



**Calhoun: The NPS Institutional Archive**  
**DSpace Repository**

---

NPS Scholarship

Publications

---

2018-04

## Reverse Engineering in Reverse

Thompson, Michael

Monterey, California. Naval Postgraduate School

---

<https://hdl.handle.net/10945/60500>

---

This publication is a work of the U.S. Government as defined in Title 17, United States Code, Section 101. Copyright protection is not available for this work in the United States.

*Downloaded from NPS Archive: Calhoun*



<http://www.nps.edu/library>

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

**Dudley Knox Library / Naval Postgraduate School**  
**411 Dyer Road / 1 University Circle**  
**Monterey, California USA 93943**

## Run Computers Backwards to Analyze Vulnerabilities

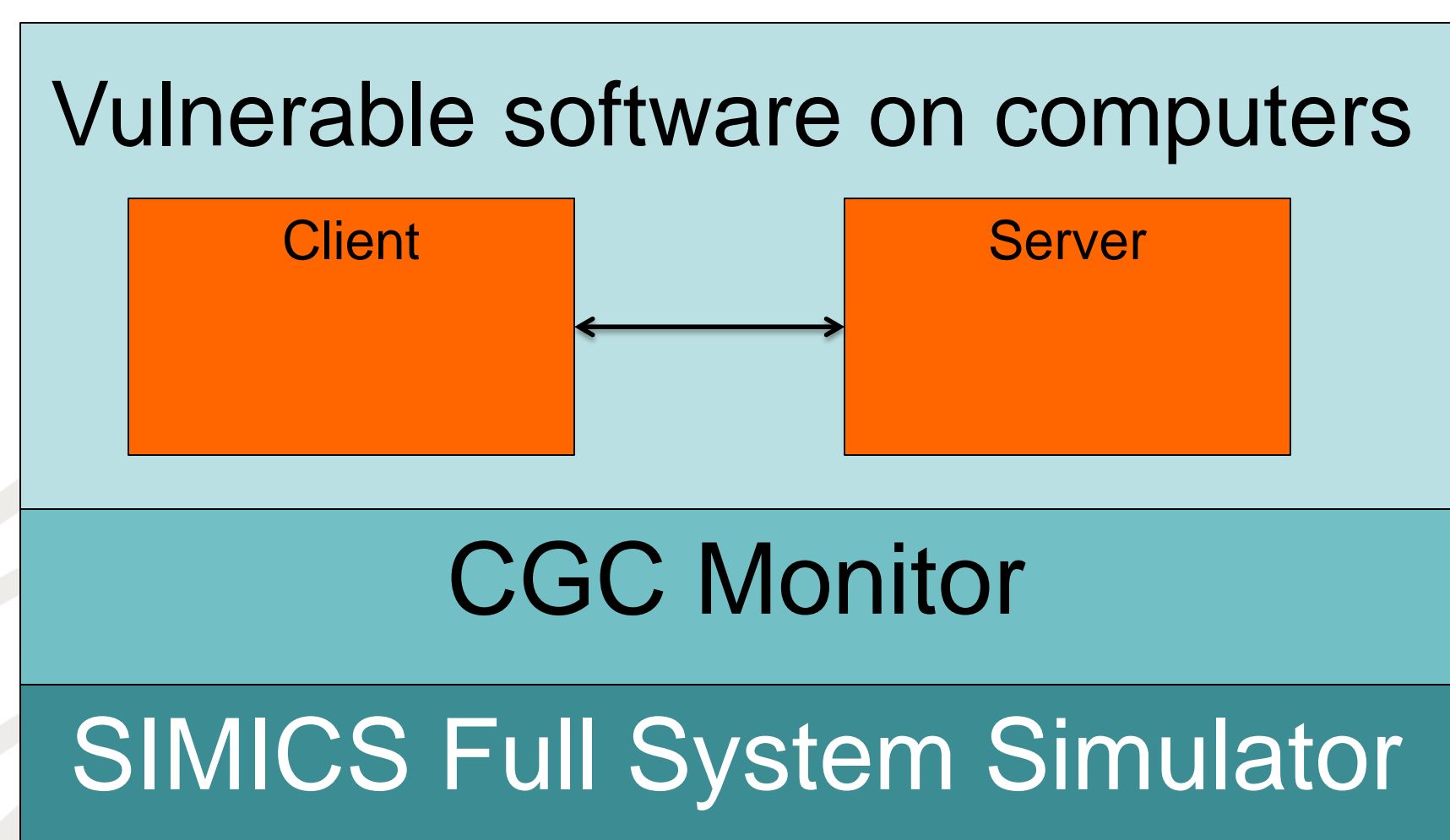


- The CGC Monitor automated analysis of the DARPA Cyber Grand Challenge
- Built on SIMICS full system simulator
- DoD has hundreds of unused licenses for the CGC monitor

- **Automated systems may find flaws to exploit, but not bugs to fix**
  - Example: CGC contestants primarily used generic defenses
  - Specific program flaws were found & exploited, but not patched
  - Finding/exploiting flaws was decoupled from defense
- **CGC Monitor (semi) automates identification of the bug**
  - Given a “Proof of Vulnerability” (PoV), help identify the actual flaw
  - Reverse execution to code and data breakpoints
  - Reverse to invocation of function
  - Back-trace sources of data

IDA Pro Debugger  
Client

- IDA Pro disassembler / debugger
- Python plugin for reversing



- Full system emulation of multi-component topologies
- Heterogeneous operating systems
- Reverse execution

- Developed as part of the CGC game infrastructure integrity protection effort
- Vetted all competitor software submissions (patched services & PoVs)
- Analyzed all successful CGC exploits
  - Found that half of the exploits were not as intended by authors of deliberately vulnerable software
  - Unintended flaws in custom developed services



Initial work sponsored by DARPA

Department of Computer Science

Michael Thompson [mftthomps@nps.edu](mailto:mftthomps@nps.edu)

<https://github.com/mftthomps/cgc-monitor>