Carnegie Mellon

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
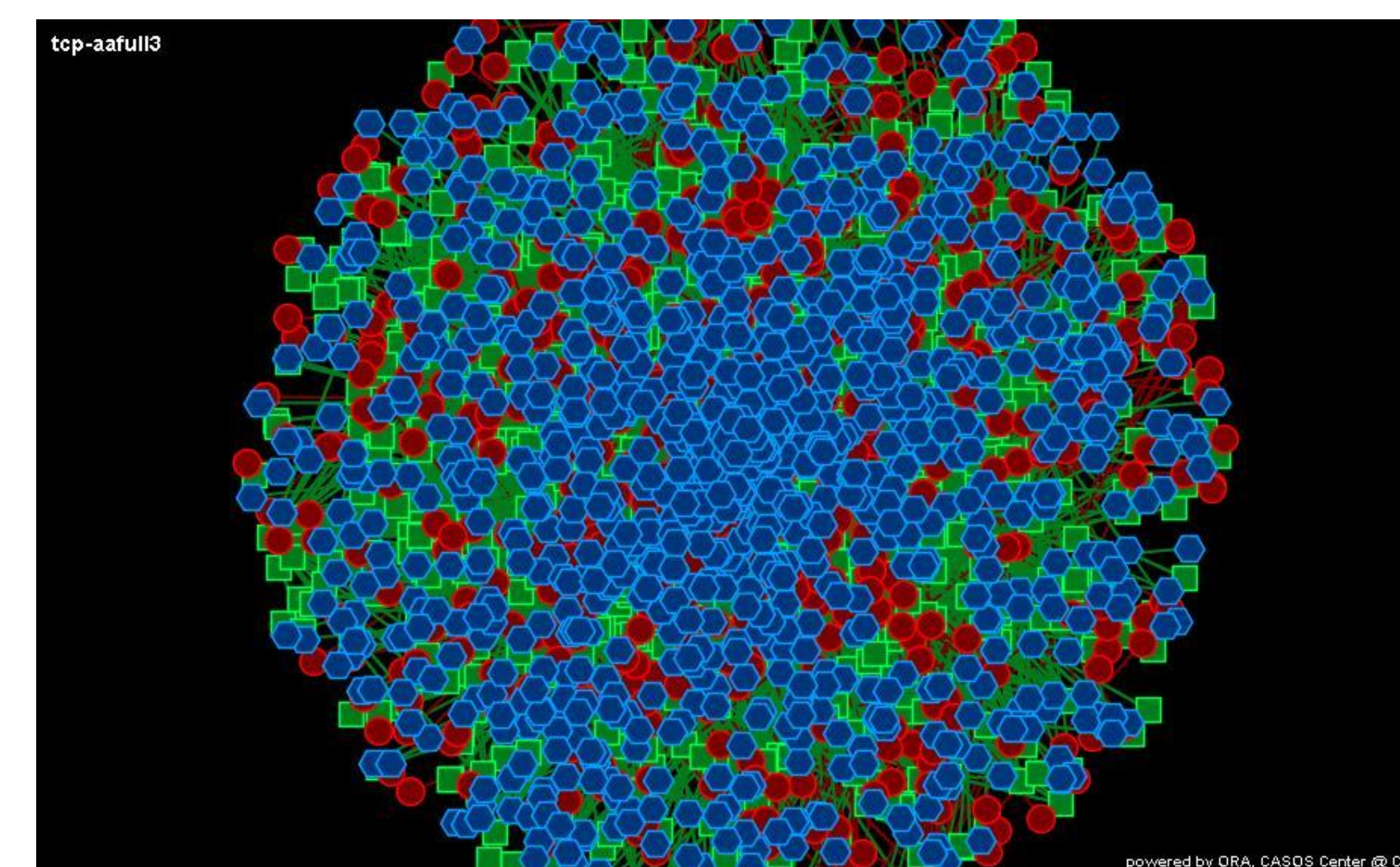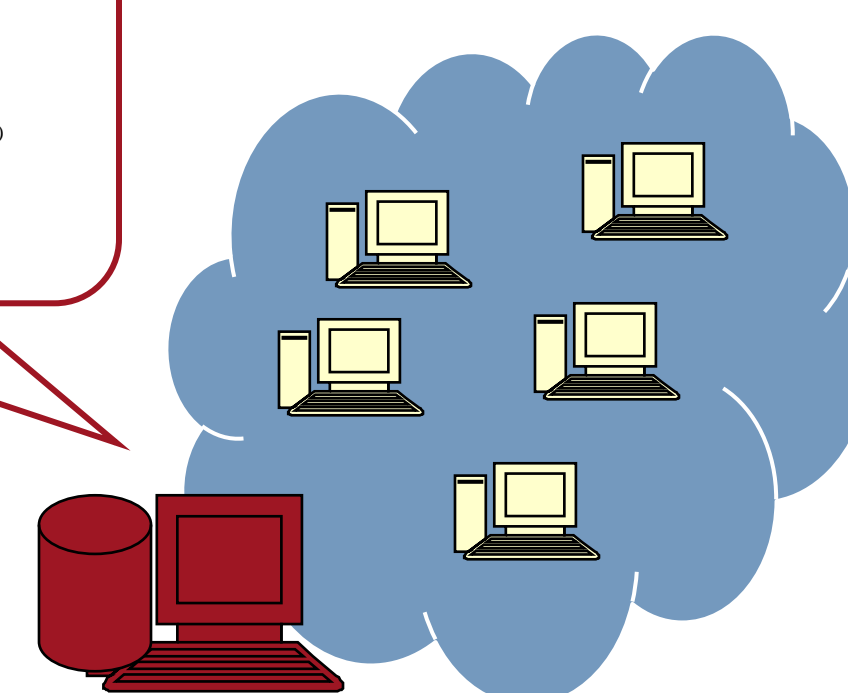
70% of incidents happened during
working hours

