



Novel Applications of Xen: Virtual Training & Malware Evaluation

June 23, 2008

Stephen Brueckner
ATC-NY
Ithaca, NY



ATC-NY

Architecture Technology Corporation

Introduction

- ▶ Novel applications
 - ▶ Not typical enterprise usage
 - ▶ User works both inside & outside VMs
 - ▶ One user interacts with many VMs
 - ▶ Minimize external footprint inside VMs
- ▶ User space
 - ▶ Minimal changes to Xen
 - ▶ Scripting using “xm” commands



Projects

- ▶ CYDEST (virtual training environment)
 - ▶ Management interface
 - ▶ Automating access to VM internals
- ▶ EXAMIN (malware testing environment)
 - ▶ VM configuration tool
 - ▶ VM introspection work
- ▶ Started 3 and 2 years ago, respectively



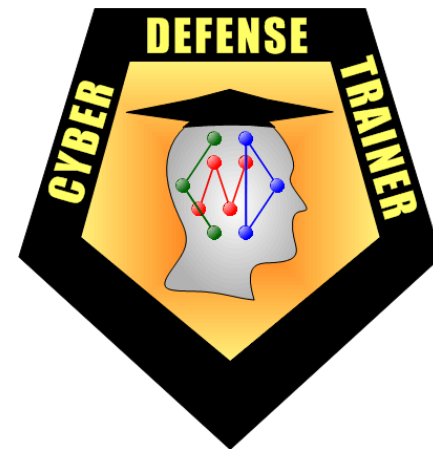
Objectives

- ▶ Inform you of our projects' requirements
- ▶ Show you the tools we developed
 - ▶ Describe Xen features we built upon
 - ▶ While seeking advice on alternatives
- ▶ Provide feedback to Xen community
 - ▶ Problems
 - ▶ Wish lists
 - ▶ Questions

