



Communication + Social Network Insider Threat Vulnerability Assessment

Ph.D. Program in
Computation,
Organizations
& Society

Michael W. Bigrigg
bigrigg@cs.cmu.edu

Prof. Kathleen M. Carley
kathleen.carley@cs.cmu.edu

Approach

The biggest problem with intrusion detection is the “allowances” afforded to resources inside. Evaluation of the vulnerabilities in the computer network based on who/what can do “anything”
The “anything” computers are a vulnerability: limits anomaly or rule based intrusion detection.

Motivation

CERT 2004 Report Evaluating Insider Threat Incidents:

83% of incidents at workplace

70% of incidents happened during working hours

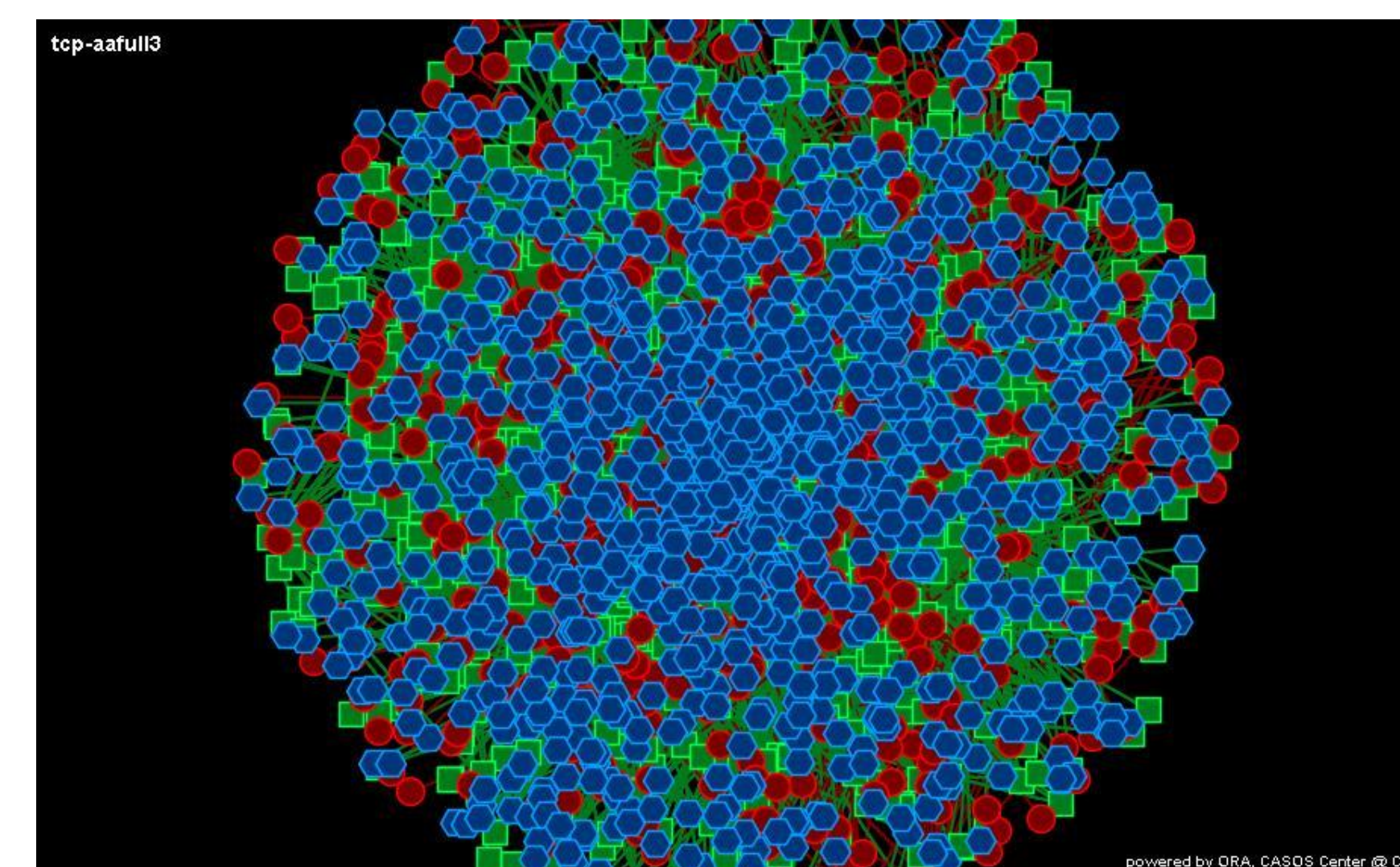
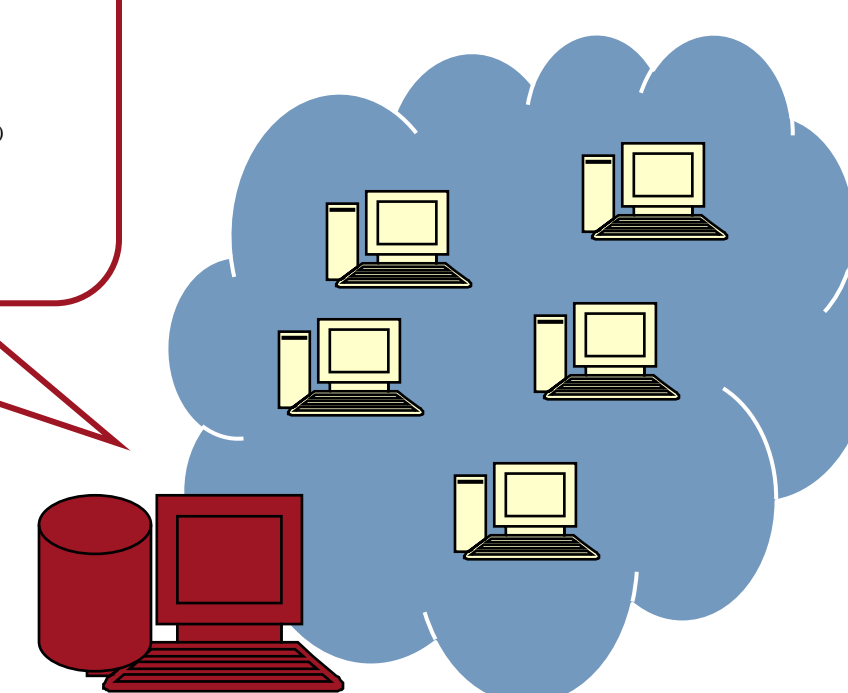
87% of insiders used simple authorized commands

