CryptoFirewall™ Technology Introduction

Cryptography Research, Inc.
www.cryptography.com
575 Market St., 21st Floor, San Francisco, CA 94105

About Cryptography Research, Inc.

- Founded in 1995
- Provide security technology and services to companies that build and use security products
- Seek to anticipate long-term trends and develop "must have" solutions to complex problems
- Products designed by CRI engineers secure over $100 billion annually

Our focus is solving complex fraud and digital piracy problems

Our business

Technology Licensing

- DPA: Hardware tamper resistance
- CryptoFirewall: Protecting Pay-TV signals (satellite, cable) and other tamper-resistance applications
- SPDC/BD+: Renewable security platform for digital content

Services

- Product/technology evaluation
- Security design assistance
- Education

Primary Industries Served

- Financial Services
- Pay Television
- Wireless/Telecom
- Internet
- PC hardware/software
- Smart Card
- Entertainment

Cryptography Research

Specialists in Solving Complex Data Security Problems 3

CryptoFirewall™ Overview

Specialists in Solving Complex Data Security Problems 4

Cryptography Research

The tamper resistance problem

Effective hardware security difficult in high-risk environments

- Applications: Anti-piracy/pay TV, printer consumables, value transfer
  - Determined adversaries willing to reinvest profits from past attacks
- Business models depend on robust hardware
  - Hardware replacements are expensive or impossible
  - Adversaries have physical possession of security device
  - If security fails, attackers can reverse engineer, emulate, clone system
- A hard problem: Many past tamper resistant designs have failed
  - Bug exploitation (buffer overflow, protocol failure…)
  - Non-invasive attacks (timing, power analysis, glitching/fault induction…)
  - Invasive attacks (decap and reverse engineering, die extraction…)

Academic papers about security hardware (smart cards, TPMs, etc.) are published in the proceedings of the Cryptographic Hardware and Embedded Systems (CHES) conference.

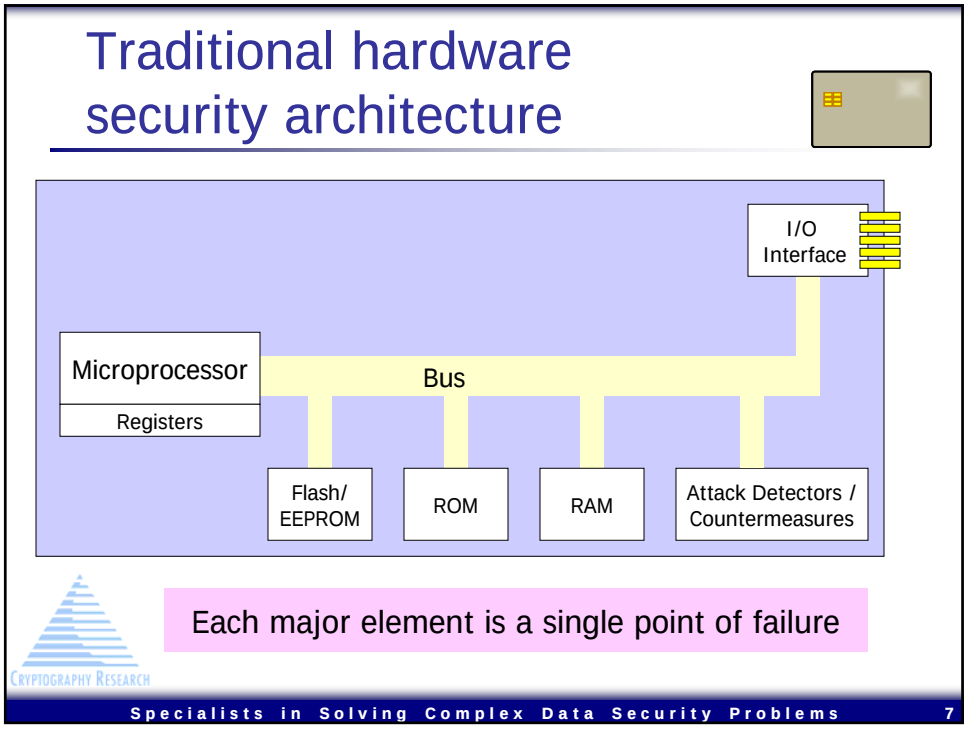
Specialists in Solving Complex Data Security Problems 5

