Communication + Social Network Insider Threat Vulnerability Assessment

Carnegie Mellon
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

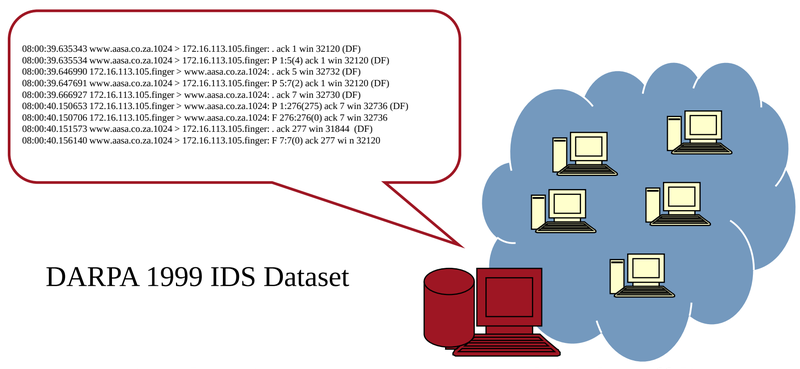
CERT 2004 Report Evaluating Insider Threat Incidents:

83% of incidents at workplace

70% of incidents happened during working hours

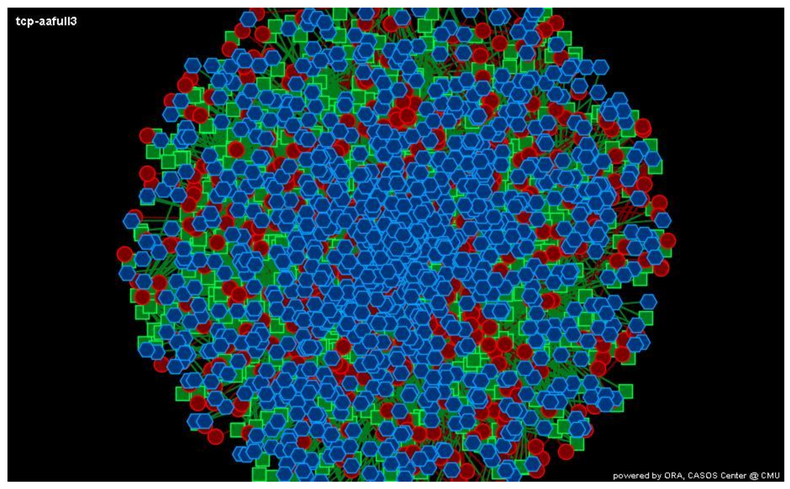
87% of insiders used simple authorized commands

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.



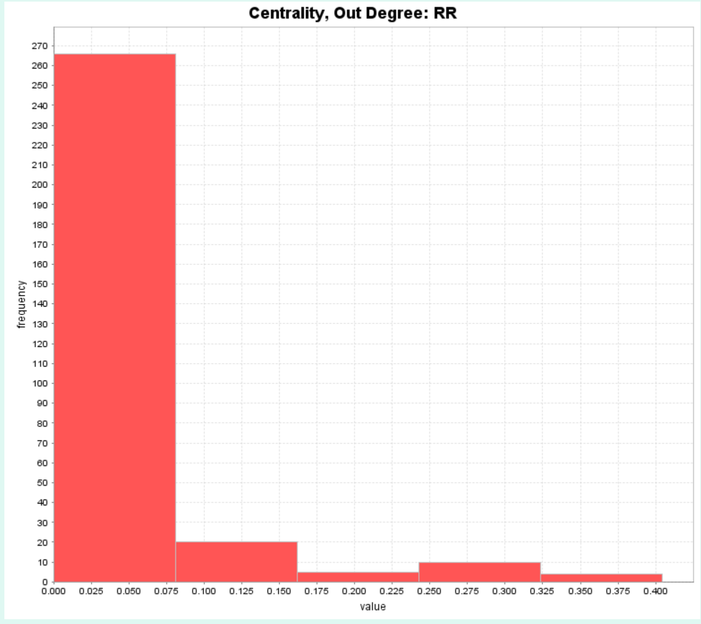
DyNetML Visualization of DARPA 1999 IDS Dataset

