N-Variant Systems

John Knight, Jack Davidson, David Evans, Anh Nguyen-Tuong

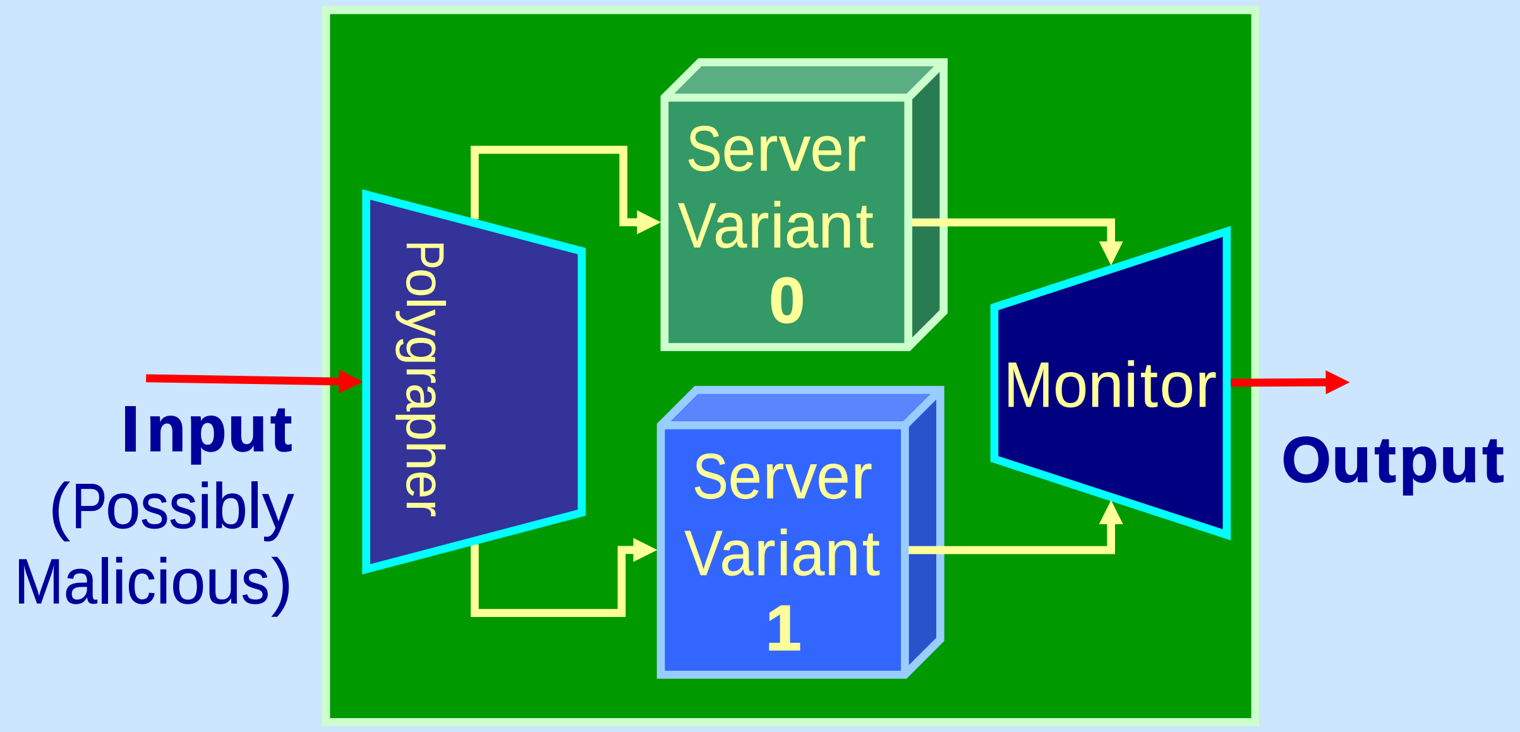
University of Virginia Computer Science   **http://www.cs.virginia.edu/nvariant**

N-Variant Systems provide a general mechanism for detecting and preventing classes of attacks on vulnerable software.

N-Variant Systems use artificial diversity techniques to provide provable resilience against classes of attacks **without needing secrets**.

The variant processes all implement the same service but are constructed so as to provably detect attacks. The system runs the variants in parallel, giving each variant identical inputs and monitoring that they behave similarly before allowing external effects.

