SecureBoot™

Security ROM Code SDK

Features

- Toolkit for preparing security ROM code
- Customized for individual applications
- Field proven
- International gaming regulation compliance

Introduction

SecureBoot™ SDK provides a toolkit for the developer to produce low-cost, low-overhead security mechanisms for gaming machines. The mechanisms security features cover various aspects of security control and ensure:

- Customers' software applications can only run on designated hardware.
- Designated systems only run designated software.
- Compliance with U.S. and international gaming regulations for media validation.

SecureBoot™ is suited to tightly controlled environments where physical security of the machine and its environment are reliable. SecureBoot™ SDK offers several security schemes, each customisable to individual requirements. The SDK tools allow development of security ROM code that works in conjunction with the system BIOS. The game application boots normally only if verification completes successfully.

Simple Single-Stage Solution

This is the most common solution deployed. SecureBoot™ verifies contents of the boot medium using SHA-1 hash function of a chosen section of the boot media; and halts the system if verification against golden values fails.

Two-Stage Solution

In a two state SecureBoot™ mechanism, the boot process proceeds as for the single-stage solution but the verification is applied to a second stage which contains further verification code and a RSA Certificate (public key only).

This is then used to check the game application's signatures.

Package Contents

The package includes the following;

- Compiler/Assembler and tools
- Sample source code
- Sample precompiled binaries for Advantech-Innocore products
- User manual describing key concepts, protection schemes and sample code

Development Machine Requirements

- Linux®, Windows® XP (SP3) or Windows® 7
- 768MB RAM
- 10MB disk space

OEM Customization and Product Development

- Advantech-Innocore specializes in the fields of PC-based hardware design and software development. Our in-depth knowledge and global resources make us your ideal partner.
- Advantech-Innocore is part of the Advantech Co., Ltd. Group of Companies.
- Specifications subject to change. E&OE.
-