87% of insiders used simple
authorized commands

9% of insiders employed advanced
programs

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

ORA
*The Organizational
Risk Analyzer*

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
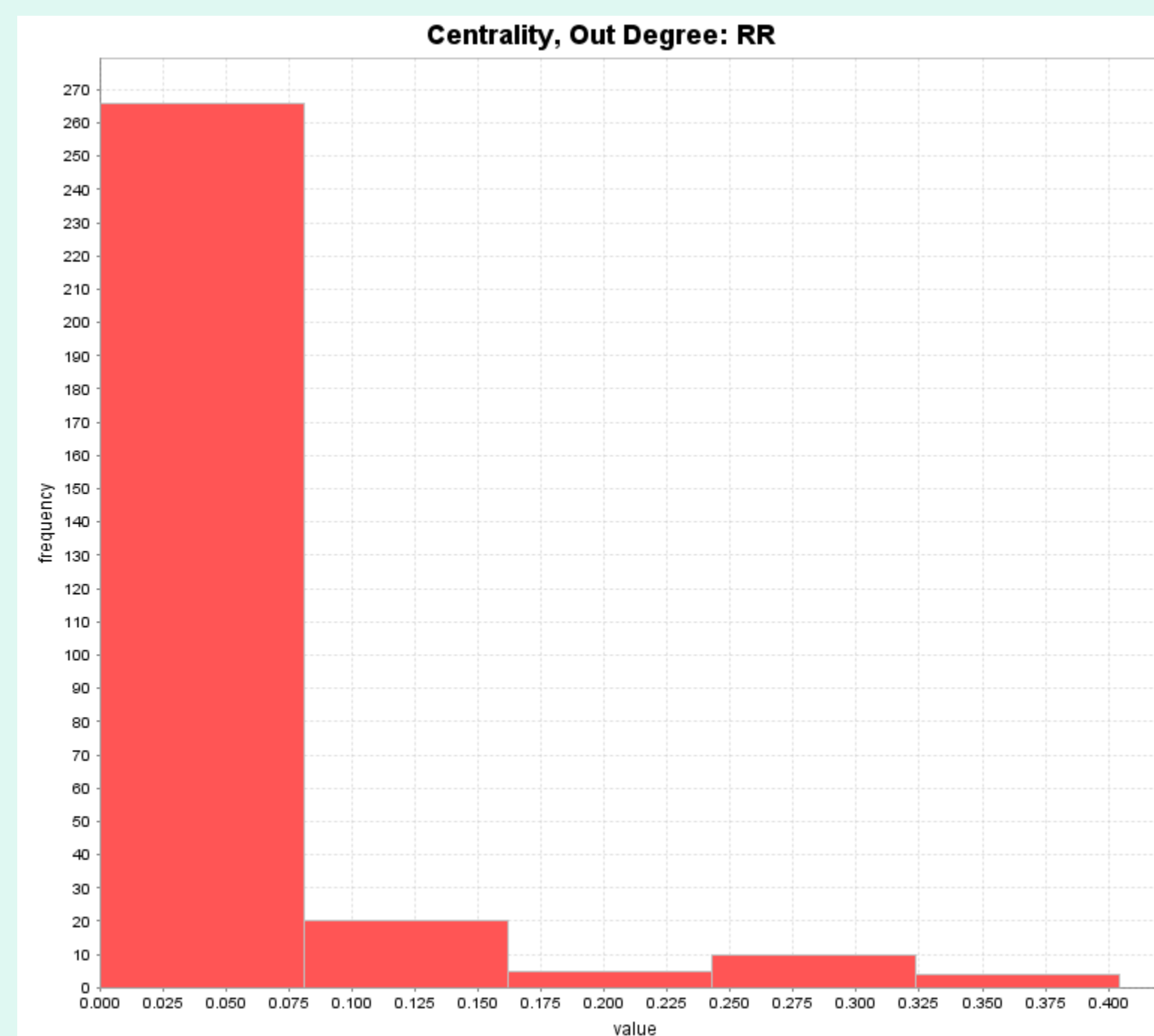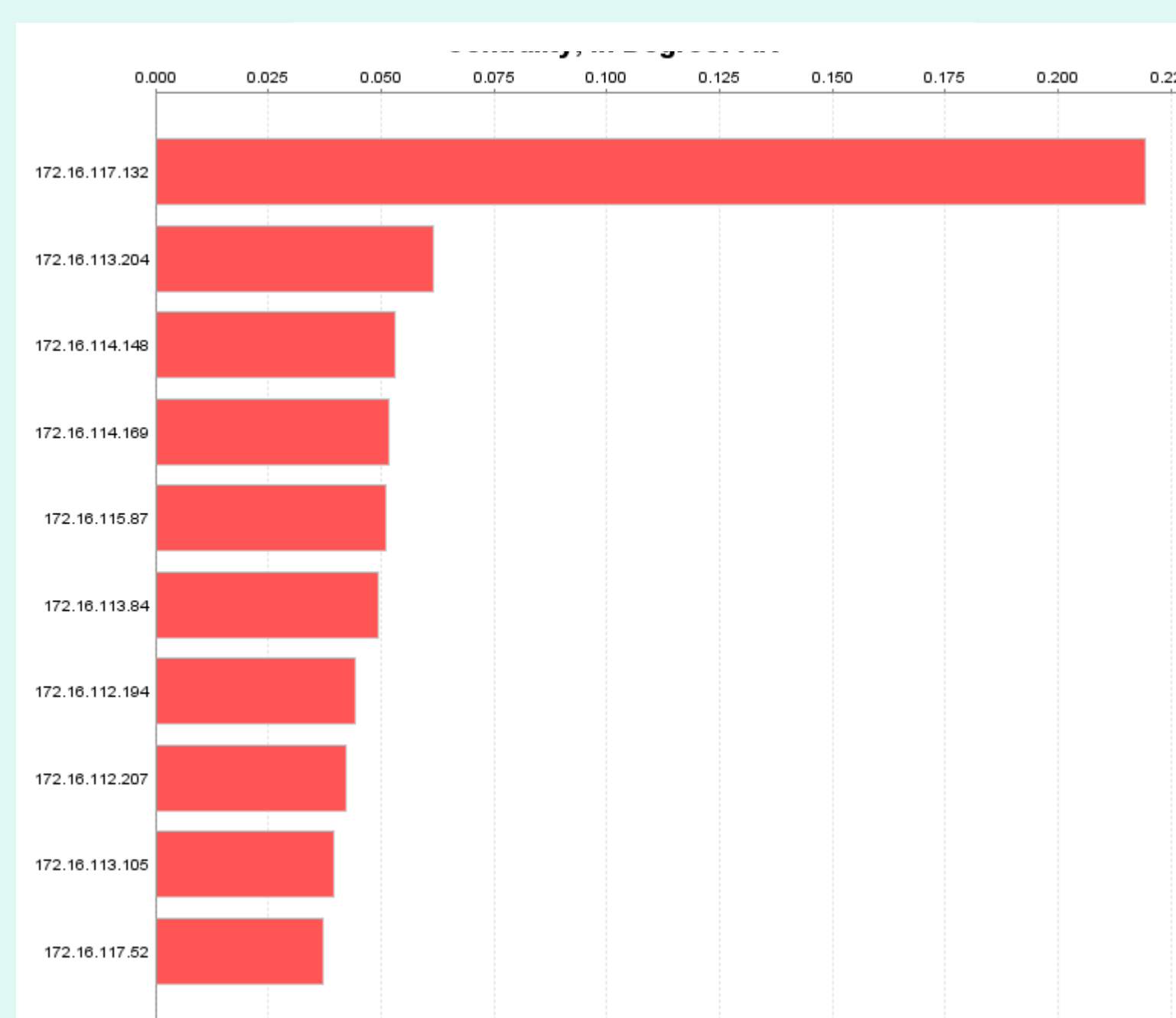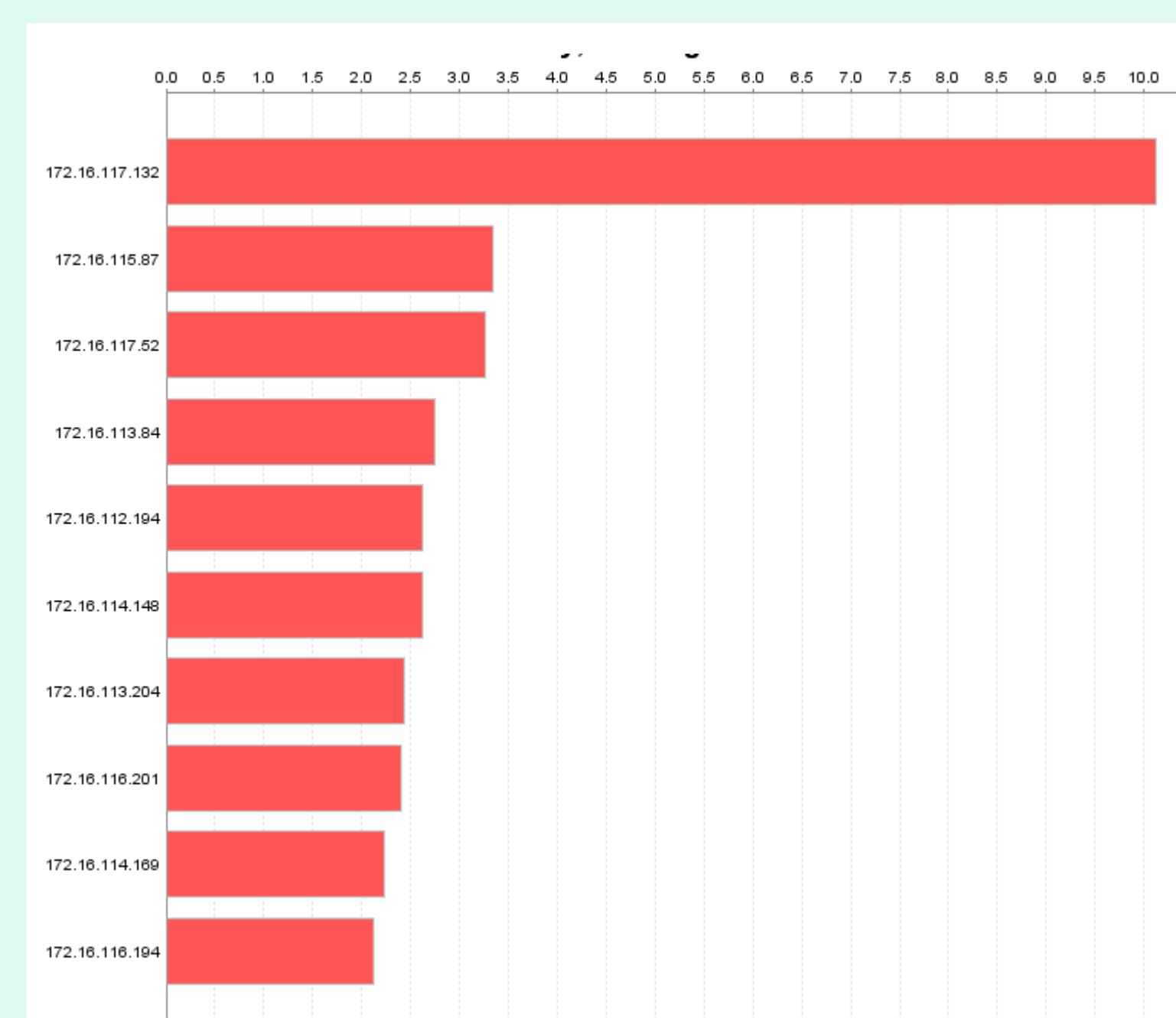