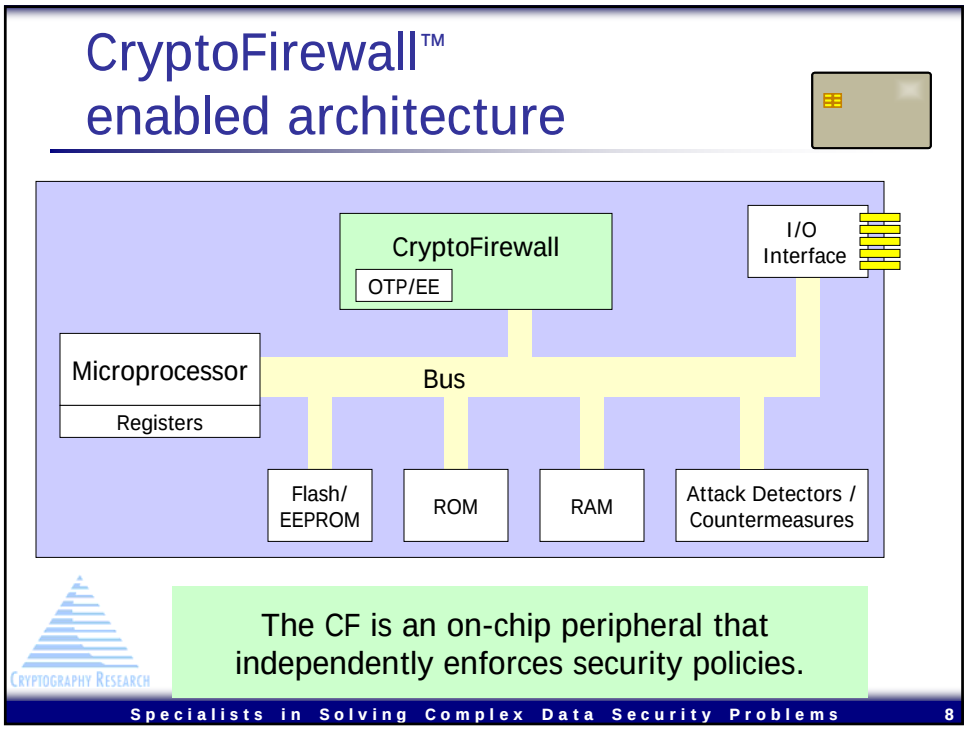
CryptoFirewall™ overview

A HW core that ensures cryptographic security and tamper resistance.

- Technology objectives
  - Robust enforcement of critical policies
  - Complement existing security systems & design processes
  - High assurance, designed for open review
- Design team
  - Leader in tamper resistance technology & research
  - Cryptography, design assurance, system robustness
- Field proven
  - >50M fielded devices, piracy eliminated in deployments

Specialists in Solving Complex Data Security Problems 6





Security & Compatibility

Security core that does not rely on microprocessor

- Independent enforcement of security policies
  - A layer of defense independent from the rest of the card
    - No single point of failure: Piracy prevented if either standard CA elements or CryptoFirewall is intact
  - CF ensures signal security even if other security components (e.g., set-top box, smart card, etc.) are compromised

Emphasis on compatibility

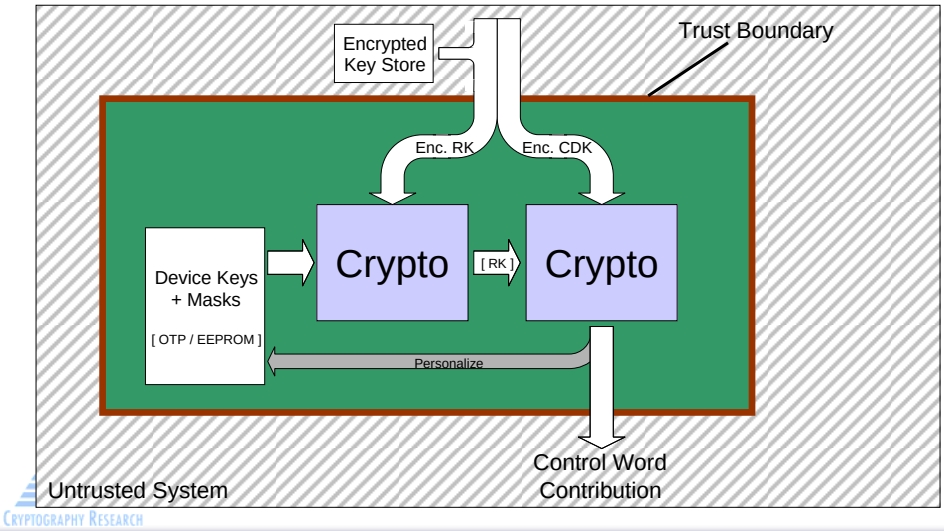
- System architecture unchanged
  - Pay TV: No change is required to set-top box architecture
    - Support advanced STBs (control word encryption, DVR)
- Compatible with existing protocols
  - Pay TV: Standard DVB stream (w/SimulCrypt compatibility)
  - Minimal head-end impact (none if inactive)