Attackers must now compromise all variants **simultaneously** to carry out a successful attack. Our goal is to set up variants such that a given class of attacks is **provably impossible** since any input that can compromise one variant will produce a detectable alarm in another variant.



Input (Possibly Malicious)

Polygrapher

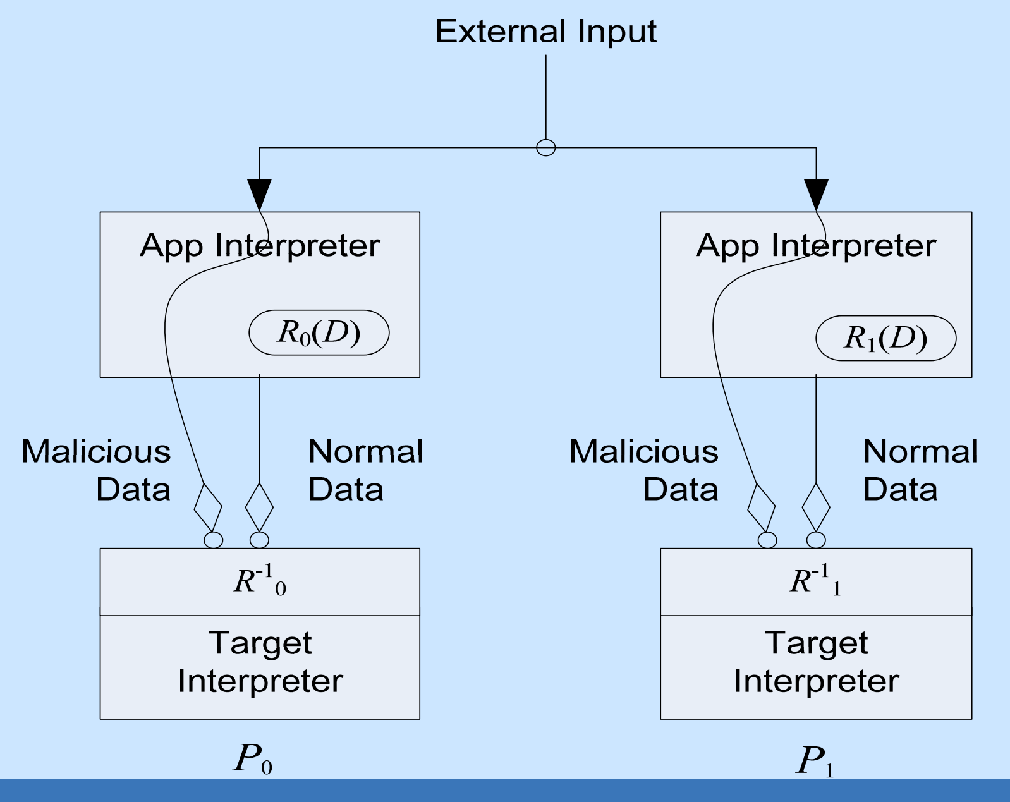
Server Variant **0**

Server Variant **1**

Monitor

Output

Generic 2-Variant System



Data Diversity 2-Variant System

New approach

No secrets required: protection provided even if attacker knows all details about the system and variants.

Structured diversity: variants constructed to vary some property on which attacks rely.

Impact

Allows *low-entropy* diversity techniques and *higher-level* variations.

Enables formal proofs of resilience against attack classes.

Example Variations

Address Partitioning: variants have disjoint address spaces so that addresses that are valid in one variant are guaranteed to be invalid in others