9% of insiders employed advanced programs

```
08:00:39.635343 www.aaa.co.za.1024 > 172.16.113.105.finger: ack 1 win 32120 (DF)
08:00:39.635534 www.aaa.co.za.1024 > 172.16.113.105.finger: P 1:544 ack 1 win 32120 (DF)
08:00:39.646980 172.16.113.105.finger > www.aaa.co.za.1024: ack 5 win 32732 (DF)
08:00:39.647691 www.aaa.co.za.1024 > 172.16.113.105.finger: P 5:7(2) ack 1 win 32120 (DF)
08:00:39.666927 172.16.113.105.finger > www.aaa.co.za.1024: ack 7 win 32730 (DF)
08:00:40.150651 172.16.113.105.finger > www.aaa.co.za.1024: P 1:276(273) ack 7 win 32736 (DF)
08:00:40.150706 172.16.113.105.finger > www.aaa.co.za.1024: F 276:276(0) ack 7 win 32736
08:00:40.151573 www.aaa.co.za.1024 > 172.16.113.105.finger: ack 277 win 31844 (DF)
08:00:40.156140 www.aaa.co.za.1024 > 172.16.113.105.finger: F 7:7(0) ack 277 win 32120
```

DARPA 1999 IDS Dataset

Intrusion detection systems were tested in the off-line evaluation using network traffic and audit logs collected on a simulation network.