Specialists in Solving Complex Data Security Problems 9

CryptoFirewall™ Design Features

Specialists in Solving Complex Data Security Problems 10

Protocol architecture (Pay TV)

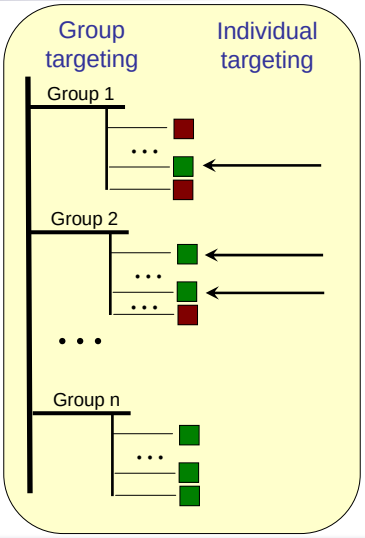


Specialists in Solving Complex Data Security Problems 11

Key management: Rights keys (Pay TV)

Access enforced by rights keys

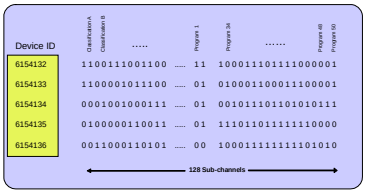
- Encrypted Rights Keys (ERKs) packaged for group or individual devices
  - Keys updated in broadcast, point-to-point, pre-stored E^2
  - Encrypted keys cached by (untrusted) µP
- Decrypted keys never leave core
  - Crypto & ASIC prevent key tampering, cloning, cryptanalysis...
  - Low-security processes (encrypted key cache) in host µP
- Real-time key selection via ECM
  - Channel & program-level control



Specialists in Solving Complex Data Security Problems 12

Key derivation based on user privileges

- Addressing modes enable efficient rights key distribution
  - "Sub-rights" bitmaps enable efficient transmission of ERKs
    - ~2 bits/device
  - Other key attributes can be added
    - Expiration date, usage condition...

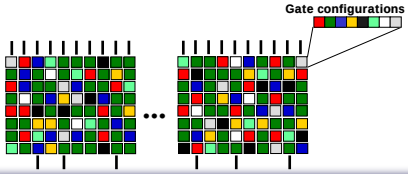


Sub-rights Bitmap

- Binding of user permissions to cryptographic processing
  - Derived keys are cryptographically bound to user permissions
    - Key attributes cannot be altered without changing derived key
    - Strong hardware enforcement
      (does not rely on software-controlled usage rules)

Key management: Hardware keys

- Automated netlist generation
  - Entropic array generator
    - Uses cryptographically-strong seed value
    - Leverages cell library features and layout constraints
    - Achieves strong anti-reverse engineering properties
    - Emulation infeasible even on workstation-class PC
  - Works with fab-provided library, design flow
    - Specialized / camouflage libraries supported (optional)
- Designed for open review



Resistance to fault injection

- Security boundary at edge of CF
  - CF has independent, enforced HW state machine
  - Where possible, external signals considered *malicious*
    - CF translates/releases reset signals, etc.
    - Manufacturing scan test circuitry not used
  - External glitch/environmental sensors recommended but not relied upon

Canaries used to detect CO gas in mines (Hollinger Mine, Ontario, 1928)

- Canary logic designed to fail first
  - Critical path logic performs continual hash of control state
  - Detects internal errors, provides independent control on system output

Cryptography Research

Specialists in Solving Complex Data Security Problems 15

High-assurance security

- High assurance design
  - Open review encouraged
    - Cryptographic design enables security reviews
    - 3P review without exposing system secrets
  - No single point of failure
    - Critical functions perform under independent dual controls
    - CryptoFirewall™ & CA system can each assume other is untrusted
  - Aggressive feature and state management
    - Minimize possibility of unintended functionality (design bugs)
    - Clean design eases integration
- Extreme validation (10x)
  - Custom CRI tools for extended system validation
    - Predict, model, and anticipate internal faults
  - Exceptional manufacturing test coverage (>99% w/o scan)

