

Arc3D: A 3D Obfuscation Architecture

M. Gomathisankaran & A. Tyagi

18-Nov-2005

Outline

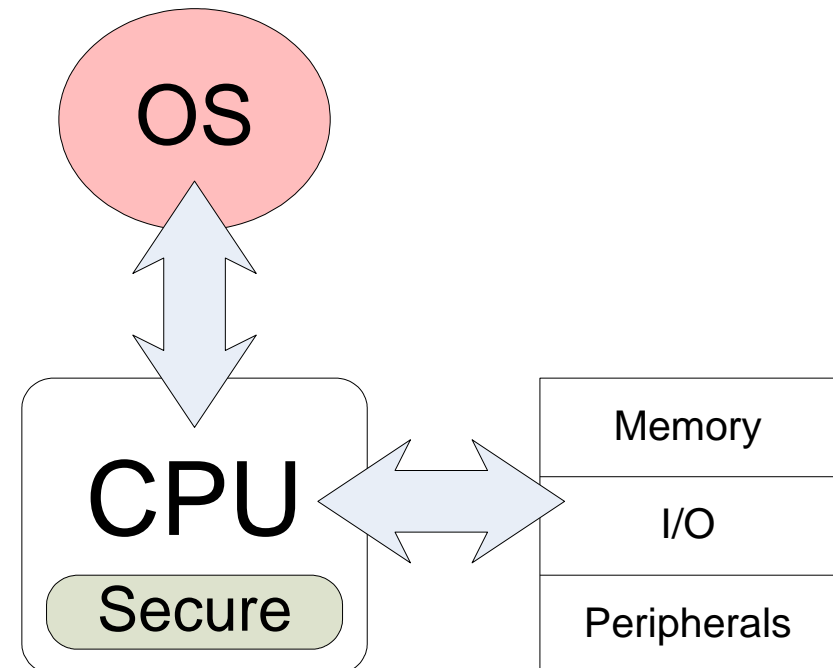
Arc3D

- Introduction
- Related Work
- Obfuscation Schema
- Permutation Unit
- Architecture
- Conclusion

Introduction

Arc3D

- Model
 - Protect application from OS
 - Powerful adversary model
- Applications
 - DRM Systems
 - Grid Computing



Related Work

- ABYSS
- XOM
- AEGIS
- HIDE

Motivation

Arc3D

- Efficiency
 - Encryption/Decryption is a heavy hammer
 - 80 cycles to do 64 bytes encryption in AES-CBC mode assuming 2 cyc/round
 - Smaller CPU's have more than 70% overhead
 - Not applicable to generic architectures
 - Requires L2 to be on-chip
 - Energy considerations
- Alternate architecture
 - Uses the basic characteristics of program to make it tamper resistant

Goals

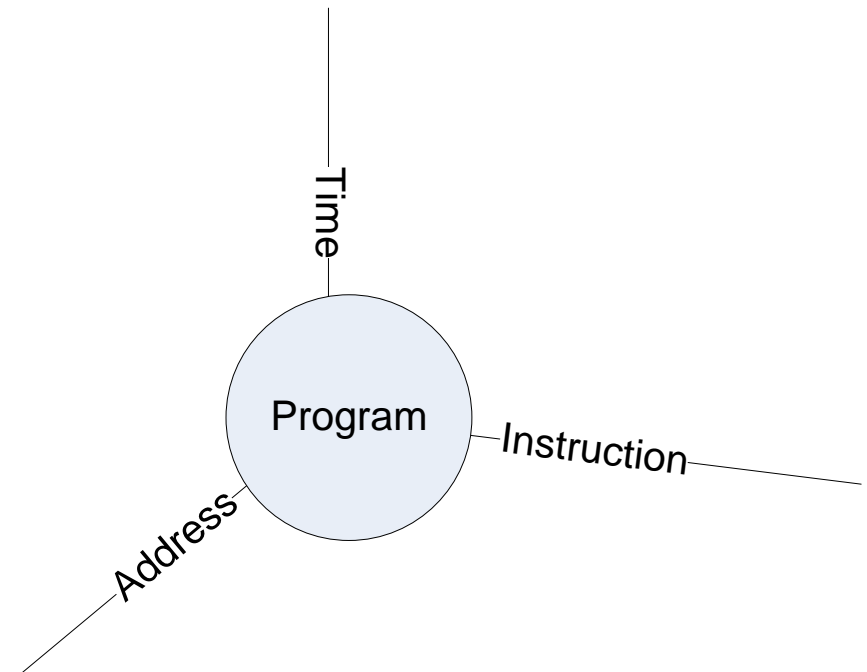
Arc3D

- Copy protection
- IP Protection
- Tamper resistance
- Efficient
 - Energy
 - Performance

