secure Initial State**

- Signed Code Certificate
- Quality Attribute
- Software Loader

**Owner**
- Secure Boot Constraints

**Trusted Platform Subsystem**
- Compute Label
- Validation Profile
- Global Root
- Immutable Boot Block

**Secure Boot Constraints**
- Trusted Platform Subsystem
- Compute Label
- Validation Profile
- Global Root
- Immutable Boot Block

**Distributed Dynamic Labels & Global Root**

- Root “Liability Assuming”
- “BFG Root”
- TCPA Registry
- Enterprise “Identity”
- CA
- HP
- CA
- Phoenix

- Principle “User”
- Production
- Platform Certificate
- Endorsement Certificate
- Signed Code Certificate
- Signed Code Certificate

- DDL
- DDL
- DDL
- DDL
TCB Extension Achieves SAC With COTS

Standard PC Hardware & Software

- Standard Client Applications
- COTS Client Operating System (e.g., Windows)
- Trusted Subsystem For Secure Boot

TCB Extension (Plug-in Card With Processor)

- Protocols & Custom Functions
- High Assurance TCB With SAC
- Hard Disk
- Network

Driver