Cryptography Research

Specialists in Solving Complex Data Security Problems 16

Cryptography Research

Emphasis on tamper resistance

- Information leakage: SPA / DPA / Timing
- Glitching: Error handling and response
- Protocol attacks: Rigid command set
- Invasive attacks / Reverse engineering: Entropic netlist
- Emulation: Netlist design tools
- Software: µP assumed malicious

Contact CRI for more information.

Specialists in Solving Complex Data Security Problems 17

CryptoFirewall™ Typical Deployment

Specialists in Solving Complex Data Security Problems 18

Typical CryptoFirewall™ Customer

- Has a major piracy / fraud exposure
  - Sophisticated attackers
    - Risks of protocol, non-invasive, and/or invasive attacks
    - Revocation capability minimally effective
  - Hardware deployment/upgrade planned in >12 months: security is critical
  - CF purchased to extend life of new security hardware
- CRI manages CryptoFirewall™ deployment process
  - Provides everything needed (specs, netlists, tools, IP licenses…)
  - Helps CA vendor integrate with firmware & protocols
  - Supports semiconductor fab with netlist integration, testing
  - Provides security validation & support
- Deployment occurs with next-generation hardware
  - If swapout, migrate high-risk subs first
- Results: Successful deployments & zero security problems

Customer references available

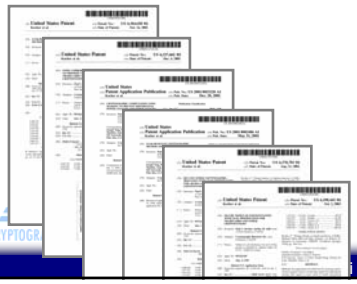
Specialists in Solving Complex Data Security Problems 19

Technology licensing

The CryptoFirewall™ architecture is protected under U.S. patents and international patents including:*

- 6,289,455 (“Method and apparatus for preventing piracy of digital content”)
- 6,640,305 (“Digital content protection method and apparatus”)
- 20040111631 (“Using smartcards or other cryptographic modules for enabling connected devices to access encrypted audio and visual content”)

A license under the CRI DPA/tamper resistance patent portfolio is also included



Selected Patents

- **Patent 6,278,783: “DES and Other Cryptographic Processes with Leak Minimization for Smartcards and Other Cryptosystems”**
- **Patent 6,298,442: “Secure Modular Exponentiation with Leak Minimization in Smartcards and Other Cryptosystems”**
- **Patent 6,304,658: “Leak Resistant Cryptographic Method and Apparatus”**
- **Patent 6,327,661: “Using Unpredictable Information to Minimize Leakage from Smartcards and other Cryptosystems”**
- **Patent 6,381,699: “Leak Resistant Cryptographic Method and Apparatus”**
- **Patent 6,510,518: “Balanced Cryptographic Computational Methods and Apparatus for Leak Minimization in Smartcards and other Cryptosystems”**
- **Patent 6,539,092: “Leak Resistant Cryptographic Indexed Key Update”**
- **Patent 6,654,884: “Hardware-Level Mitigation and DPA Countermeasures for Cryptographic Devices”**

DPA Cryptography Research DPA Countermeasure Licensing Program

* Additional U.S. and international patents issued + pending

ing Complex Data Security Problems 20

CryptoFirewall™ Summary

- Highest possible security with standard silicon processes
  - Enforcement of critical security policies
  - Comprehensive integrated countermeasures
  - Ensures security independently from the rest of the chip
- Design process minimizes deployment risk
  - Includes high level of security validation & manufacturing assurance
  - Robust, well-defined security boundary
  - Experienced team with proven record of on-time delivery
- Cost-effective way to dramatically increase hardware security lifespan
  - Extremely strong tamper hardware resistance
  - Customized for pay TV & other applications
- Proven solution

Specialists in Solving Complex Data Security Problems 21

For More Information

Licensing

Kit Rodgers
kit@cryptography.com
Tel: 415-957-2601

Technology and Services

Benjamin Jun
ben@cryptography.com
Tel: 415.397.0123

Specialists in Solving Complex Data Security Problems 22

Cryptography Research