3D of Information

Arc3D

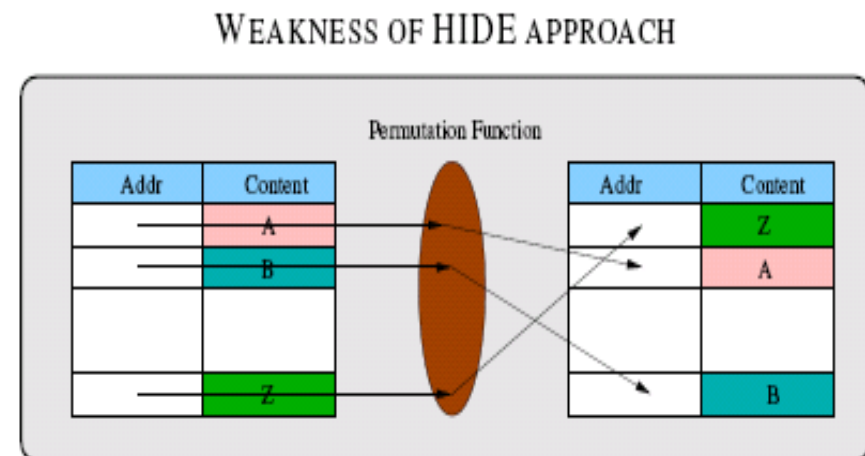
- *What, When* and *Where*
 - Static image contains only two dimensions of information
 - Traditional architectures preserve the correlation of *static image* and *process image*



Observations

Arc3D

- Address trace can reveal Control Flow Graph (HIDE – ASPLOS 2004)
 - CFGs are almost unique
 - 70% industry software is reuse code
 - 39% code at binary level is due to libraries
 - Malicious OS can manipulate cache to expose all memory accesses
- Weakness in HIDE approach



Obfuscation Schema

Arc3D

- Obfuscating 3D of Information
 - Sequence – Permutation
 - Content – OTP
 - Time – Protected L2 Cache
 - Two levels of obfuscation to remove *static image* and *process image* correlation

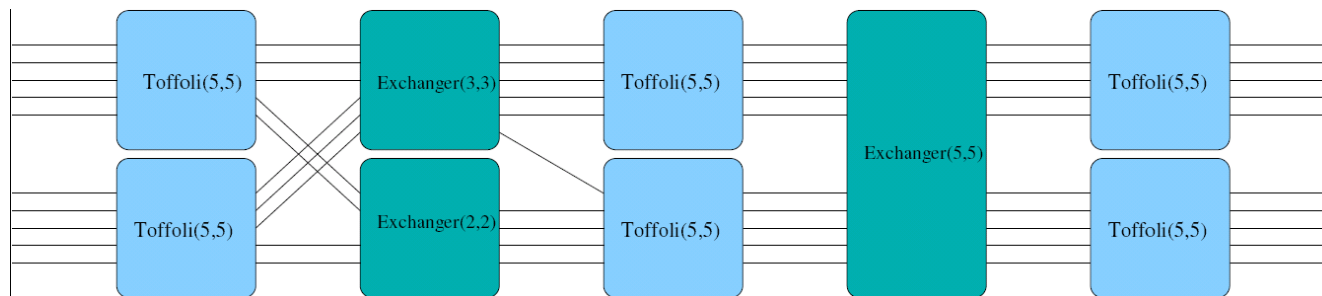
Sequence Obfuscation

Arc3D

- Permute the sequence of contents
- Boundaries
 - *Cache block* by architecture
 - *Page* by OS
- Permutation function considerations
 - $N (\log N)$ bits to represent permutation of N values
 - Should be able to support multiple permutations
 - Reconfigurable logic comes in handy

Reconfigurable Permutation Unit Arc3D

- $\binom{2^n}{n}$ possible functions implemented by $n*n$ LUT
 - Only $2^n!$ of them are bijective
 - Random configurations will not satisfy the criteria
 - Subset of these bijective functions need to be chosen
 - Use reversible gates to build this subset



Reconfigurable Logic Issues

Arc3D

■ Configuration

- For a support set of 5 variables and control sets of size greater than 1 we get 55^6 configurations
- Redundancy
 - Estimated to be 0.3% with 99% probability
- Store these configurations in LUT itself – similar to DPGA of DeHon
 - In addition to input bits LUTs will get configuration selection bits as well
 - 39 bits of configuration selection in total