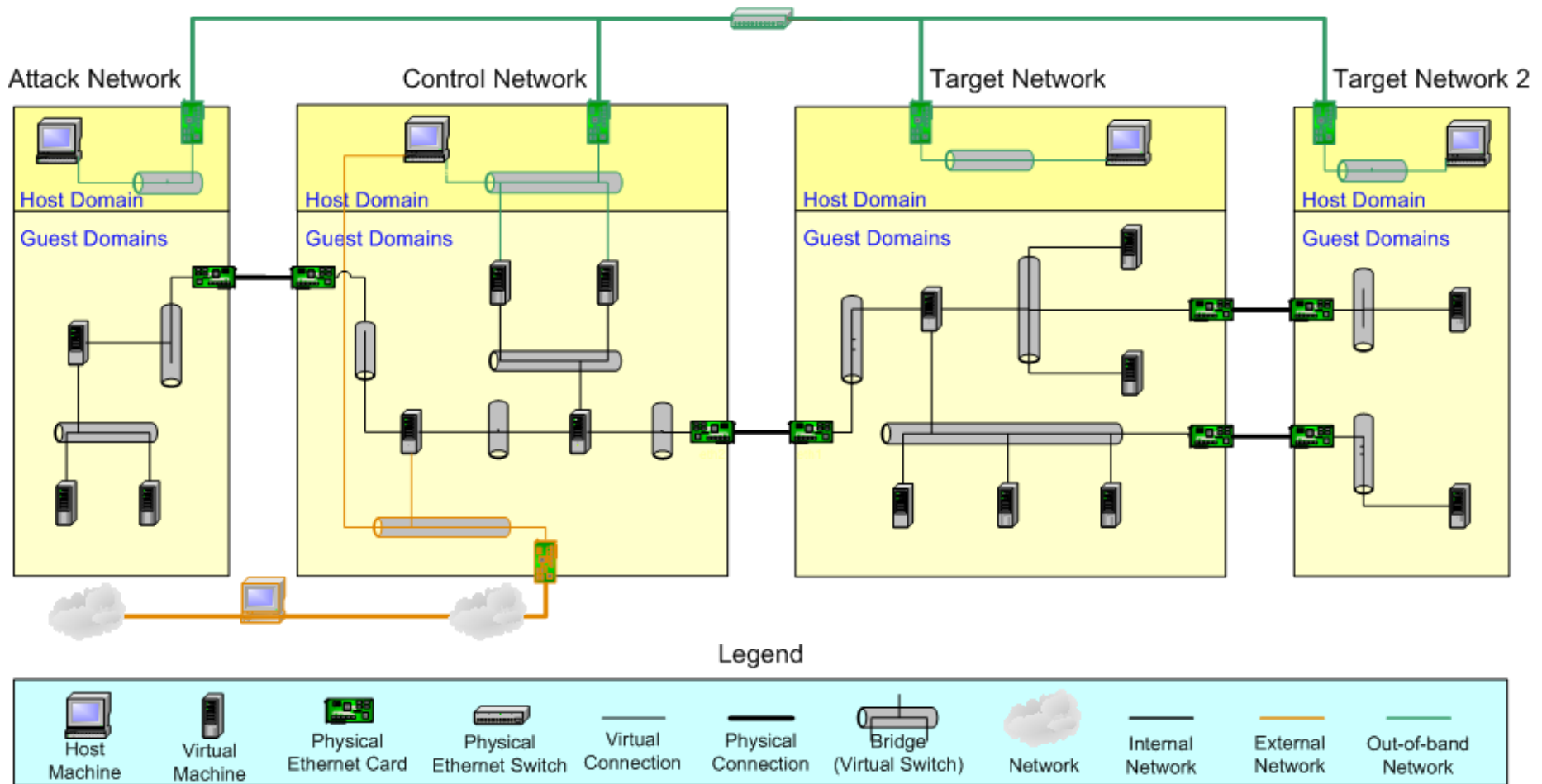


CYDEST: Cyber Defense Trainer

- ▶ Realism
 - ▶ Real attacks & defense tools
 - ▶ Both network and hosts
 - ▶ Full fidelity (not a simulator)
- ▶ Availability
 - ▶ Web access
 - ▶ Up 24/7/365
- ▶ Automation
 - ▶ Auto-assessment
 - ▶ Automated dynamic attacks



CYDEST Architecture



Trainee's Management Interface

- ▶ Goal: Maintain trainee's situational awareness
- ▶ Graphical representation (with labels)
 - ▶ Net topology, hostnames, IPs, OSs
- ▶ Component Status (using colors)
 - ▶ VMs & bridges: "up," down, booting/shutting down
- ▶ Controls (buttons)
 - ▶ Start, Stop, VNC
- ▶ Implementation
 - ▶ Web-enabled
 - ▶ Manually configured



CYDEST Management GUI

The screenshot shows a Mozilla Firefox browser window displaying the CYDEST Management GUI. The address bar shows the URL: `https://192.168.1.98/cgi-bin/scenarioselect.pl?ticket=0.75318220886698&scenid=2`. The GUI is titled "Target Network" and displays a network diagram with the following components:

- external:** 156.23.209.103 (IDS), 156.23.209.3 (firewall).
- firewall:** 192.168.3.2 (Debian).
- internal:** 192.168.3.1 (IDS), 192.168.2.1 (Router), 192.168.1.1 (Router).
- servers:** DataBase (192.168.2.105), Backup DB (192.168.2.104), Admin 1 (192.168.2.103), Portal server (192.168.2.100), Backup portal (192.168.2.101), Admin 2 (192.168.2.102).
- staff:** Plans WS (192.168.1.10), Operations WS (192.168.1.11), Strategy WS (192.168.1.12), ISR WS (192.168.1.13).

At the bottom of the GUI, there are two control panels:

- Simulation Control:** Simulation status: not ready. Click (once) on the "Start the network" link. Buttons: Cancel.
- Network Control:** Start the network, Stop the network, Refresh.

The browser window also shows a sidebar with "Network", "Notebook", and "View Log" tabs, and a status bar at the bottom with "Done" and the IP address "192.168.1.98".

