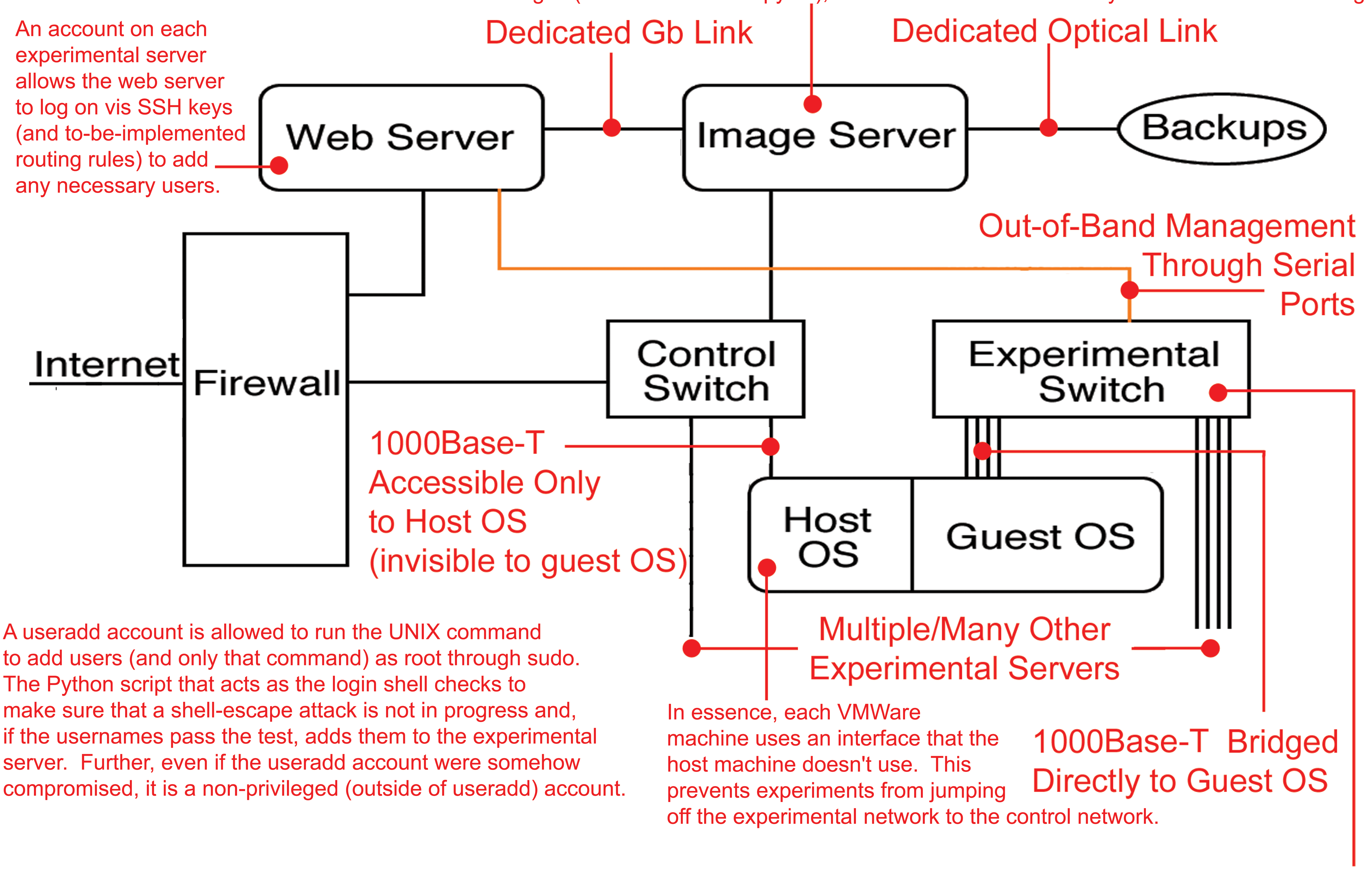
CERIAS

the center for education and research in information assurance and security

# reassure

## A Contained Environment for Testing the Impact of Potentially Malicious Code

On the image server, there is an account that allows the web server to log into it via SSH keys. The login shell for this user is a Python script that takes, interactively, the experimental server (i.e. destination of images), the user who will own the images (i.e. what user to copy as), and the names of an arbitrary number of VMWare images



Dedicated Gb Link

Dedicated Optical Link

An account on each experimental server allows the web server to log on vis SSH keys (and to-be-implemented routing rules) to add any necessary users.

Out-of-Band Management Through Serial Ports

1000Base-T Accessible Only to Host OS (invisible to guest OS)

Multiple/Many Other Experimental Servers

A useradd account is allowed to run the UNIX command to add users (and only that command) as root through sudo. The Python script that acts as the login shell checks to make sure that a shell-escape attack is not in progress and, if the usernames pass the test, adds them to the experimental server. Further, even if the useradd account were somehow compromised, it is a non-privileged (outside of useradd) account.

In essence, each VMWare machine uses an interface that the host machine doesn't use. This prevents experiments from jumping off the experimental network to the control network.

1000Base-T Bridged Directly to Guest OS

ReAssure utilizes VLANs which are configured on the fly over a serial interface by a handful of custom python library commands. The VLANs offer a very secure logical network which allows experiments to be run in parallel while simultaneously preventing interference between them. The VLANs themselves are controlled by a Cisco 4948 switch that runs Cat IOS 12.2 and offers a switching fabric speed of 96-Gbps.

Funded by NSF grant #0420906

Poster Authors: Michael Yang
Primary Investigators: Pascal Meunier - Jan Vitek
Additional Developers: Forrest Fleming - Amanda Denton -Drew Anderson

PURDUE
UNIVERSITY

CERIAS®

Discovery Park
e-Enterprise Center