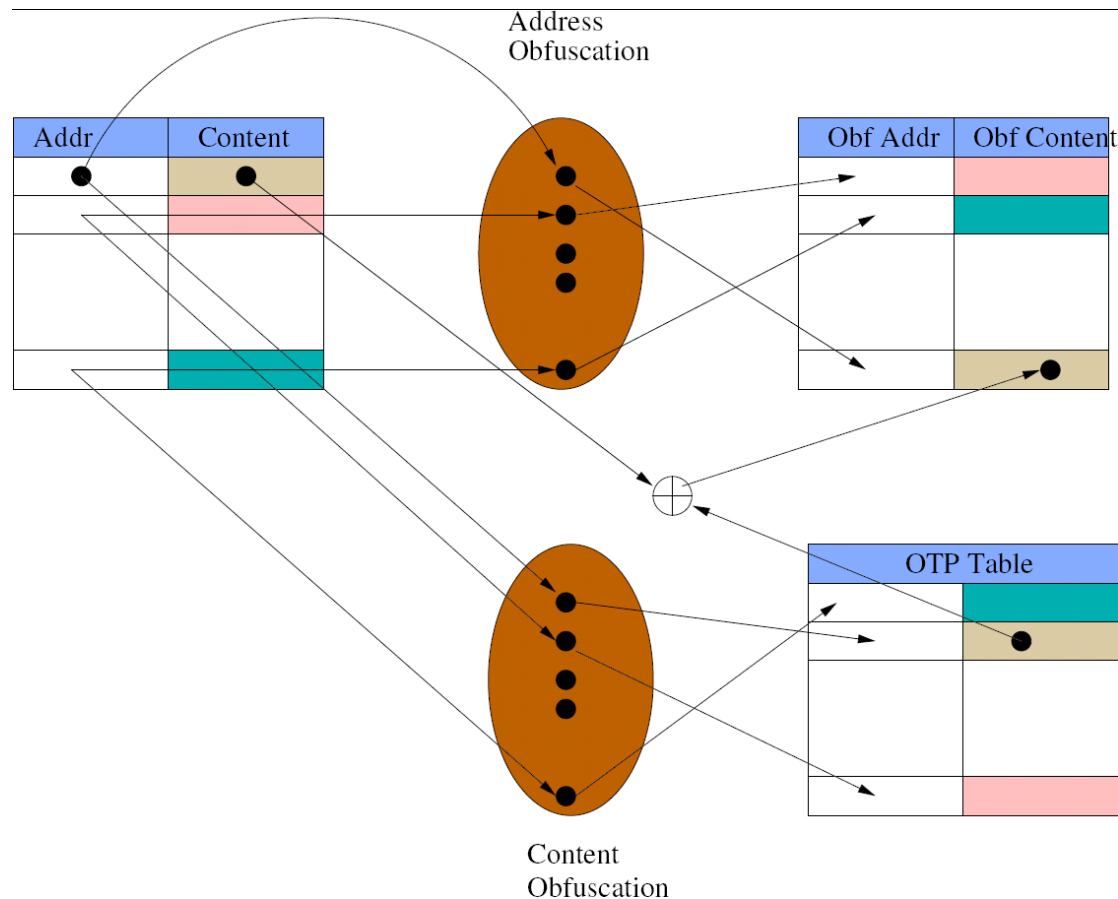
Obfuscating Contents

Arc3D

- OTP is theoretically unbreakable method of encryption
 - Contents can be considered as message of *cache block* size
 - But has to be unique per message hence highly inefficient
 - To overcome weakness of HIDE approach uniqueness has to be guaranteed within a *page*
 - Pre-generate OTPs for all the cache blocks in a *page*
 - Association of OTP with a cache block is randomized with permutation function

