Crypto Processor Design and Trusted Platform Module

Mohammad Tehranipoor

ECE 4095: Hardware Security & Trust
University of Connecticut
ECE Department

Overview

- Introduction to crypto processors
- Designs of crypto processors
- Performance analysis of cryptographic hardware
- Introduction to Trusted Platform Module
- Attacks on crypto processors and how to defend against them
- Investigate documented attack on crypto processor

What is a Crypto Processor?

- A specialized processor that executes cryptographic algorithms within hardware
- Definition varies, but the standard definition includes
  - Acceleration of encryption
  - Protection against tampering
  - Intrusion detection
  - Protection of data
  - Secure I/O

Why Crypto Processors?

- Most modern security work is based on either protecting or cracking vulnerabilities in target's OS
  - Majority of systems use conventional processors, standard OS, and standard communication channels
  - A lot of good work has been done here but may be seen as a dead-end for high security
  - Software isn't enough to protect system, need physical protection

Why Crypto Processors?

- Motivation for securing processors
  - Protection of IP
    - Algorithms, FPGA config files, etc.
  - Protection of key data where simple storage encryption isn't enough
  - Prevent exploits in vulnerabilities
    - In ATMs and other high risk applications
- Offer advantages in speed and power consumption
  - Increasing data rates and complexity in security protocols cause s/w implementations to be slow
  - Typically the same software crypto algorithms are implemented in hardware

History of Crypto Processors

- Military applications
  - Nuclear weapons arming, battlefield comms hardware, etc.
- Earliest civilian crypto processor was IBM 3848 (1980s)
  - Used for ATMs and mainframe computers
- Recently, been used in many consumer level goods and applications
  - Smart cards, GSM phone SIM cards, set-top TV boxes, etc.
  - Manufactures can exercise control over aftermarket accessories
    - Game controllers, car electronics, ink cartridges, etc.
- "Trusted Computing" initiative to incorporate "Trusted Platform Module" crypto processors into chips

Design

- Start from the ground up
- Start with secure silicon, meaning must trust your fab
  - No backdoors, no undocumented features, etc.
- Design and program in secure environment and limit access to design info
- Have a strong and reliable key management system

Design Considerations

- Need to consider level of security needed
  - Paranoia, IP protection, protection of sensitive data, protection of legally liable data or financial transactions
- Ground up design may not be practical
  - Expensive, time consuming, may need to conform to commercial communication standards, e.g. TCP/IP
- Ground up design is infeasible for many applications
  - Mobile devices make h/w security difficult/impossible
  - High complexity of modern systems make fully custom hardware impractical

Security Levels and Costs

- Exponential relationship describes security vs. cost
- Low end: vulnerable
  - Microcontrollers using 3DES, AES
  - Keyless entry and RFID devices

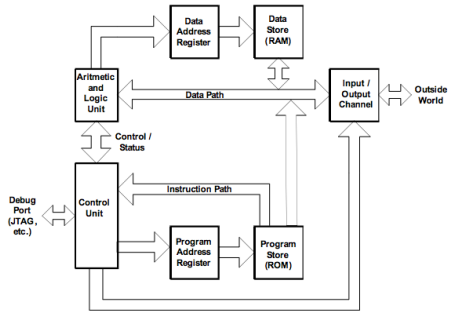
- Middle range: hardened security
  - Single-chip ASIC
  - USB tokens, smart cards, TPM

- High end: highest security
  - Multiple chips on protected PCB
  - Hardware Security Modules: ATMs, internet servers

Families of Crypto Processors

- Double encryption
  - Protects programs and data
- Standard processor architecture + dedicated crypto blocks
  - Increased throughput
- FPGA implementation
  - Flexible and allow efficient complex arithmetic operations
- ASIC implementation
  - Fast and low power consumption

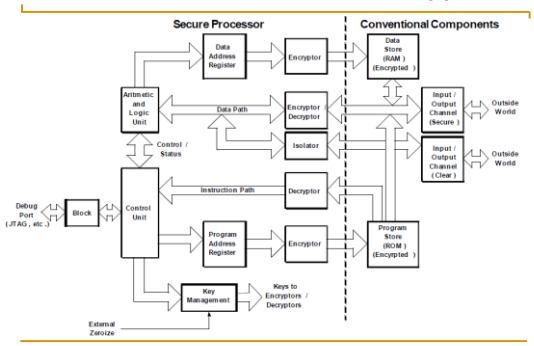
Conventional Harvard Processor



Double Encryption

- This type of crypto processor protects the programs running and the data
  - Data and addresses are encrypted
- All info is decrypted within the security of the processor and then encrypted again before memory storage or I/O transmission
  - A barrier of encryptors and decryptors stands between the the processing elements, data storage, and I/O elements.

