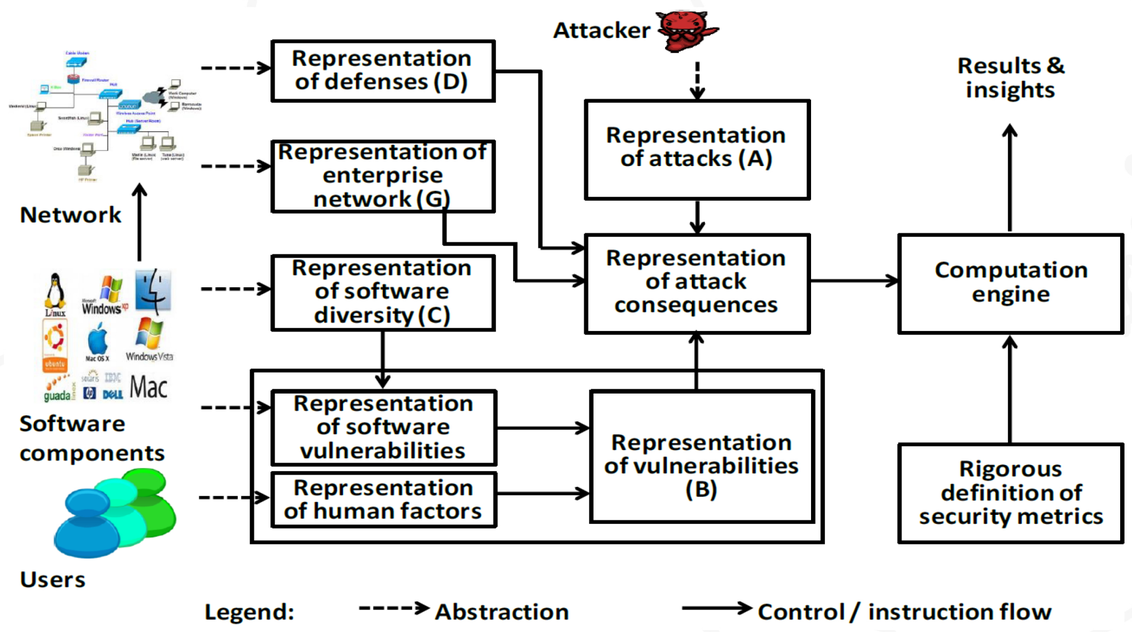
# Quantifying the Security Effectiveness of Network Diversity

Huashan Chen[1], Jin-Hee Cho[2], Shouhuai Xu[1]
[1](UT San Antonio, email: Shouhuai.Xu@utsa.edu)
[2](US Army Research Lab, email: jin-hee.cho.civ@mail.mil)

## Introduction

- The risk of employing monoculture software prompts the need of *artificial diversity* via N-version programming, which uses multiple, independent versions of software that provides a same functionality. Market competition also leads to the so-called *natural diversity* that multiple software programs offer a same functionality.
- Artificial diversity and natural diversity manifest the broader notion of network diversity. While intuitive, security effectiveness of enforcing network diversity has yet to be characterized quantitatively.
- In this work, we propose the first systematic, fine-grained framework for modeling the diversification of software stacks in networks and quantifying the security effectiveness of network diversity via a suite of security metrics.

## Framework

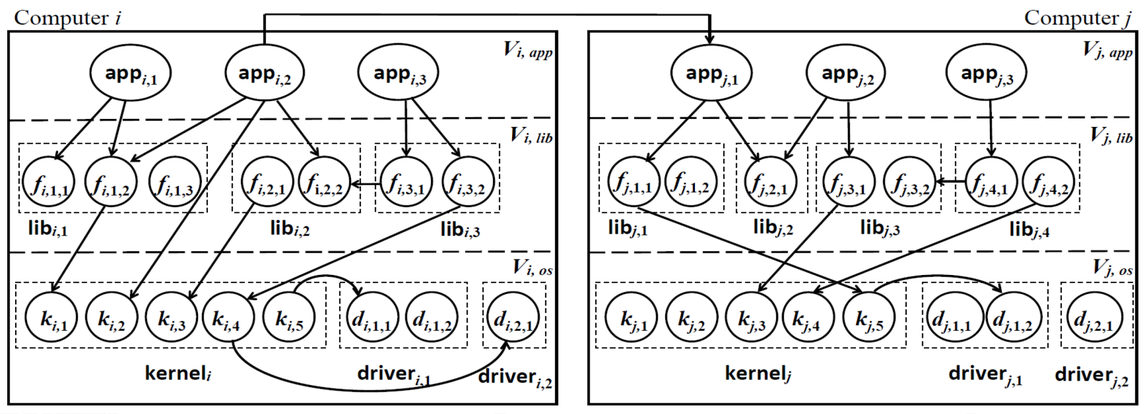


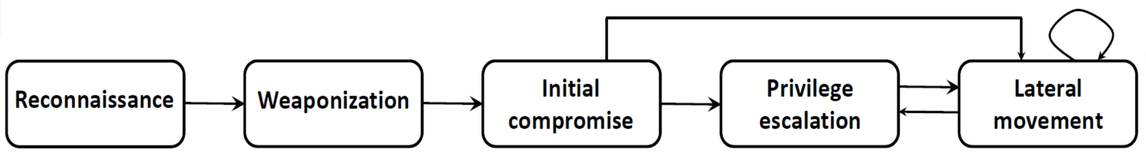

- The research is to characterize a family of mathematical functions $f_i$ such that

