SENSS: Security Enhancement to Symmetric Shared Memory Multiprocessors

Youtao Zhang[§], Lan Gao[*], Jun Yang[*], Xiangyu Zhang[¶], Rajiv Gupta[¶]
[§]University of Texas at Dallas
[*]University of California, Riverside
[¶]University of Arizona

Why Secure Processors?

- Potential Impact
  - Digital Rights Management
  - Virus Protection
  - Mobile Agent Applications
  - Grid Computing
- Trusted Computing Group (TCG)
  - IBM ESS
  - Microsoft NGSCB
  - Intel LT
  - ...

Outline

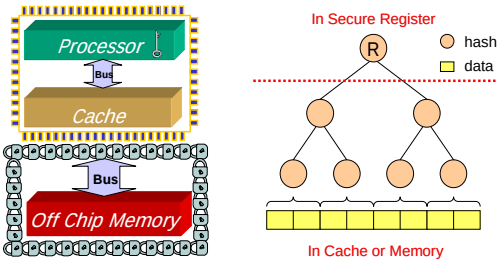
- Background & Motivation
- SENSS Design
- SHU Design
- Integrated System
- Experimental Evaluation
- Summary

Outline

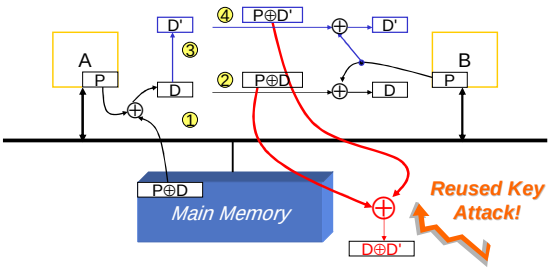
- Background & Motivation
  - Secure Uniprocessor Model
  - Vulnerabilities in SMP
  - Potential attacks on the bus
- SENSS Design
- SHU Design
- Integrated System
- Experimental Evaluation
- Summary

Secure Uniprocessor Model

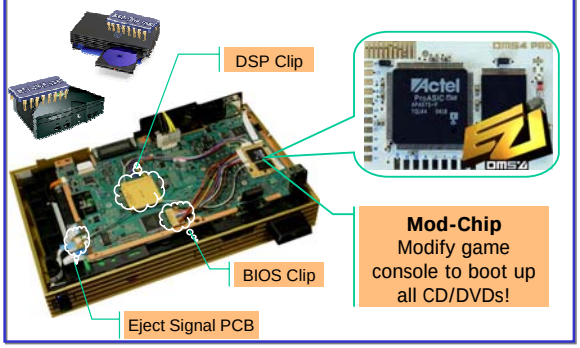
- Confidentiality
- Integrity



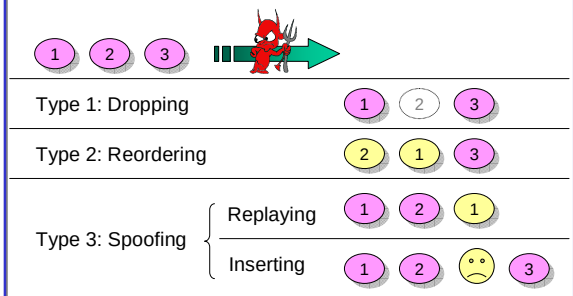
Why Not the Uniprocessor Scheme?



Why Need Bus Protection?



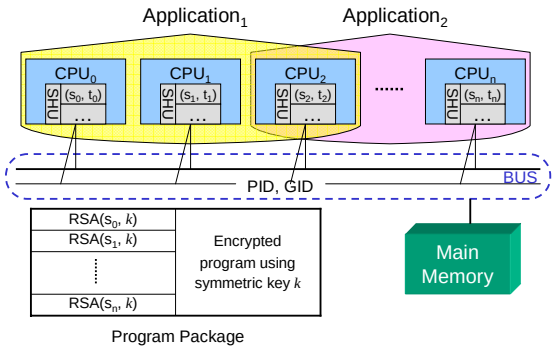
Potential Attacks on the Bus



Outline

- Motivation
- SENSS Design
  - Encryption Scheme
  - Authentication Scheme
  - Defense against Potential Attacks
- SHU Design
- Integrated System
- Experimental Evaluation
- Summary