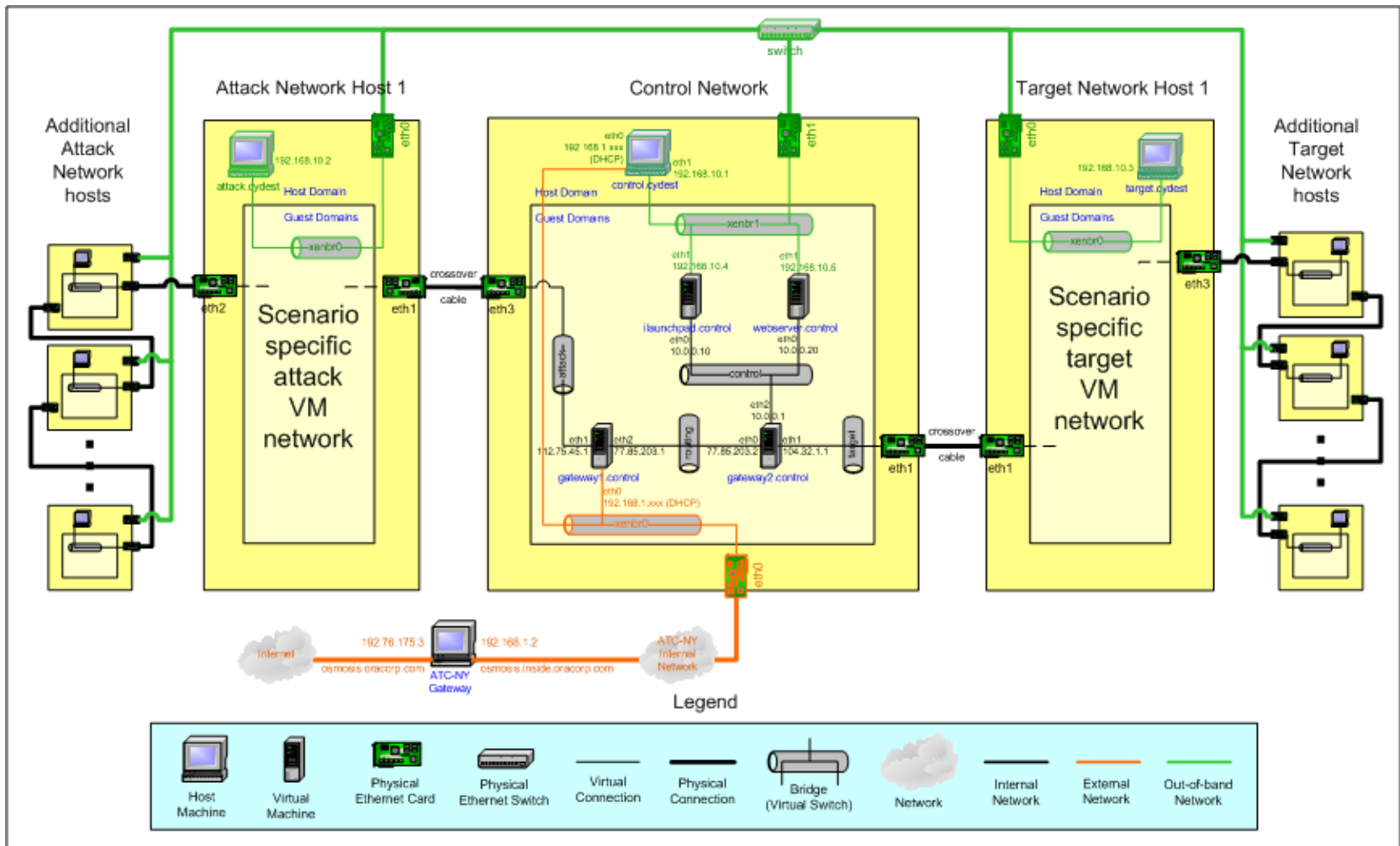


Monitor & Control Channels

- ▶ Requirements
 - ▶ Automatable
 - ▶ Out-of-band (network traffic not visible to trainee)
 - ▶ Reliable (not network dependent)
- ▶ Solution
 - ▶ Separate networks (physical & virtual)
 - ▶ Use guest's serial consoles
 - ▶ Program to negotiate guest interaction
- ▶ Consoles to control Windows VMs
 - ▶ Windows serial console listener and shell
 - ▶ Unfortunately, violates guest sanctity



CYDEST Network Separation



Monitor & Control Channels (cont.)

