CERIAS

Virtual Playgrounds For Worm Behavior Investigation

Xuxian Jiang†, Dongyan Xu†, Helen, J. Wang‡, Eugene H. Spafford†

†CERIAS and Department of Computer Science,
Purdue University, West Lafayette, IN 47907
{jiangx, dxu, spaf}@cs.purdue.edu

‡Microsoft Research
Redmond, WA, 98052
helenw@microsoft.com

Motivation

Worm Outbreaks
- Fast, Virulent, and Camouflaged

Blended Worm Threat
- Spam/DDoS/Zombie Networks
- Access For Sale

Objective

Understanding Worm Behavior
- Exploitation, Propagation, Payload…

Existing Approaches
- Large-Scale Propagation
  - ✓ Simulation (e.g., SIR, Two-Factor)
- Relative Static/Local Actions
  - ✓Reverse Engineering (e.g., IDA pro, gdb)

What's Missing
- ***A Safe and Realistic Worm Playground***

Key Features

High Fidelity

Strict Confinement

Flexible & Convenient Control

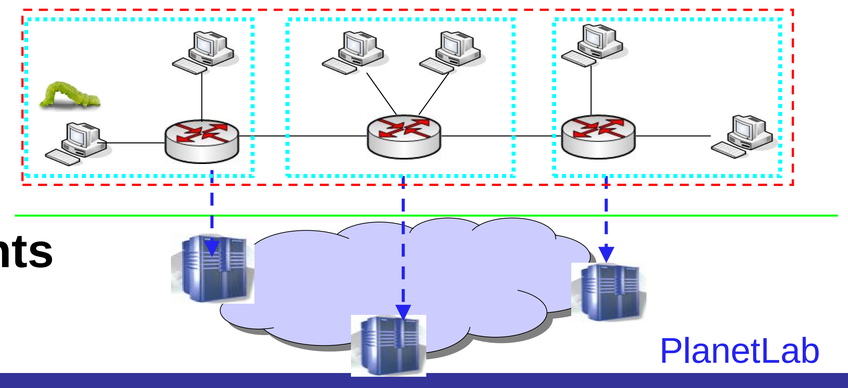
Good Scalability
- **3000** Virtual Hosts in **10** Physical Nodes

Unique Experiment Capabilities
- Iterative Worm Experiment
- Stealthy/Polymorphic Worms
- Routing Worms and Infrastructure Instability

vGround Approach

Virtualized Resources
- Full-System Virtualization
- Network Virtualization

Configurable Experiments



Key Techniques

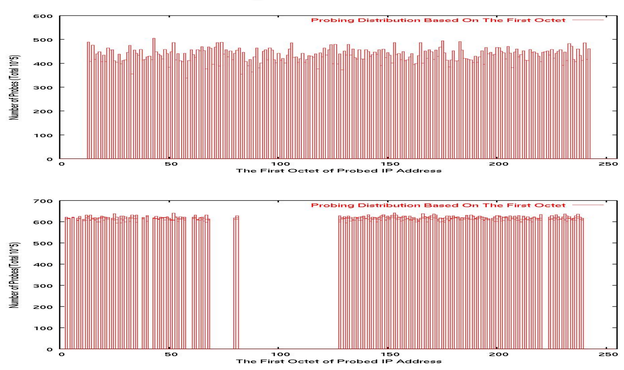
Resource Virtualization
- Existing Virtual Machine Techniques
  - ✓ Kernel-Level Virtualization (e.g., VMware)
  - ✓ Para-Virtualization (e.g., Xen, Denali)
- NEW! **User-Level Virtualization** (enhanced UML)
- New Virtual Network Techniques
- NEW! **Link-Layer Virtualization**

User Configurability
- NEW! Node Customization
- NEW! Topology Specification

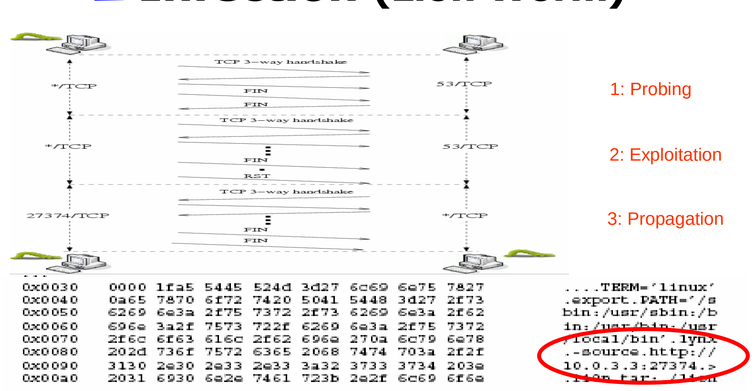
Experiment Convenience
- NEW! Automatic Bootstrap/Cleanup
- NEW! Monitoring and Trace Collection

Real-World Worm Behavior Reproduction

Probing



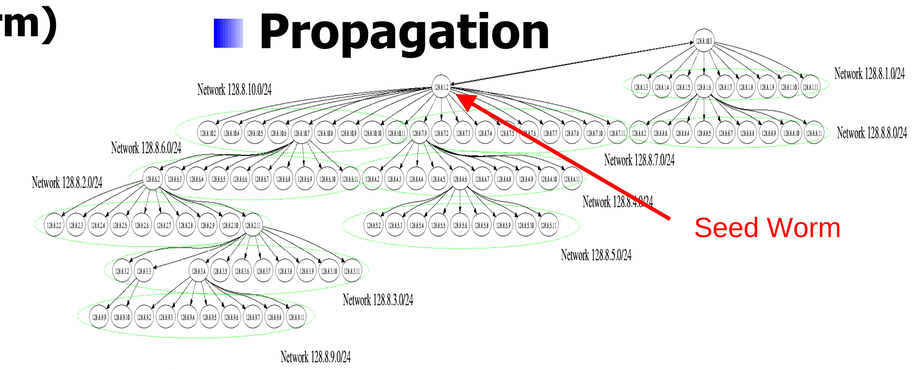
Infection (Lion Worm)



Payload (Slapper Worm)

```
[root@c1_2 /root]#pudclient 127.0.0.1
PUD Client version 11092002Ready, type in the
commands as follows, or type help for a list:

help
The commands are:
  * kill       kills the daemon

  * log        log output to file

  * bounce     adds a bounce
  * close      closes a bounce

  * info       requests info
  * list       lists the current servers
  * sh         execs a command
  * udpflood   send a udp flood
  * tcpflood   send a tcp flood
  * dnsflood   send a dns flood
  * escan      scans hard drive for emails
```

Propagation



http://www.cs.purdue.edu/homes/jiangx/vGround

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center