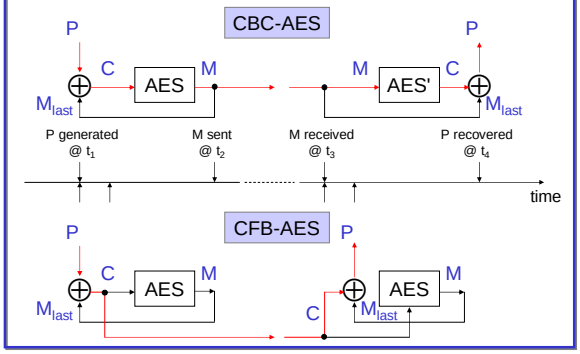
SENSS Overview



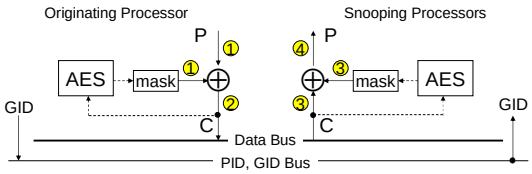
Secure Cache-to-Cache Transfers

- Goal:
  - Security: Confidentiality & Integrity
  - Efficiency
- Algorithm Selection:
  - Block Cipher
    - Provide high security level
    - Capable of data authentication in certain modes of operation
  - Stream Cipher
    - Overlap pad generation with bus transfer

Comparison of Two Block Cipher Modes

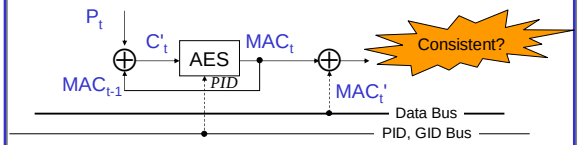


Bus Encryption Scheme



- Crypto Operations (in solid lines)
  - C is transferred instead of mask
  - One XOR operation in the critical path
- Mask Update (in dashed lines)
  - Generated by AES unit with the preceding C
  - Done in parallel with bus transfer

Bus Authentication Scheme

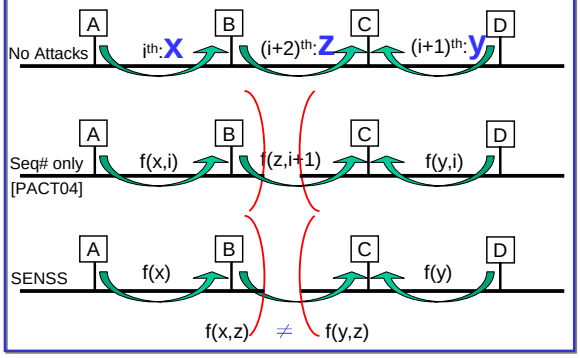


- MAC:
  - MAC_t authenticates the whole sequence of transfers up to time t
  - Check the consistency of MACs periodically to detect attacks
- Initial Vector:
  - Different from IV in the encryption scheme so that $C'_t \neq C_t$
- PID
  - Used for origin authentication

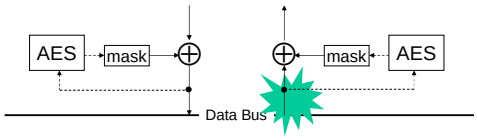
Outline

- Motivation
- SENSS Design
  - Defense against Potential Attacks
    - Message Dropping
    - Message Reordering
    - Message Spoofing
- SHU Design
- Integrated System
- Experimental Evaluation
- Summary

Dropping Attacks and Defense

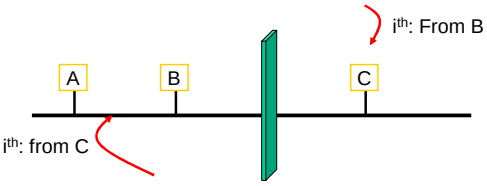


Reordering Attacks and Defense



	Sender	Receiver
i^{th}:x	x / f(x)	y / f(y)
$(i+1)^{th}$:y	y / f(y)	x / f(x)
$(i+2)^{th}$:z	z / f(z)	z / f(z)

Spoofing Attacks and Defense

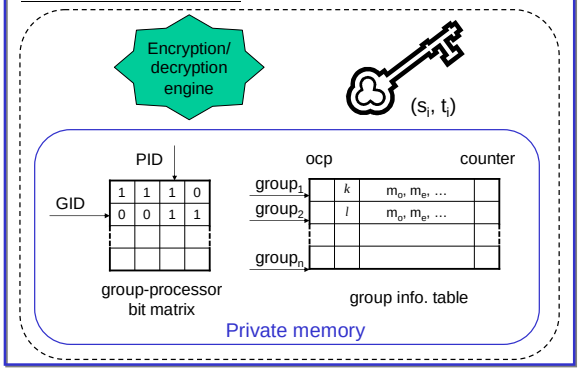


	A&B	C
MAC w/o PID	f(i)	f(i)
MAC w/ PID	f(i, C)	f(i, B)