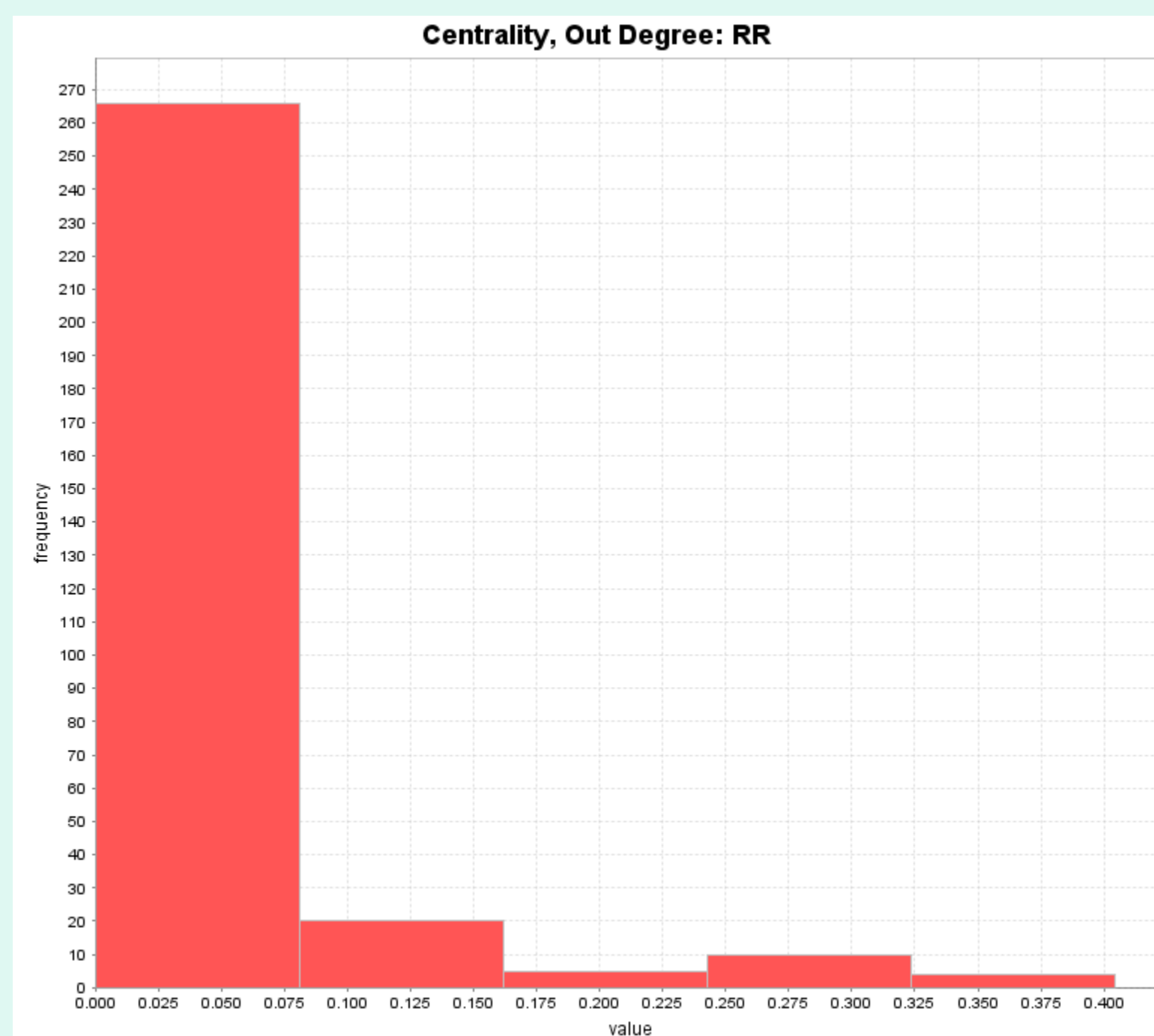
DyNetML Visualization of DARPA 1999 IDS Dataset

Using ORA metrics to evaluate the DARPA 1999 IDS Dataset for Insider Threat Vulnerabilities