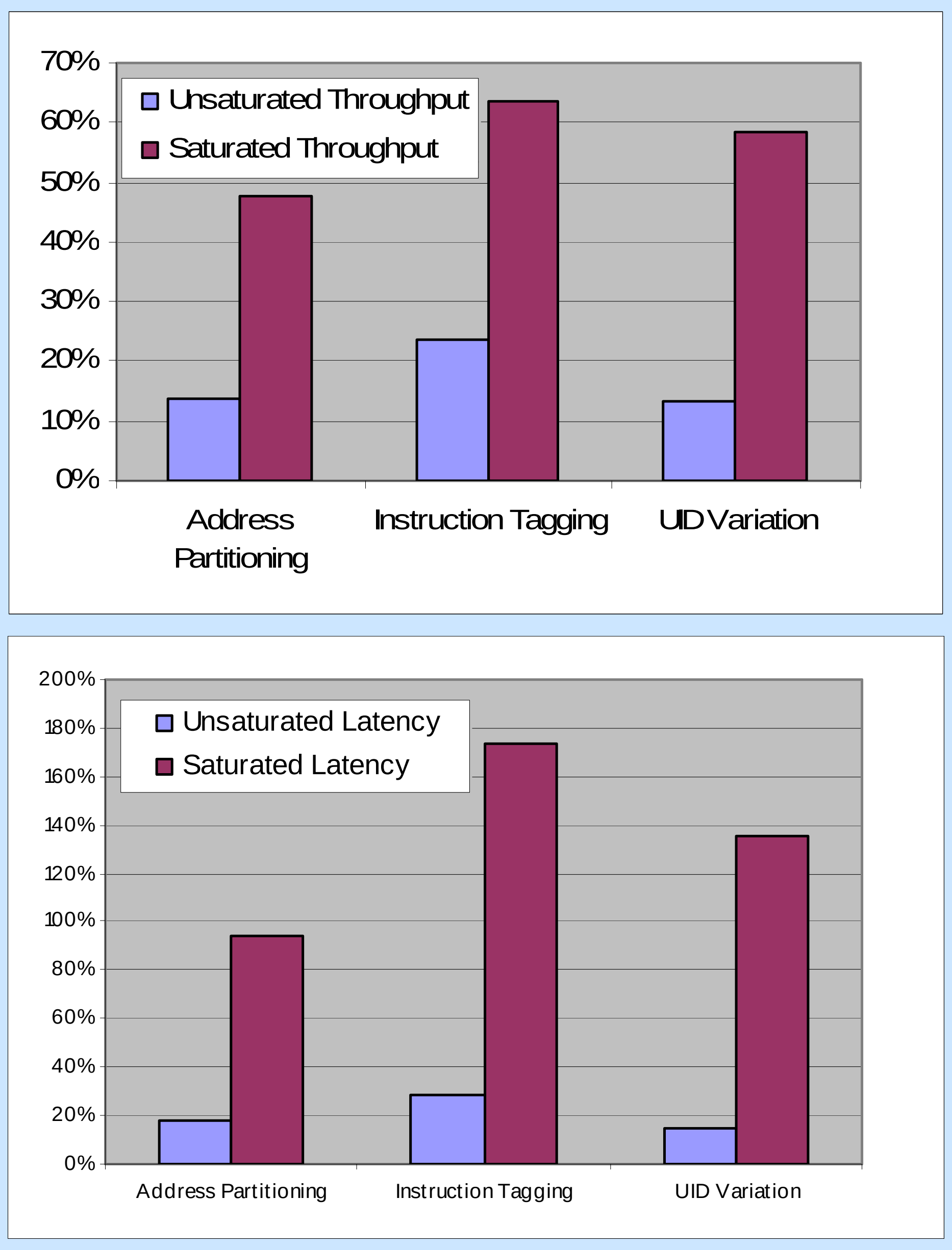
- *Thwarts attacks that rely on absolute addresses*

Instruction Tagging: variants have disjoint instruction sets so instructions for one variant are invalid in others

- *Thwarts code-injection attacks*

Data Diversity—UID Variation: user ids are unchanged for one variant, whereas for the other they are obtained by id' = uid ⊕ 0x7FFFFFFF. In general, data diversification requires semantic changes to application code.

- *Thwarts data corruption attacks, e.g. UID*



Apache Web Server Overhead

Papers

N-Variant Systems: A Secretless Framework for Security through Diversity. Benjamin Cox, David Evans, Adrian Filipi, Jonathan Rowanhill, Wei Hu, Jack Davidson, John Knight, Anh Nguyen-Tuong, and Jason Hiser. *15th USENIX Security Symposium*, Aug. 2006.

Security through Redundant Data Diversity. Anh Nguyen-Tuong, David Evans, John Knight, Benjamin Cox, and Jack Davidson. *38th IEEE/IFIP Conference on Dependable Systems and Networks*, June 2008.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

Computer Science
***at the* University *of* Virginia**