- ▶ open2xm.pl
 - ▶ Automated console interactions
 - ▶ Queueing of access requests
 - ▶ External & internal timeouts
 - ▶ Buffering I/O (for processes, not humans)
 - ▶ XML encapsulation (separation of stdout and stderr)
 - ▶ Handles login (handles various users & prompts)
 - ▶ Batch mode
- ▶ Implementation
 - ▶ Scripted using “xm console”
 - ▶ Currently experimenting with Xen API (XML RPC)



EXAMIN:

Exploit and Malware Incubator

- ▶ A testing/reverse engineering platform
- ▶ Motivation:
 - ▶ Closed-sourced software has uncertain pedigree
 - ▶ May therefore include embedded malicious code
- ▶ Virtualization is common approach
 - ▶ VM detection currently an anti-tamper technique...
 - ▶ Not anticipated to be an issue in the future



EXAMIN Design

- ▶ Native kernels (HVMs)
 - ▶ Stealthy malware may not execute in paravirt
 - ▶ E.g., LKM rootkit expecting “sysenter_entry”
- ▶ Components
 - ▶ Incubator: the VM network
 - ▶ Instrumentation
 - ▶ Internal: standard tools
 - ▶ External: VM introspection

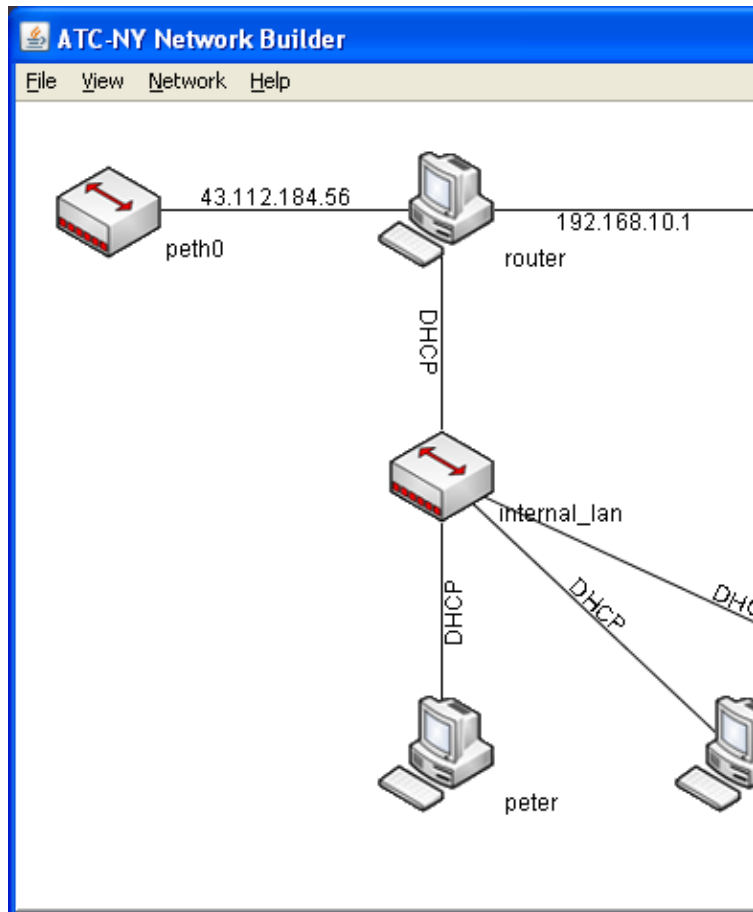


EXAMIN Incubator Creation

- ▶ Objective:
 - ▶ User-configurable heterogeneous VM network
- ▶ Virtual Network Builder (VNB)
 - ▶ Front-end topology editor
 - ▶ Back-end VM provisioning
 - ▶ Linux (dead image manipulation)
 - ▶ mount, chroot, rpm
 - ▶ Windows (provisioning live VMs)
 - ▶ Because registry can't be modified w/o Win API



EXAMIN VNB



ATC-NY VM Data Editor

General Physical Users Services Applications **Network** Startup

DNS 92.130.48.115 Note: Xen imposes a maximum of 3
 Ethernet card information table: ethernet cards per virtual machine.