$$m_i = f_i(G, A, B, C, D)$$

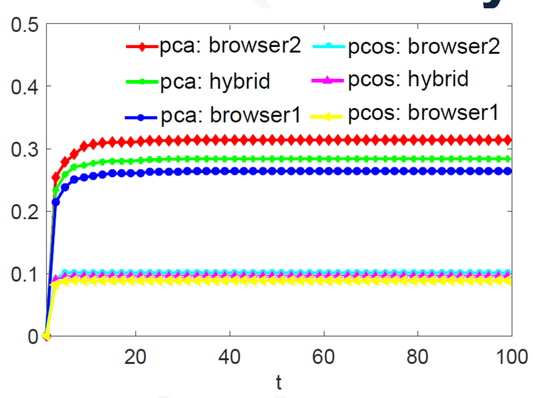
$m_i$: security metric
$G$: an enterprise network in a certain representation
$A$: attacker profile (including attack strategy)
$B$: vulnerabilities of network software and human factors
$C$: software stack configuration
$D$: defense employed to protect the network

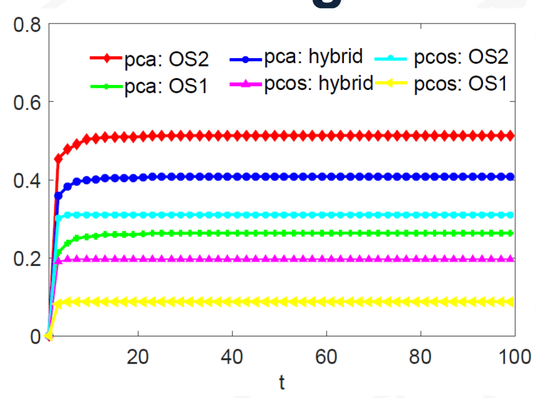
## Illustration of G and Attack Strategy



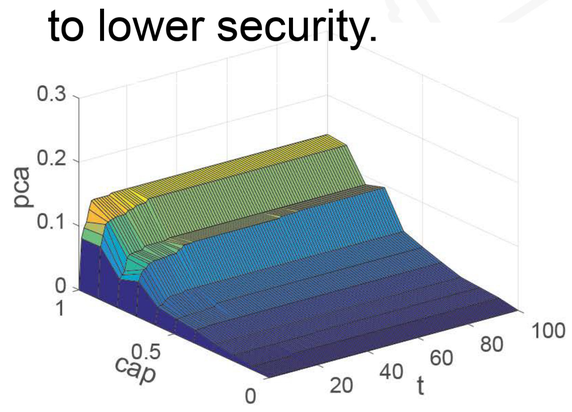




## Preliminary Results & Insights

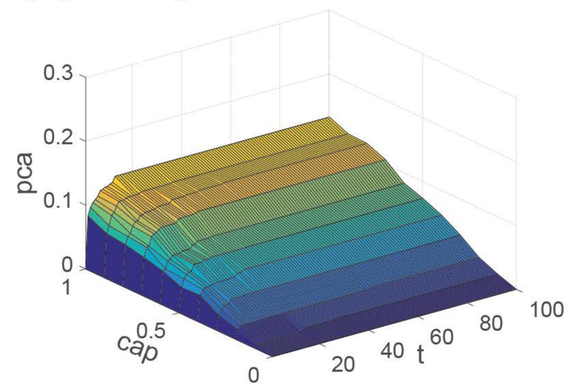


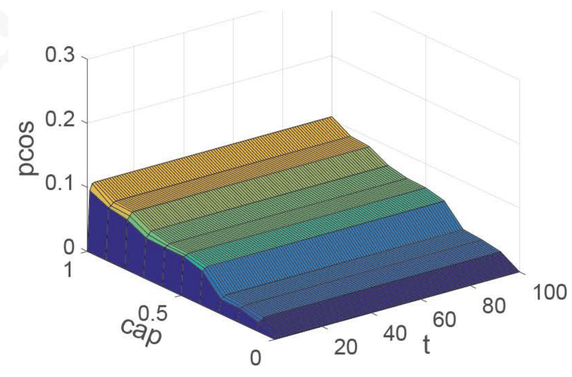

- **Insight 1.** Natural diversity can lead to higher security when the diversified software implementations have a higher security quality (than monoculture implementations); otherwise, natural diversity can lead to lower security.