Client Computers Activity
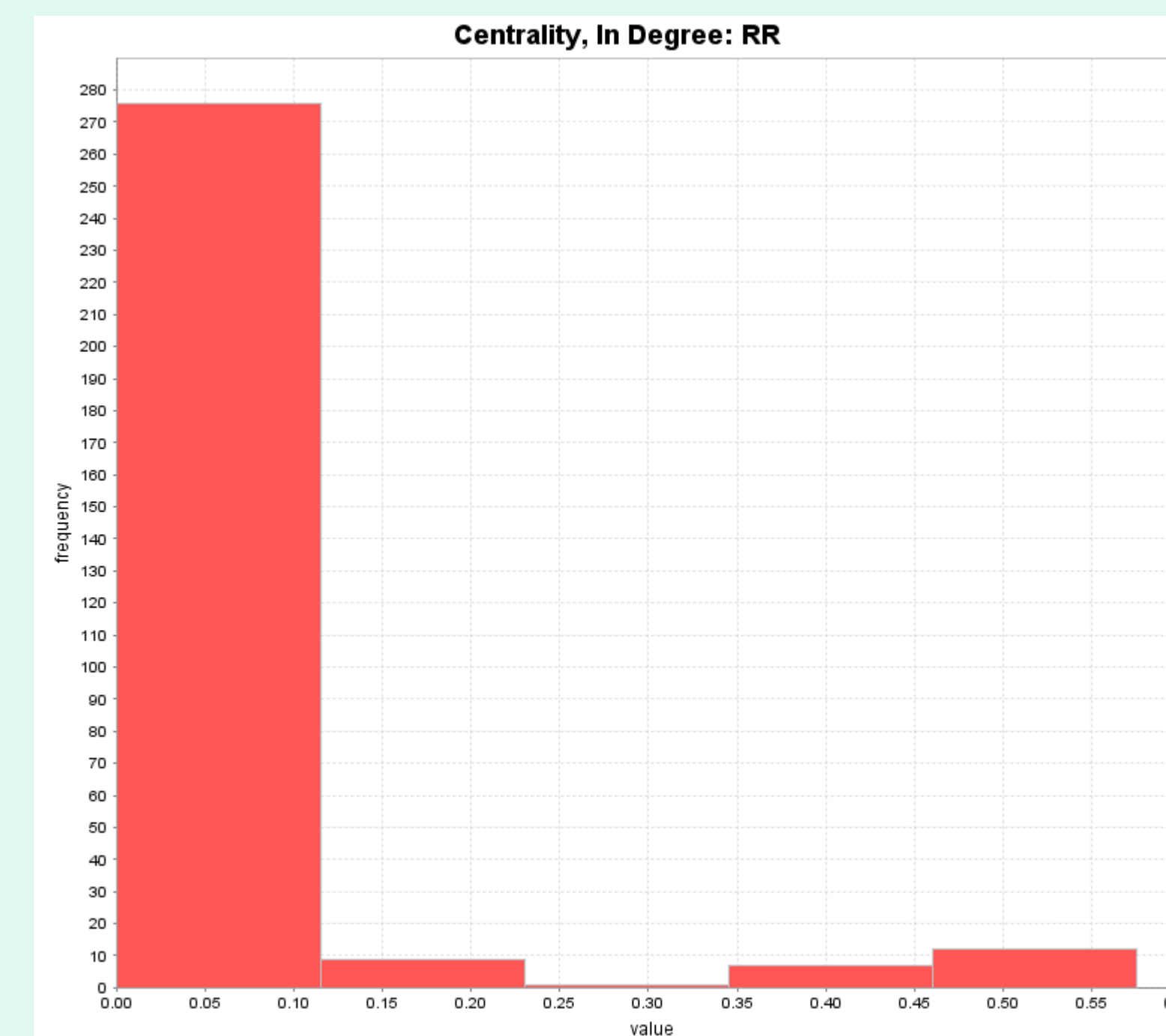
Server Computers Activity