Static Obfuscation

Arc3D



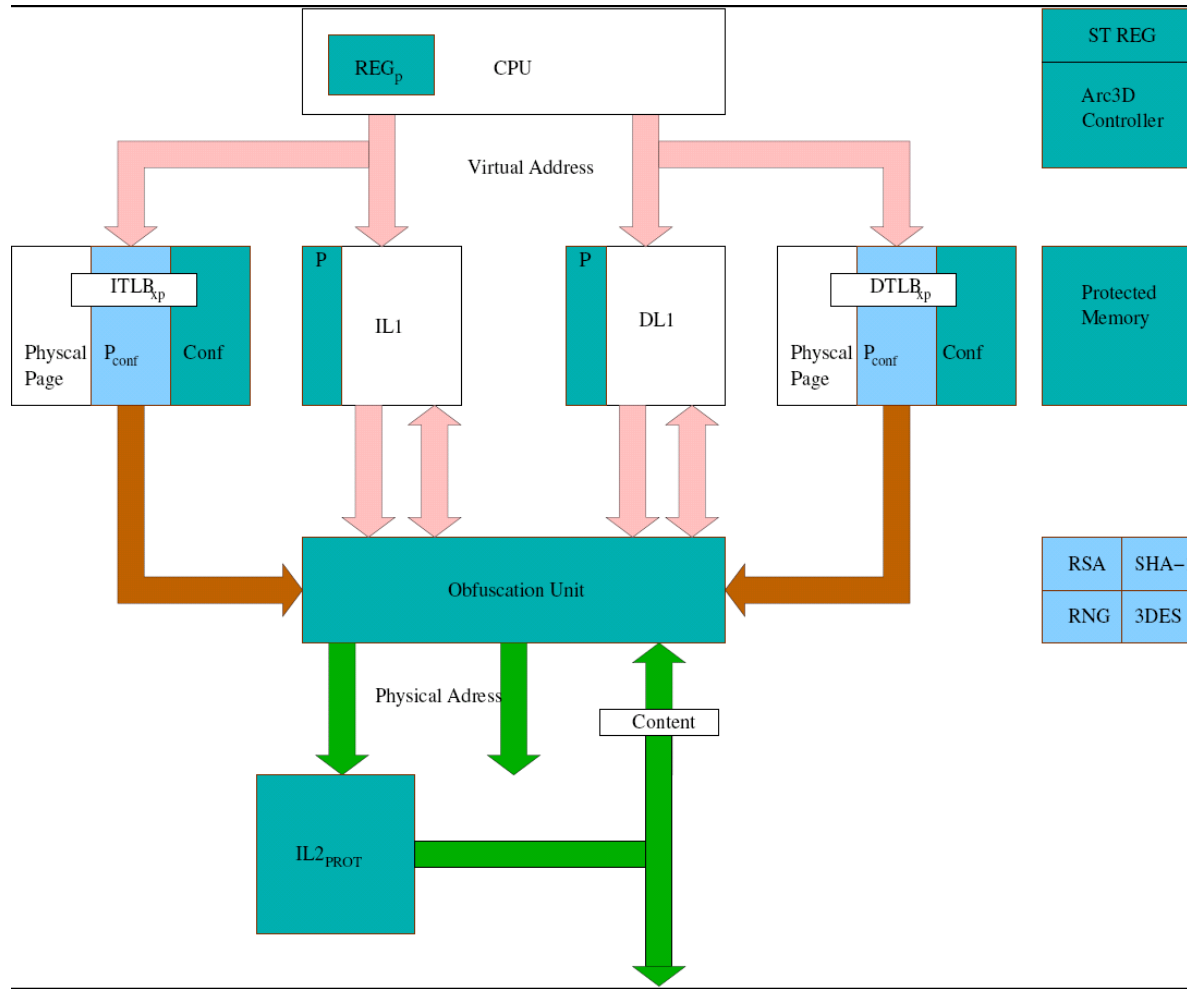
Dynamic Obfuscation

Arc3D

- Similar to static obfuscation
 - Generate OTP's when page is brought in
 - Obfuscate the page and load it in memory
 - Removes the correlation between static image and process image
 - Makes address trace unique per run
 - Prevents attacks based on interrupts

Architecture

Arc3D



Architecture

Arc3D

- Protects *initial state, context on interrupts* and *on-chip cache contents*
- Tamper resistant for off-chip memory hierarchy
- Only one active protected context
- Easy context switch between protected to unprotected process

Usage

Arc3D

Generation: $I \Rightarrow I_{obf} + E_K\{conf, OTP\}$

Distribution: $I_{obf} + E_K\{conf, OTP\} + E_P^+\{K\}$

Execution: $start \leftarrow I_{obf} + E_K\{conf, OTP\} + E_P^+\{K\}$
exit

Interrupt: $save \rightarrow E_K\{REG_P, conf, OTP\}$

restore

return

MemoryAccess: $store$

$load$

Attacks

Arc3D

- Replay attack
 - Replay attack on Process Context is prevented by associating a state register
- Spoofing and Splicing attack
 - Arc3D is tamper-resistant
 - Every cache block in every page potentially has a unique OTP
 - Modifying a value advantageously for an adversary is highly impossible

Performance Analysis

Arc3D

- Factors
 - Increased TLB latency – 2 cycles
 - L2 accesses on block boundary
 - Obfuscation of pages on every TLB miss
- Alpha-21264
 - Less than 1% performance degradation
 - Due to large TLBs - 128
- XSCALE
 - Very high impact – worst case 500%
 - Due to lesser number of TLBs

Thank You

Questions to
{gmdev,tyagi}@iastate.edu