



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

---

Faculty and Researchers

Faculty and Researchers' Publications

---

2022

# High-Fidelity Virtual Machine Artifact Mitigation

Singh, Gurminder

Monterey, California: Naval Postgraduate School

---

<https://hdl.handle.net/10945/71792>

---

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*



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**

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

## Goals

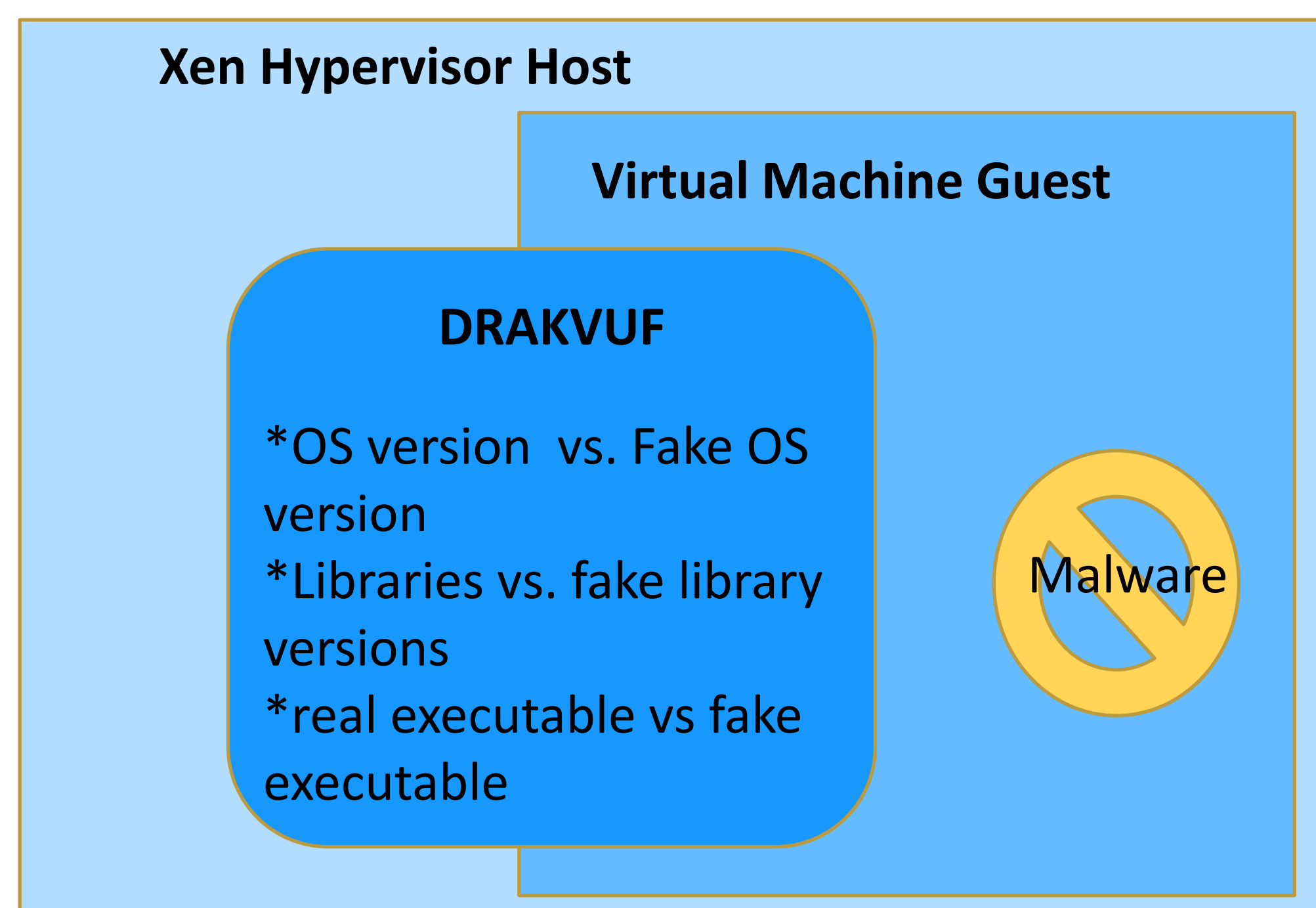
- Protection of Cloud infrastructure
- Resilience of Cloud infrastructure
- Protection from external attackers and internal attackers
- Expose attacker
- Analyze attacker methods

## Malware Trends

- Intelligent, analyzes surroundings
- Based on findings, attacks using a series of vectors dependent on surroundings
- If it detects that it is being analyzed, it hides and continues to spread
- Partially automated
- Becoming more important