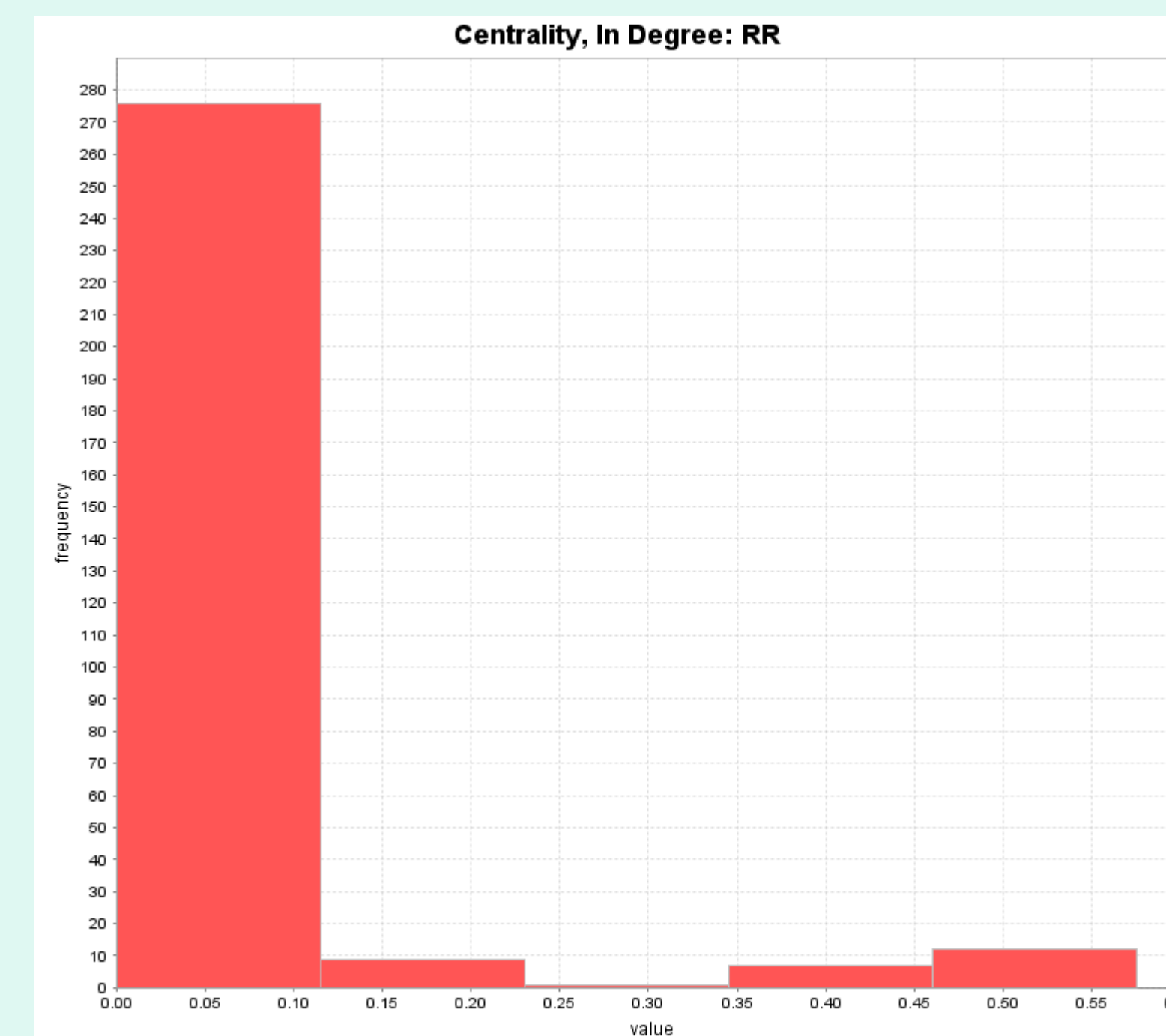


Recommendation: Use an automated IDS system for most computer. Use a human-based IDS system for the centralized computer

Less activity on computer the easier for an anomaly or rule based intrusion detection system to identify uncharacteristic behavior. Only a handful of machines are very active on network