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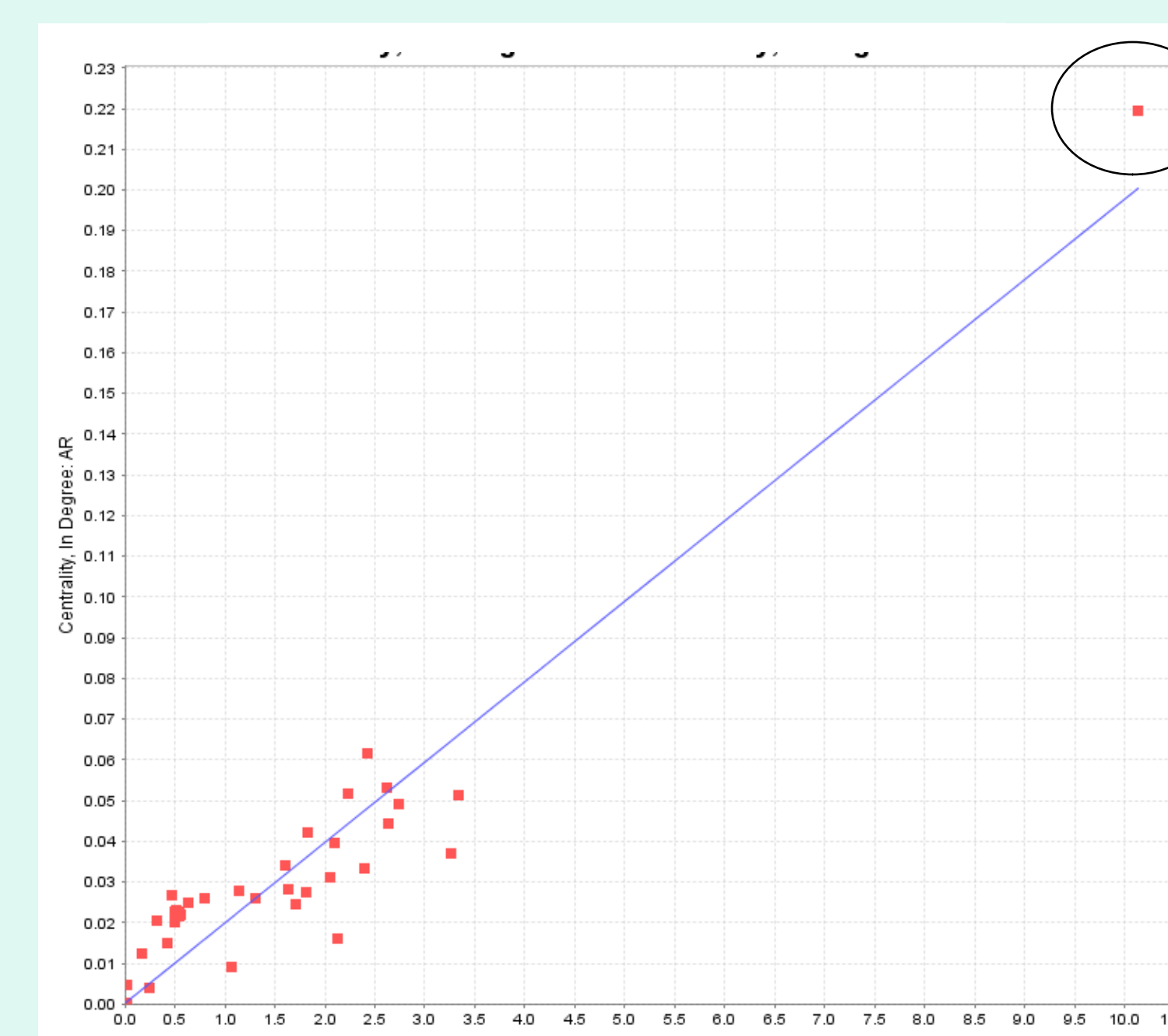an anomaly or rule based intrusion detection system to identify uncharacteristic behavior

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

Users Per Computer

Tasks Per Computer

Users vs. Tasks Comparison

www.casos.cs.cmu.edu

institute for
SOFTWARE
RESEARCH