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

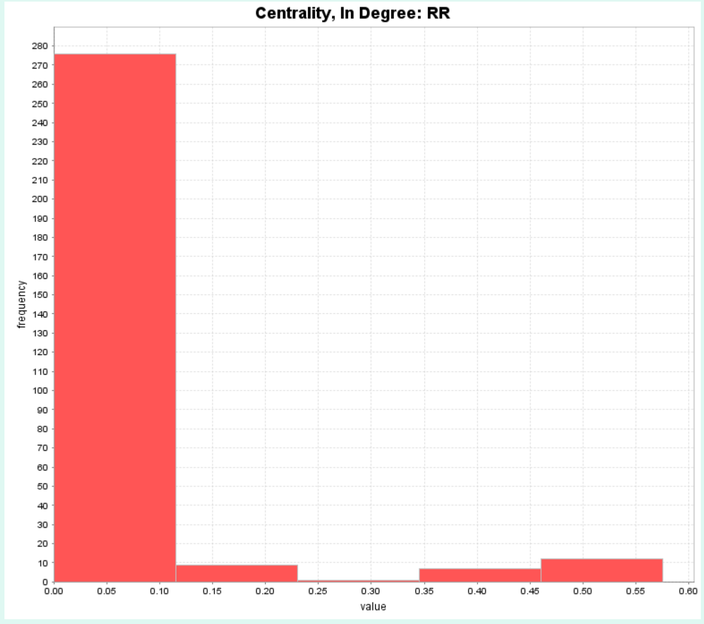
ORA
The Organizational Risk Analyzer

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

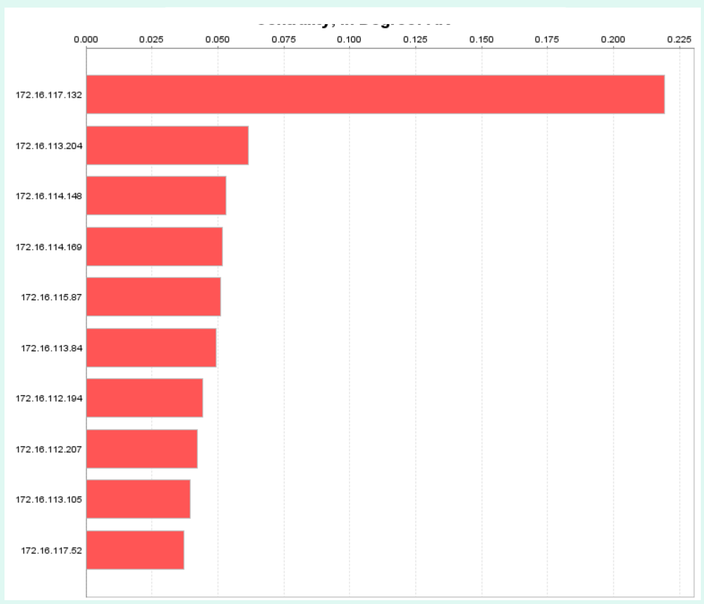


Client Computers Activity

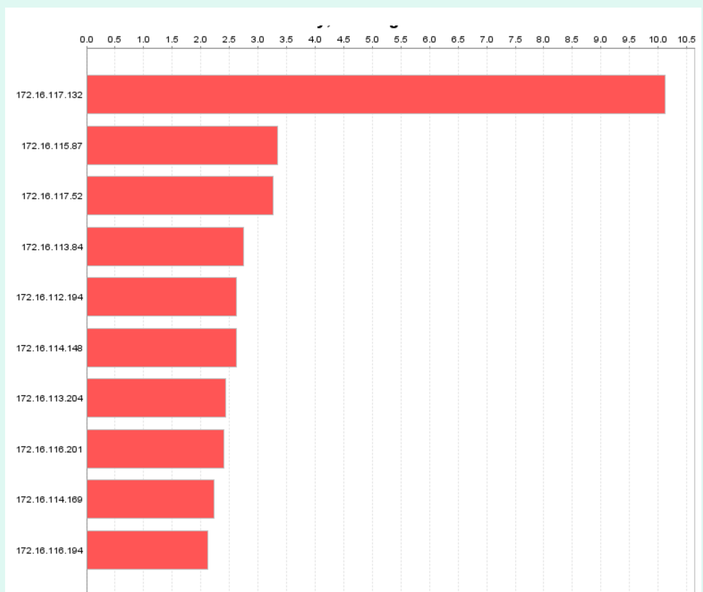


Server Computers Activity

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

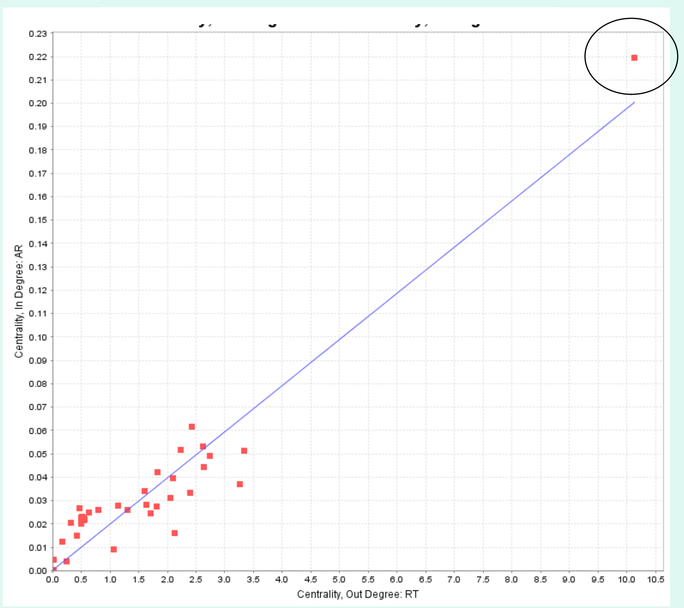


Users Per Computer



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.