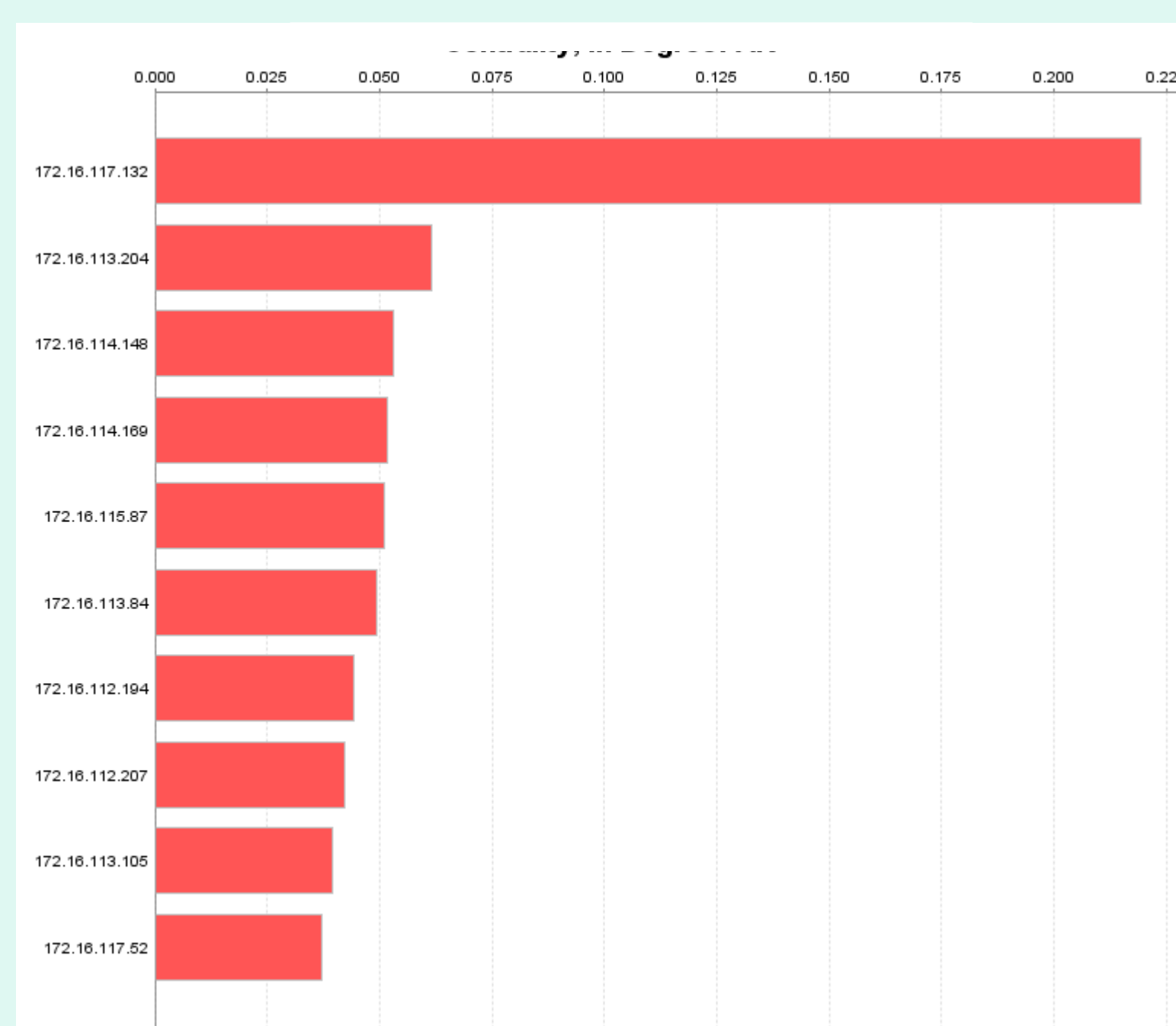


Client Computers Activity

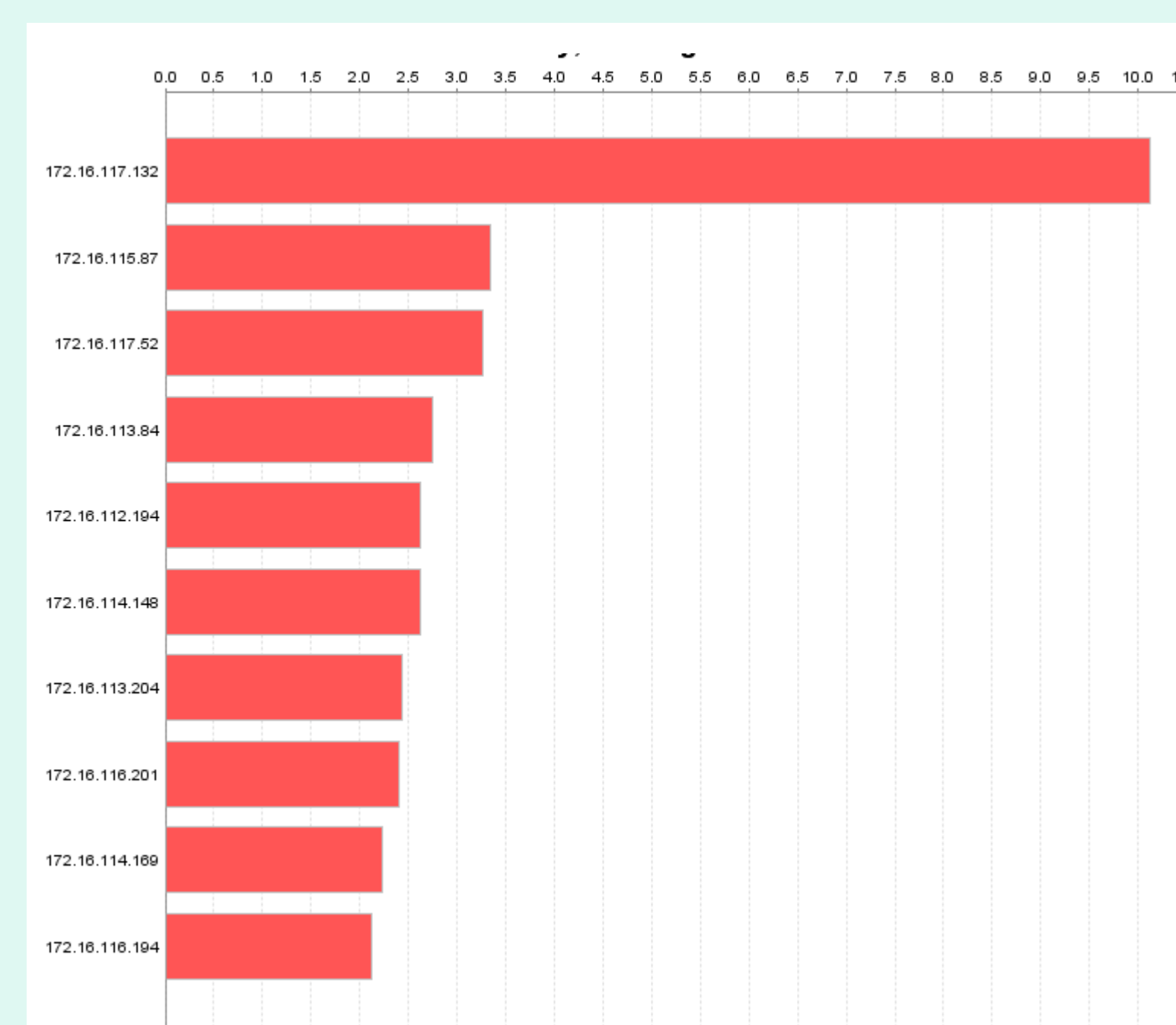


Server Computers Activity

Smaller the number of users and the smaller number of computer tasks the easier for an anomaly or rule based intrusion detection system to identify uncharacteristic behavior