Outline

- Motivation
- SENSS Design
- SHU Design
  - SHU Architecture
  - Hardware Overhead
- Integrated System
- Experimental Evaluation
- Summary

SHU Architecture



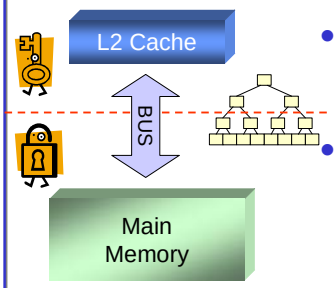
Hardware Overhead

- Table Size for 1024 groups:
  - group-processor bit matrix: 4KB
  - group information table: 148.6KB
- Bus Design
  - 3 additional message type
  - 12 extra bus lines
- Encryption Unit
  - latency: 22cycles@266Mhz v.s. 80cycles@1Ghz
  - throughput: 30-70Gb/s v.s. 3.2GB/s

Outline

- Motivation
- SENSS Design
- SHU Design
- Integrated System
  - Memory Encryption
  - Memory Integrity Check
- Experimental Evaluation
- Summary

Integrating with Cache-to-Memory Protection



- Memory Encryption
  - Each processor performs fast memory encryption on its own
  - Pad consistency
- Memory Integrity Check
  - Each processor maintains its local part of the hash tree
  - Node consistency

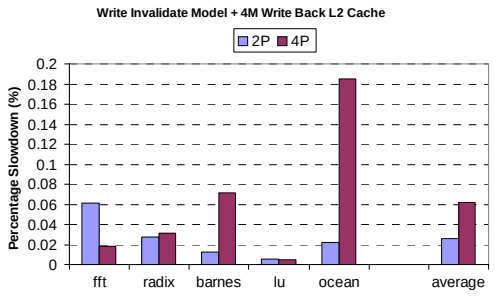
Outline

- Motivation
- SENSS Design
- SHU Design
- Integrated System
- Experimental Evaluation
- Summary

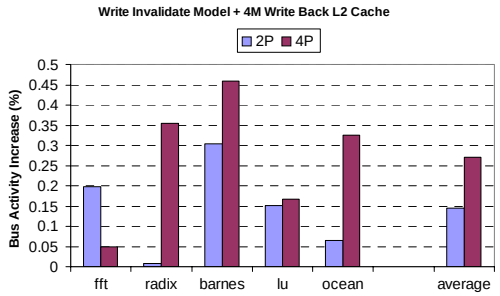
Experiment Environment

- Tools
  - Simics full-system multiprocessor simulator
  - 5 benchmarks from SPLASH2 suite
- Configuration
  - Machine: 1Ghz, SPARC V9, Solaris 9
  - Cache
    - Separate L1 I- and D-cache: write-through, 64K, 32B line
    - Integrated L2 Cache: write-back, 1M/4M, 64B line
    - MESI Coherence Protocol
  - Latency
    - cache-to-cache: 120 cycles; cache-to-memory: 180 cycles
    - AES: 80 cycles

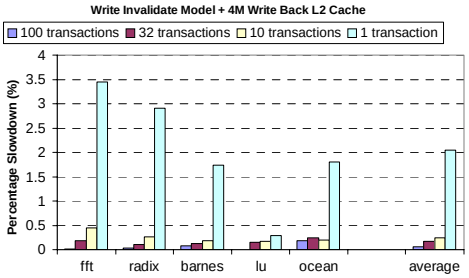
Performance Slowdown



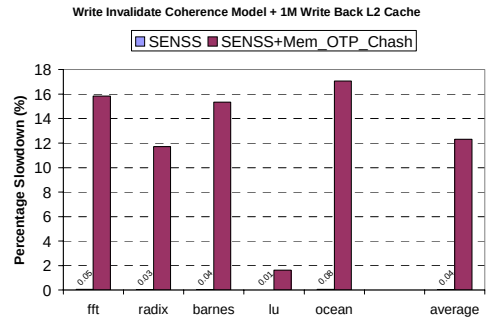
Bus Traffic Increase



Varying Authentication Interval



Integrated System



Conclusion

- Develop a fast and secure computation model for SMPs
- Secure cache-to-cache transfers:
  - Bus encryption and authentication scheme
  - Hardware implementation
- Preliminary experiments:
  - Slight performance degradation
  - Modest hardware overhead