ROSS: Randomization of Operating System for Security

Anya Berdichevskaya
Jared Crane
Wenliang Du (Kevin)
Rajeev Gopalakrishna
Advisor: Gene Spafford
Problem

• An attack script developed on one machine is likely to work on thousands of other machines.

• Examples:
  - Denial-of-service attack.
  - Buffer overflow attack.
  - Virus, worm.
Motivations

• If every intrusion, virus, or worm had to be crafted explicitly to a particular machine, the cost of trying to penetrate computer systems would go up dramatically.

• How to do this?
  - Randomization or specialization of software.
Objectives

• Randomization on operating system.
  - What features of an operating system can be randomized to improve system security, and how?
  - How does that affect usability?
  - How does it affect system performance?

• Develop a prototype system based on OpenBSD as a proof of concept.
Framework

OpenBSD

Randomize

Secret Mapping

Program

Randomized OpenBSD

Randomize

execute

execute

execute
What Can Be Randomized?

- Dynamic libraries.
- System calls.
- Names for system files.
- Environment variables.
- Data locations.
- System behaviors.
- And more ...
Current Work

- Randomizing system calls.
  - Write() $\rightarrow$ exit(), execve() $\rightarrow$ kill();

- Randomizing dynamic libraries.
  - Dynamic loader: ld.So.
  - fwrite() $\rightarrow$ fread(), fread() $\rightarrow$ fclose();
Example 1: Buffer Overflow

STACK

exec("/bin/sh")

Rt: 3456923

overwritten

Mapping table

exec ➔ exit
write ➔ read

correct execution
Example 2: Malicious Code

Good Code → Dynamic Loader (ld.so) → execution

mapping

Inverse mapping

Malicious Code → Dynamic Loader (ld.so) → execution

No execution
Limitations

• What it works for:
  - Specialized machine, such as firewall
  - Relatively stable environments

• What it does not work for:
  - Inside intrusions
  - Dynamic environments (inconvenience)
Future Plans

- Investigate other features.
- Study specialization techniques used for other purposes, and try to use them for the security purpose.
- Randomizing applications.
  - How to systematically randomize applications?