Card Name	MAC	Static/DHCP	IP Addr.	Netmask	Broadcast
eth0	7A:C0:6E:1...	static	192.168.10.1	255.255.255.0	192.168.1....
eth1	4E:62:0A:7...	DHCP			

Add Card Edit Selected Delete Selected

Default Gateway: IP 92.130.48.115 Interface eth1

Routing table:

Destination	Gateway	Genmask	Interface
192.168.10.0		255.255.255.0	eth0

Add Route Edit Selected Delete Selected

Apply Cancel



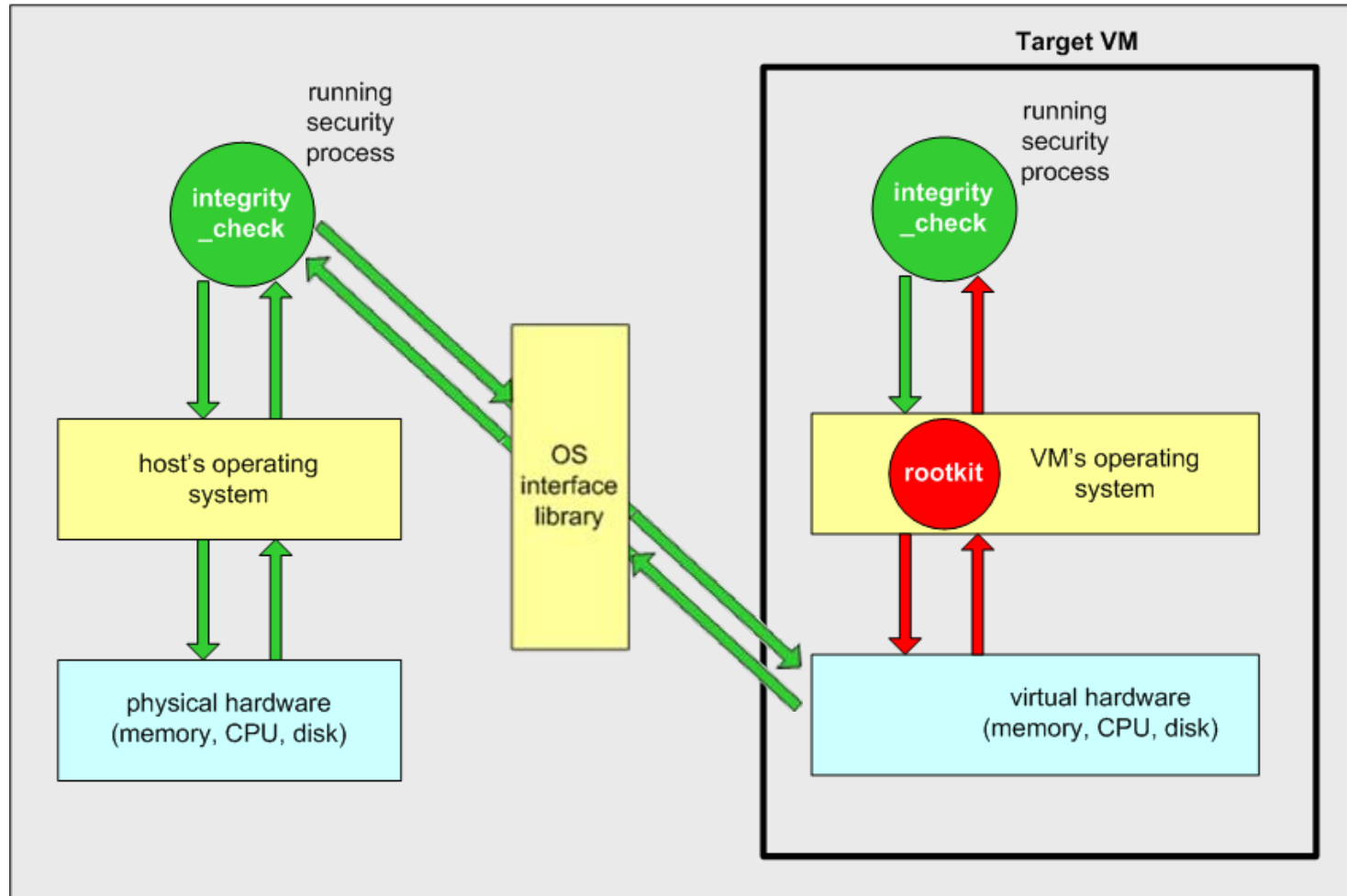
EXAMIN External Instrumentation

- ▶ High-assurance security monitoring services
 - ▶ VM introspection of guest kernel's memory
 - ▶ Using XenAccess (open source introspection library)
- ▶ Current services:
 - ▶ Integrity checking kernel & processes
 - ▶ Code segments
 - ▶ Specific structures (IDT, system call table)
 - ▶ “Mostly static” structures (module list)
 - ▶ Cross-view checking
 - ▶ High assurance versions of standard HIDS
 - ▶ NIDS (not true VM introspection)



EXAMIN: Bridging Semantic Gap

EXAMIN host



Bridging Semantic Gap: Preview of WIP

- ▶ Automated
 - ▶ Determine data structure layouts and magic numbers
- ▶ Generalizable to most OSs
 - ▶ Implemented for both Linux and Windows
- ▶ Run same code on host and guest
 - ▶ No learning curve for a new language or API
 - ▶ Ease porting of existing apps
- ▶ Attend VMsec/CCS in October for details
 - ▶ Paper submitted...



Problems

- ▶ EXAMIN: guest isolation guarantees important
 - ▶ Continuous security bug fixes
 - ▶ Hypervisor inspection/validation concept practical?