## Methods

- Protection through obfuscation
- Protection by virtual machine introspection
- Protection at the system call kernel level

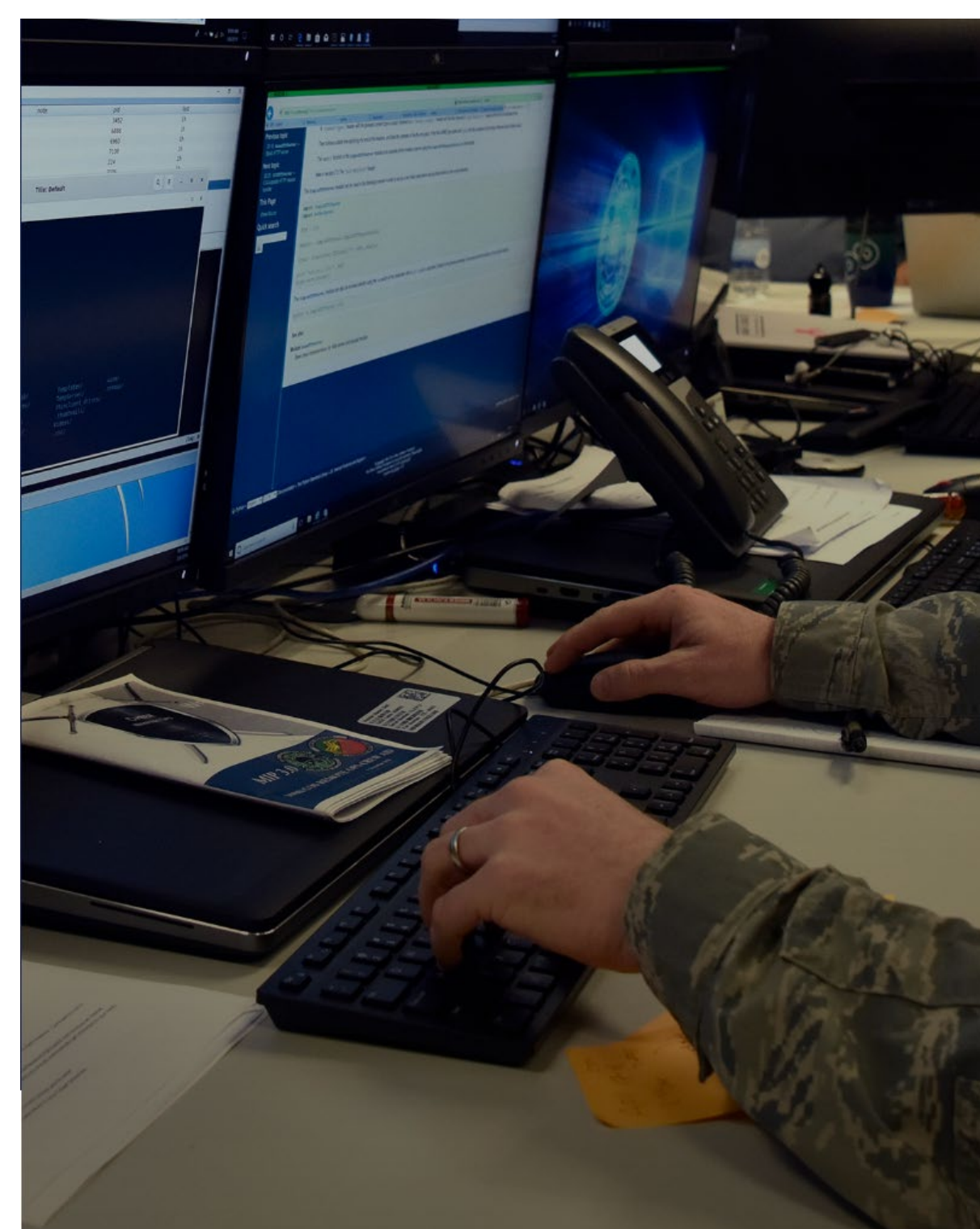


*Malware is confused into exposing itself*

## Persistent Cyber Training Environment (PCTE)

### Helps with PCTE

- Training of Malware detection and analysis
- Help with offense cyber operation munitions
- Training of low-level detection of malware
- Creation of better decision trees
- Creation of better Techniques, Tactics, and Practices



**Researchers:** Dr. Gurminder Singh, Computer Science Dept., Dr. Allan Shaffer, Information Science Dept., and Charles Prince, Computer Science Dept.

**Topic Sponsor:** Marine Corps Forces Cyberspace Command (MARFORCYBER)

NRP Project ID:  
NPS-21-M006-A