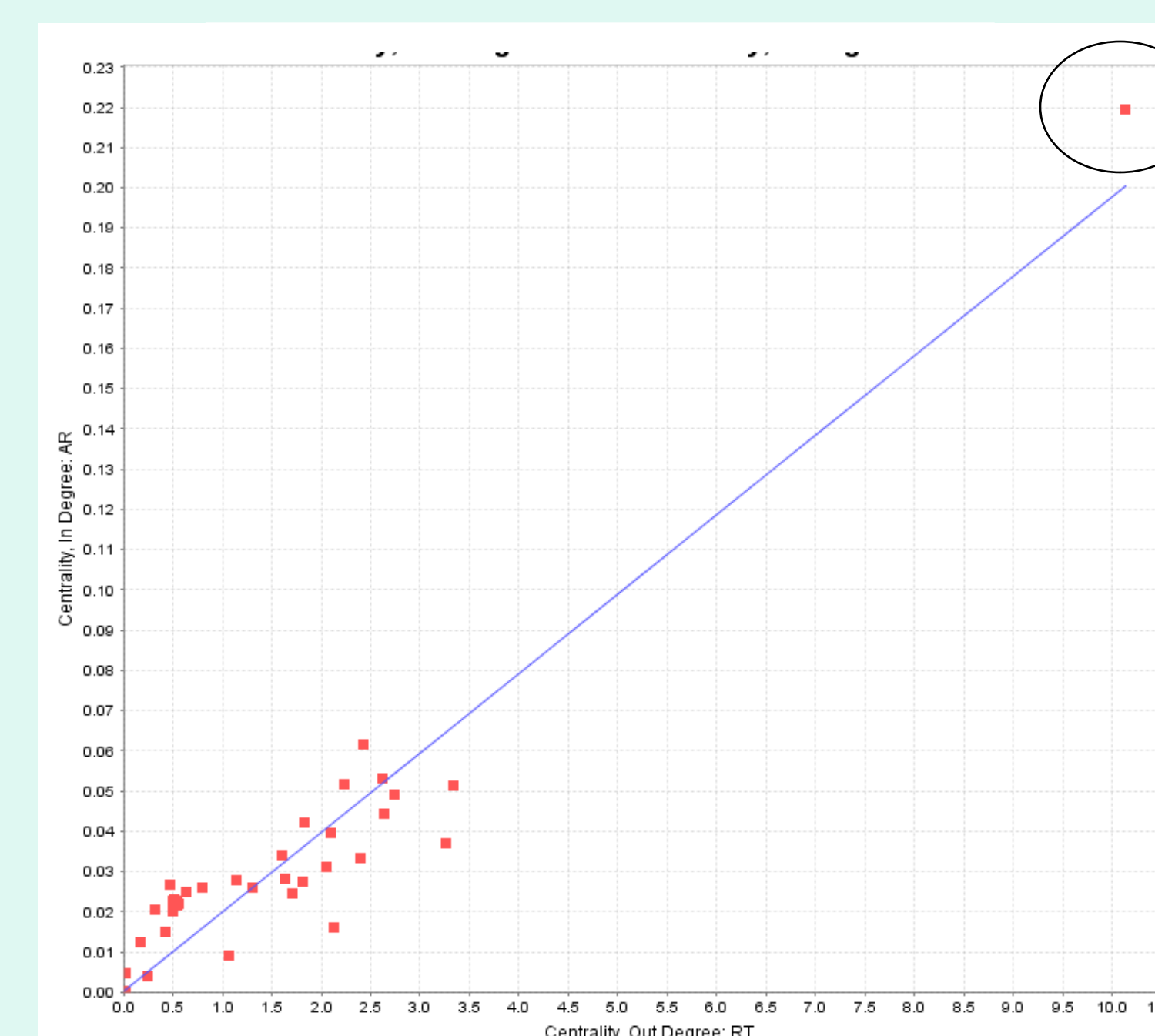


Users Per Computer



Tasks Per Computer

Evaluation shows an ultra-centralized system. One machine is the most vulnerable. Cannot use an IDS on that central machine.



Users vs. Tasks Comparison

This work is part of the Dynamics Networks project at the center for Computational Analysis of Social and Organizational Systems (CASOS) of the School of Computer Science (SCS) at Carnegie Mellon University (CMU). Support was provided, in part, by National Science Foundation (NSF) Integrative Graduate Education and Research Traineeship (IGERT) program, ARL, and ARI. The views and proposal contained in this document are those of the author and should not be interpreted as representing the official policies, either expressed or implied, of the Office of Naval Research, the National Science Foundation, or the U.S. government.