 - ▶ Others are working hard on this
- ▶ Xen's rapid development
 - ▶ Changing APIs
 - ▶ Emerging tools
 - ▶ Both are poorly documented



Wish List

- ▶ Faster serial console or equivalent channel
 - ▶ EXAMIN's cross-view checking needs to stream large pcap files from guest to host
- ▶ Multiple serial consoles
 - ▶ CYDEST's queueing of simultaneous access requests isn't optimal
- ▶ Limit of >3 vif's on a guest?
 - ▶ Never mind...new Xen handles up to 8 vifs



Questions

- ▶ Are there other management interfaces we should look at?
- ▶ We have unusual requirements
 - ▶ Graph-drawing capability for network topology
 - ▶ Integrated remote VNC/shell access
 - ▶ Display & control of bridges
 - ▶ Display of VM internals (hostnames, IPs, OSs)
 - ▶ Web browser interface



Questions (cont.)

- ▶ Are there other VM builders we should be considering?
 - ▶ MLN was originally UML, not a very active project
- ▶ Our requirements:
 - ▶ GUI network builder
 - ▶ VM configuration: network, users, software
 - ▶ Support Linux and Windows



Contact Information

ATC-NY

Cornell Business & Technology Park
33 Thornwood Drive, Suite 500
Ithaca, NY 14850

Technical Contacts:

Mr. Stephen Brueckner, PI
(607) 266-7118
steve@atc-nycorp.com

Dr. Frank Adelstein, Co-PI
(607) 266-7104
fadelstein@atc-nycorp.com

Management Contact:

Ms. Julie Baker
(607) 266-7125
jbaker@atc-nycorp.com

Business Development Contact:

Mr. Gene Proctor
(202) 293-9701 x113
gproctor@atcorp-dc.com

