# Lockdown:
# Distributed Policy Analysis and Enforcement within the Enterprise Network

UNIVERSITY OF NOTRE DAME

**Andrew Blaich, Qi Liao, Greg Allan, Brian Sullivan, Aaron Striegel, Douglas Thain**
**http://netscale.cse.nd.edu/**

**Problem:** Managing, deploying, enforcing, and verifying security policy within an enterprise network.

**Solution:** By using a system of collection agents, data mining, visualization, and Linux Security Modules (LSM) Lockdown is able to achieve efficient policy creation, enforcement, and verification based upon the local context of a host.

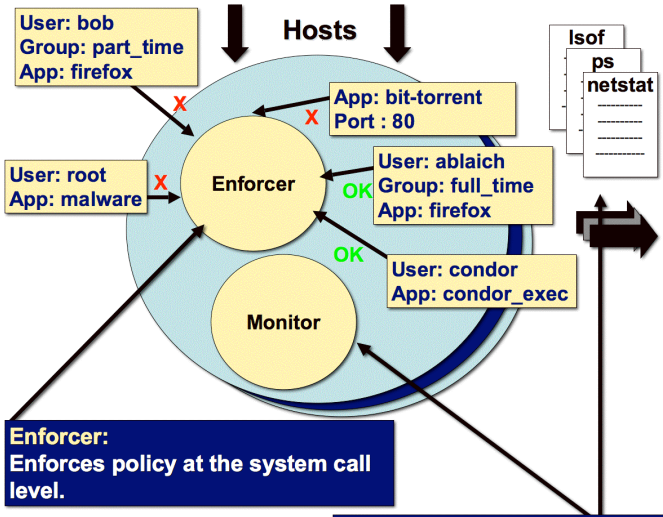
## Synopsis:

Traditional network security tools enforce a policy based on host addresses and port numbers. However, hosts and ports are often not sufficient to define a strong security policy. The Lockdown system allows a network security officer to define, distribute, and enforce a security policy that takes into account local context (such as username and application) in addition to hosts and ports. System activity is collected in a central database for monitoring and analysis.

**Higher-Level Policy:**
- Deny part-time employees from browsing the web.
- Allow full time employees to browse the web only using firefox.
- Allow condor-based grid jobs access to the network.
- Allow users to remote login throughout the network.
- Deny all other network activity.

**Lower-Level Policy:**
[Allow/deny,machine,port,application,user,group,protocol]

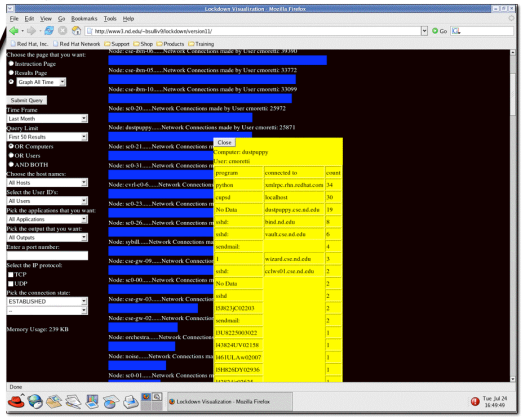
```
allow,*,*,firefox,*,full_time,*
allow,*,*,condor_*,condor,*,*
allow,*,22,sshd,*,*,*
deny,*,*,*,*,*,*
```



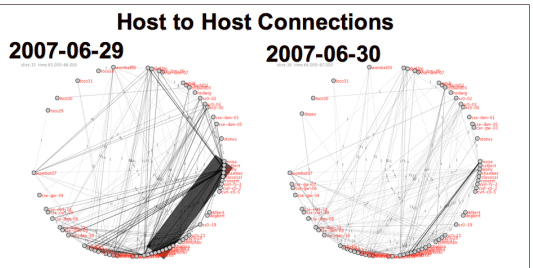

**Enforcer:**
Enforces policy at the system call level.

**Monitor:**
Collects the local context from a host and forwards it to the collection database.

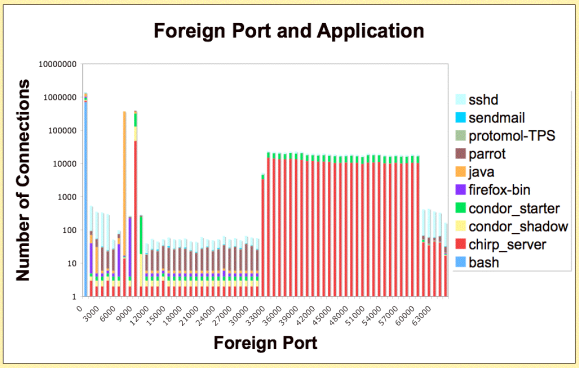
## Local Context:



## Network Visualization:



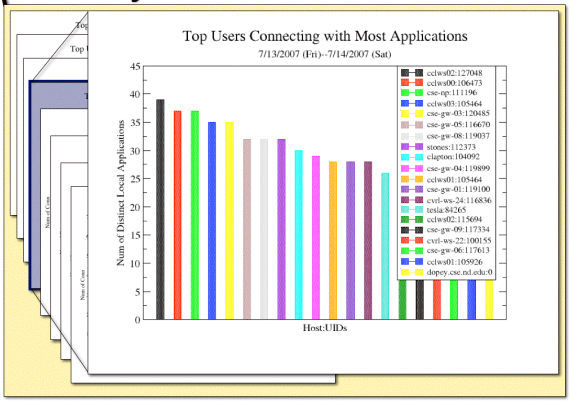

## Data Distribution:




Top 10 applications based on number of connections mapped to foreign port from:

2007-04-23 ->
2007-07-14

## Data Analysis:




Presented at USENIX Security '07 Poster Session, August 2007
This work is supported by NSF Grant CNS-05-49087