Processor With Double Encryption



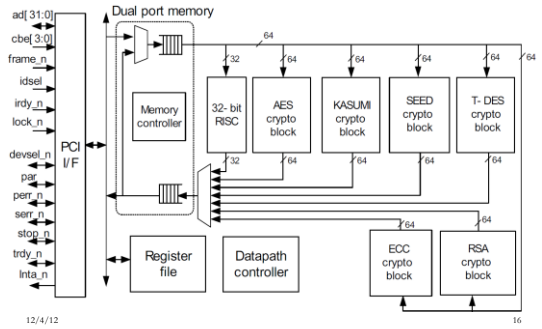
Double Encryption

- New Section for key management
  - Keys may be “hardwired” in (externally loadable)
  - Hardwiring in the keys generally allows them to be zeroized
  - Hardwired keys are generally not visible to the outside world under any (reasonable) conditions
- There is both a secure and a non-secure I/O channel
  - The strength of the security in the processor is directly dependent on how well these two channels are isolated
  - The easiest place to attack would be at this point of isolation
    - Results in data transactions being monitored “in the clear”

Processor With Dedicated Crypto Blocks

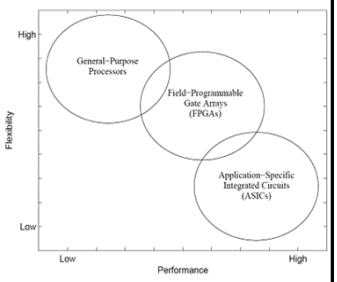
- Build upon standard processor architectures with the addition of multiple dedicated crypto algorithm blocks
  - Parallel connections to data bus
- Processor instructions are not secure
  - Handle large quantities of encrypted data, but do not need the instructions to be secure
- Ideal for network routers
  - Greatly increase throughput in network applications
  - Multiple cryptographic algorithms

Architecture of Dedicated Crypto Blocks



Performance

- Fast and efficient at the cost of flexibility
- Advantages seen with narrow or unusual bit widths
- Components not in standard processors
  - S-box look-up tables
  - Bitwise barrel shifters
  - Hardwired shifts



Crypto Processors implemented in FPGAs

- Used for speeding up cryptographic processing
- Flexibility allows for system evolution
  - Algorithm agility for security protocols
  - A must to become commercially viable
- Allow complex arithmetic operations that general CPUs cannot perform efficiently
- May be more cost-effective solution than VLSI/ASIC
  - Modifications can be made with ease

Performance of FPGA Crypto Processor

- Emphasized in literature
  - Less common in practice
- Significant improvements over standard processors
  - 500x speedup
  - 50% power reduction
- Strengths
  - Modular arithmetic, bit level manipulation
  - Uncommon length bit-vectors
- Point multiplication performance comparison
  - 66MHz FPGA: 0.36ms
  - 2.6GHz dual-Xeon: 197ms

Performance of Crypto Processor on ASIC

- Optimized ASIC compared to FPGA performance
  - 4x faster
  - 97% area reduction
  - 93% dynamic power reduction
  - May be unrealistic to see these gains
- High volume applications
  - Speed necessary applications
    - e.g. network routers
  - Low power applications
    - e.g. RFID devices

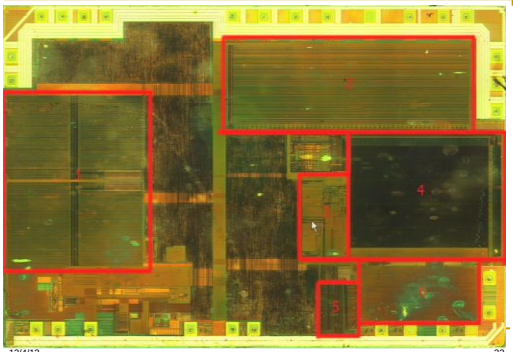
Trusted Platform Module

- TPM is a component on the CPU board that is specifically designed to enhance platform security
  - Crypto processor with a s/w microkernel
  - Securely generates and stores encryption keys, passwords, and digital certificates
- Idea is for one TPM to certify another TPM
  - Can certify both the program and the platform
  - Many different applications
    - e.g. for DRM: A TPM can assure a content vendor it is selling to a true copy of the media player rather than hacked copy

Trusted Platform Module

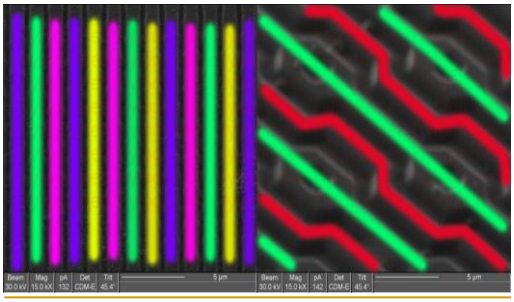
- Dependent on state of PC
- Services
  - Attestation: Cryptographic reporting of state
  - Sealing: State dependent access to information
- Used for
  - Encrypting and decrypting data
  - Control digital rights management (DRM) access
  - Authenticate users, applications, and computers
- ~250 million units, few applications actually use TPM
  - Customer resistance due to developers locking in more tightly and forcing incompatibility.
  - Due to complexity of managing chip
  - Due to the lack of awareness of its capabilities