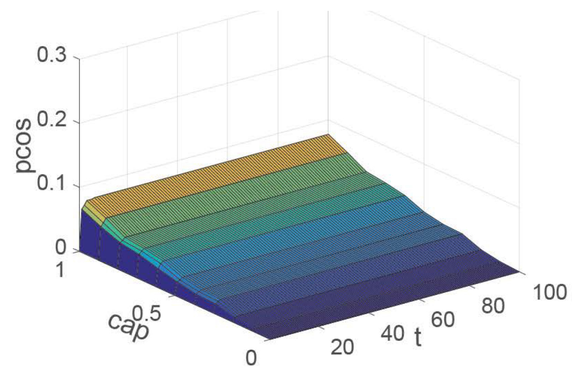

(a) $C_0$, $\zeta = 0.1$



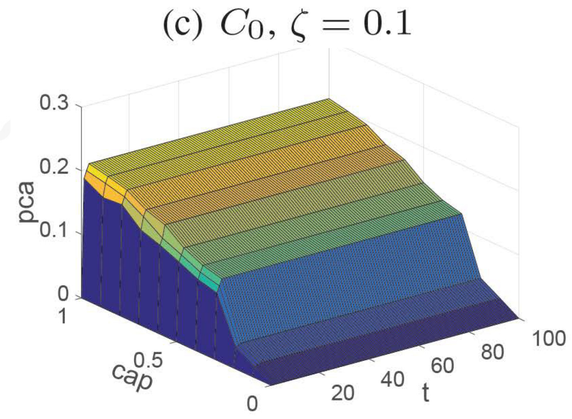

(b) $C_1$, $\zeta = 0.1$



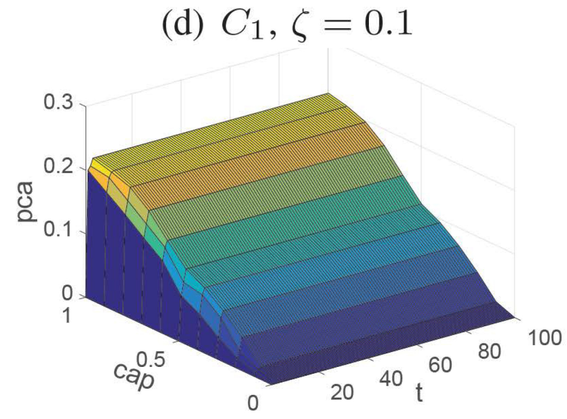

(c) $C_0$, $\zeta = 0.1$




(d) $C_1$, $\zeta = 0.1$

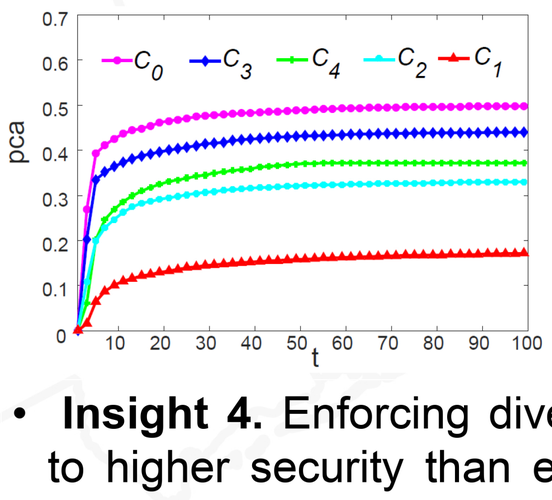


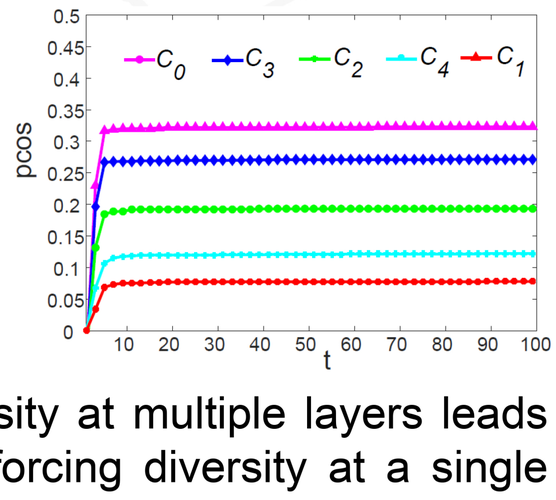

(e) $C_0$, $\zeta = 0.2$




(f) $C_1$, $\zeta = 0.2$

- **Insight 2.** Artificial diversity lead to gradually (rather than abruptly) increasing damages with respect to increasing attacker capabilities.
- **Insight 3.** Security effectiveness of network diversity largely depends on the security quality of the diversified implementations, meaning that diversity can increase, make no difference, or decrease security.




- **Insight 4.** Enforcing diversity at multiple layers leads to higher security than enforcing diversity at a single layer.

Full version of the paper will be available soon.

HOTSOS 2018
5TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**
APRIL 10-11, 2018 | RALEIGH, NORTH CAROLINA