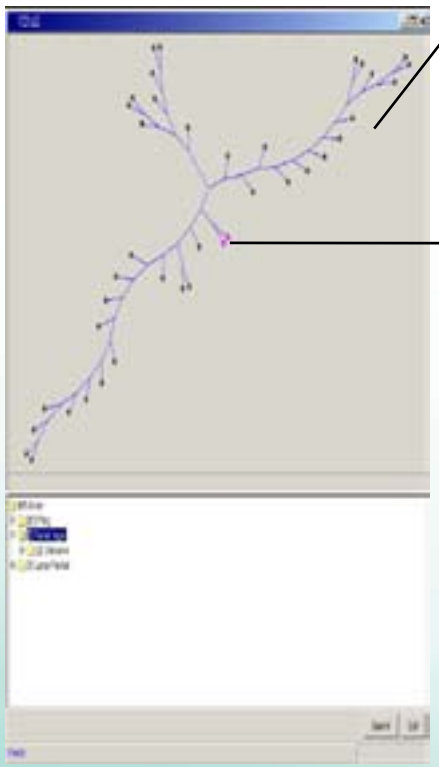
CIPHER: Counterintelligence Penetration Hazard Evaluation and Recognition

Applied Software Engineering Research Group

Computational Sciences & Engineering Division



45 "low and slow" pings from:

Czech Republic, Austria, Hungary, Latvia, France, Chile, and Canada.

2 attacks on nanotechnology scientists

Problem Statement:

- A great deal of very sensitive information (from personal credit card information to nuclear weapons design) resides on a very wide collection of computer networks. Various illicit groups use a wide variety of means (unsophisticated, semi-sophisticated, and highly sophisticated attacks) to gain access to this highly sought after sensitive data. The unsophisticated and semi-sophisticated types of attacks can be easily identified. However, there is no method available to prevent the "low and slow" attacks from sophisticated attackers.

Technical Approach:

- CIPHER analyzes activity against valuable organizational assets, not merely at network packet statistics. We have demonstrated CIPHER using one million suspect records that occur daily on the ORNL networks.

Benefit:

- CIPHER allows us to quickly find potential "low and slow" intrusion attacks from sophisticated attackers.

Point of Contact:

Yu Jiao
(865) 574-0647
jiaoy@ornl.gov

OAK RIDGE National Laboratory