Infineon TPM Die



FIB image of TPMs

Infineon TPM mesh STMicroelectronics TPM mesh



Attacks

- Early 90s, security was minimal in devices
  - Simple attacks could be performed, such as clock and voltage glitching and UV light
  - Few valuable applications and thus few serious attackers
- Soon enough, the need for security changed
  - Smart cards in pay-TV applications
  - Attackers forging cards or wanting to watch for free
  - Manufacturers introducing security chips for accessory vendors to pay a royalty. Strong incentive for vendors to reverse engineer security chips
- Triggered arms race between attack and defense

Attacks

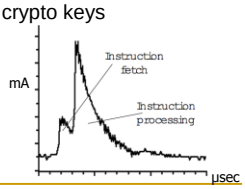
- Weaknesses are found in implementation
  - More vulnerable than the algorithm
- Analyze the *attack surface*
  - The set of physical, electrical, and logical interfaces that are exposed to potential attackers
- Four classes of attacks
  - Invasive
  - Non-invasive
  - Semi-invasive
  - Remote attacks

Invasive Attacks

- Involve direct electrical access to internal components of crypto processor
- Example: drilling into passivation layer and micro probing
- IBM 4758 interior has been exposed

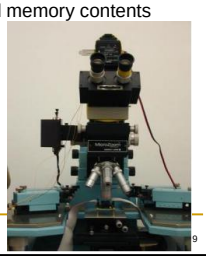
Non-invasive Attacks

- Observing or manipulating device's operation without breaking through packaging
- Examples:
  - Power analysis of processor and correlating to computations to deduce crypto keys
  - Glitching



Semi-invasive Attacks

- Involve access to the chip's surface but doesn't require electrical contact or penetration of passivation layer
- Examples:
  - UV light allows attacker to read memory contents
  - Fault injection attacks
  - Low cost probing workstation using photoflash
  - Light causes transistor to conduct. Then able to set or reset any bit in SRAM



Remote Attacks

- Not necessary to be near chip, just need to intercept encrypted traffic
- Two well known attacks but aren't specific to crypto processors:
  - Cryptanalysis and protocol analysis
- API analysis: specific to crypto processors
  - Top level s/w that governs its interactions with outside world
  - "an unexpected sequence of transactions which would trick a security module into revealing a secret in a manner contrary to the device's security policy"

Defenses

- Top of the line crypto processors must be tamper-resistant
  - Tamper sensors, UV protection, etc.
- Tamper/intrusion detection will result in
  - Crypto keys being zeroized
  - Memory erasure
  - Self-destruction of chip
- Top of the line crypto processor greatly diminishes threats from first three classes
  - Many remote attacks are independent of hardware quality
  - Security API designer must be very careful to not allow manipulations

Defense: Full-Size vs. Smart Cards

- Full-size: has many critical advantages
  - Glue logic
  - Large capacitors filter signals from external connections
  - Large enough for tamper-sensing barriers
  - Internal power supply allows constant monitoring
- Smart cards
  - Short in sensor mesh causes self-destruction
  - Unpowered most of time, chip doesn't know it's being tampered with
  - Glue logic

Top metal sensor mesh

Attack on IBM 4758

- Rated at highest level of tamper-resistance
  - Certified at FIPS level 4, highest available level
  - Requires two security officials to update keys
- Remote attack
  - Weakness in security protocols
  - A single official was able to learn all the keys
    - Took advantage of key handling routines to generate a key exporter
  - Only needed
    - 20 minutes with device
    - Standard $995 FPGA
    - About 1 day of cracking time

Questions?

References

- Broesch, James D. "Secure Processors for Embedded Applications." black hat. 2-28-2007. black hat, Web. 14 Feb 2010. http://www.blackhat.com/presentations/bh-dc-07/Broesch/Presentation/bh-dc-07-Broesch-ppt.pdf
- Anderson, R.; Bond, M.; Clulow, J.; Skorobogatov, S.; , "Cryptographic Processors-A Survey," Proceedings of the IEEE , vol.94, no.2, pp.357-369, Feb. 2006
- Kim, HoWon, and Sunggu Lee. "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System." IEEE Transactions on Consumer Electronics. 50.1 (2004): 214-224. Print
- Clayton, Richard. "Extracting a 3DES key from an IBM 4758." 2 Feb 2002. Computer Laboratory, University of Cambridge, Web. 1 Mar 2010. <http://www.cl.cam.ac.uk/~rnc1/descrack/>
- Wiens, Jordan. "A Tipping Point For TPM?." Informationweek. 1193 (2008): 39-41. Print.
- Montgomery, David, and Ali Akoglu. "Cryptographic Instruction Set Processor Design." bildiriler kitabi proceedings. (2007): 139-144. Print.