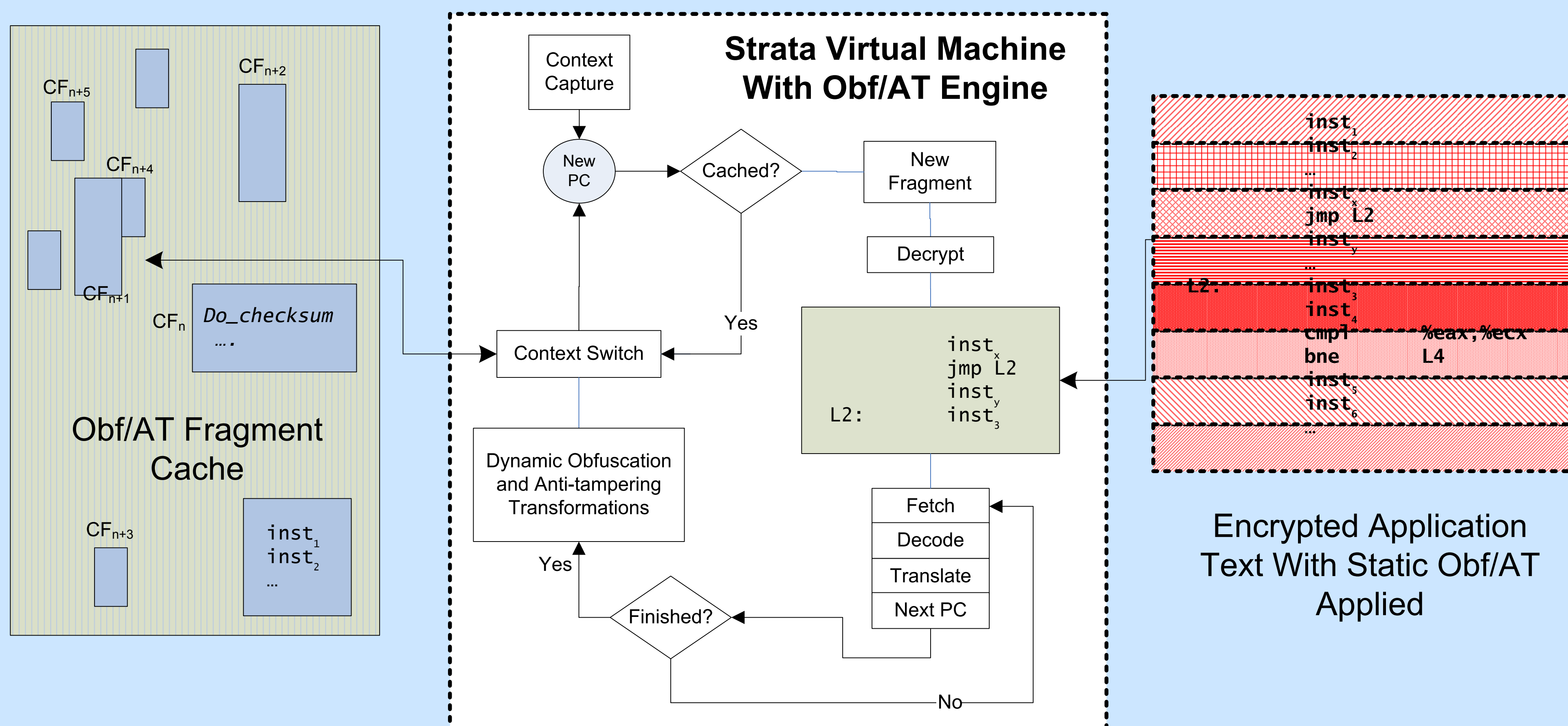


# Robust and Efficient Tamper-Resistant Software

Jason Hiser and Jack Davidson  
University of Virginia

## Protection Model

Software dynamic translator (SDT) performs “just in time” code block decryption, then obfuscation (Obf) and anti-tampering (AT) transforms are applied. Self-checksumming guards in both the SDT and encrypted code prevent tampering via “circular trust.”



## Approach and Impact

### New Approach

- Code is statically encrypted
- Continuous Obf/AT at runtime
- Periodic code cache flushes

### Research Impact

- Static analysis impossible
- Control dynamic info. leakage
- Practical, low-overhead, deployable solution

## Key Benefits

- “Real world” threat model – adversary may modify hardware, OS, other software, or use debugger/simulator/emulator to help trace the program
- Wide applicability – useful for DRM, IP, and other security applications

## Preliminary Results

- Hides 90% of application’s code with only 5% slowdown
- Naïve guards verify each instruction is unmodified 222 times (Ave. SPEC CPU2000)
  - High protection
  - High overhead
    - Use profiling to find better ways to reduce overhead while maintaining protection