Security Comparison

Security Software Solutions

Features

- Various levels of security
- Customizable to meet individual needs
- Field proven and lab approved
- Expert technical support provided

Feature Summary

	SecureBoot™ Level 1	SecureBoot™ Level 2 (not yet available)	TPM Suite	iButton®
Primary Function	▪ Verify mass storage media before boot. ▪ SHA-1 hash.	(Slimmed down version of TPM suite with reduced TSS API commands tailored to gaming.)	▪ Hardware and software security architecture for validation of platform, BIOS, firmware and application. ▪ Can be used with encryption ▪ Lock software to platform. ▪ Avoid cloning of s/w or hardware.	▪ Hardware security dongle. ▪ Secure RTC for licensing and leasing. ▪ Others depending on ibutton chosen. See http://www.ibutton.com
Primary Market/Regulations	GLI-11, NVGCB	Any	Any	Any
Architecture	BIOS extension	TPM based. Reduced TSS implementation	TPM chip on motherboard, CRTM BIOS, hardware drivers, extensive TSS API, encryption libraries.	One or two ibutton devices installed on the DPX motherboard.
Compatible Motherboards	All	All	All with TPM option installed	All
Hardware Option Required	None	TPM	TPM	ibutton carrier, ibutton device
OS Support	Does not depend on OS	Windows XP, XP Embedded, Linux	Windows XP, XP Embedded, Linux	Windows XP, XP Embedded, Linux
Fees, Licensing	One time fee plus per unit license	One time fee plus per unit license	One time fee plus per unit license	One time fee plus per unit license
Ease of Implementation	Easy to medium	Medium	Medium to hard	Easy to medium

Support & Downloads

www.advantech-innocore.com/support/

Datasheets

- Software overview datasheet
- SecureBoot™ datasheet
- TPM suite datasheet
- iButton®/GPIO datasheet

BIOS, Driver, Manual, and Certification (Log-in required)

- SecureBoot™ manual
- TPM suite manual and implementation guide
- iButton®/One-wire SDK manual