Pay TV Transport Chip / STB SOC Security

November 6, 2008
Presentation to the Copy Protection Technology Working Group (CPTWG)
Introduction

- Cryptography Research, Inc (CRI) is deploying security hardware (the CryptoFirewall™) in transport chips / STB SOC (System on Chip) used in set top boxes
- SypherMedia International (SMI) is building software solutions (the SypherMedia Kernel) that support the CryptoFirewall and provide a high level of security for Pay TV and other STB security applications

**CryptoFirewall™ in Transport chip (SOC)**
- Security ASIC core
- Provides the most tamper resistant hardware security available using standard silicon manufacturing processes
- Deployed in >50M devices, typically in smart cards
- Perfect security track record

**SypherMedia Kernel™ in Set Top Box**
- Receives and processes Kernel section of EMM and ECMs
- Manages encrypted keys and CF interface

**SypherMedia Gatekeyper™ in Headend**
- Interface to broadcast distribution
- Bitmap and Encrypted key generation
- Generates Kernel Section of EMM & ECMs
Key advantages

- **CryptoFirewall and SypherMedia Kernel are independent technologies that work together**
  - SMK can work on non-CryptoFirewall platforms, but the CF adds hardware security
  - CryptoFirewall supports other software/CA layers, but the SMK provides a complete solution

- **CF+SMK are a compelling STB security solution:**
  - Security enforced in silicon
    - Does not assume software is trusted
  - Supports all major distribution channels
    - Satellite, Cable, Digital Terrestrial, IPTV
    - Enables STB subscription, eliminates Free-to-Air STB attacks
  - Can be incorporated by any Transport Chip vendor
    - Designed for straightforward head-end integration
    - Complementary to CA systems and existing smart card functionality
  - Cost effective
    - Less expensive and more secure than separate chips/cards/modules
Overview

SypherMedia Gatekeyper generates and distributes encrypted keys

Headend

SMK manages the process

Transport Chip (STB SOC)
Control word generation

- Traditional control word generation consists of manipulating pre-existing bits in the ECM
- With this system, Control Words are no longer incorporated solely as part of the broadcast stream
  - Built “on the fly” from various contributors

Control Word

- Contribution from Smart Card (if any)
- Contribution from Custom Security Function (if any)
- Contribution from Additional Sources (if any)
- Contribution from Transport Chip CF
Flexible key distribution

- System can be run by broadcast operators or the Conditional Access (CA) provider
  - Works in conjunction with but does not replace CA system

- HW enforced key distribution controlled by the SypherMedia Gatekeyper™ in the Headend
  - System employs bitmap technology for efficient service/channel allocation to key distribution

- CryptoFirewall™ core provides hardware enforcement of these policies
  - General addressed keys
  - Unique addressed keys

- Algorithmic separation between broadcasters and transport chip vendors
Development and integration

- Fab integrates CryptoFirewall™ with Transport Chip / STB SOC
  - Provides hardware security embedded in a single transport chip
  - STB unique keys delivered in Kernel section of EMMs
  - CryptoFirewall™ output mixed with final CA Control Word (if present) and fed directly into secure key cache
    - Hardware path

- STB cannot generate control words if it does not receive “renewals” from the SypherMedia Gatekeyper™ head-end
  - Eliminates use of FTA boxes
  - Eliminates Internet-based Dream Box attacks
  - Trusted silicon core for protecting IPTV platforms and other systems currently lacking hardware security
Business process

- CryptoFirewall is a selectable feature in Transport Chips / STB SOC
  - Purchasing process same as for optional chip features
  - Chip maker enables hardware fuse on chips where the license fee was paid

- Headend and STB/Transport design provided in general CF license at no additional cost
  - If custom solutions are required, SMI can develop headend and STB software for client for time & materials

- For more information on business and licensing:

  Kit Rodgers  
  Vice President, Business Development  
  Cryptography Research, Inc.  
  kit@cryptography.com  
  +1 415 397 0123

  Gregory J. Gagnon  
  Vice President, Business Development  
  SypherMedia International  
  gjgagnon@smi.tv  
  +1 310 977 4700