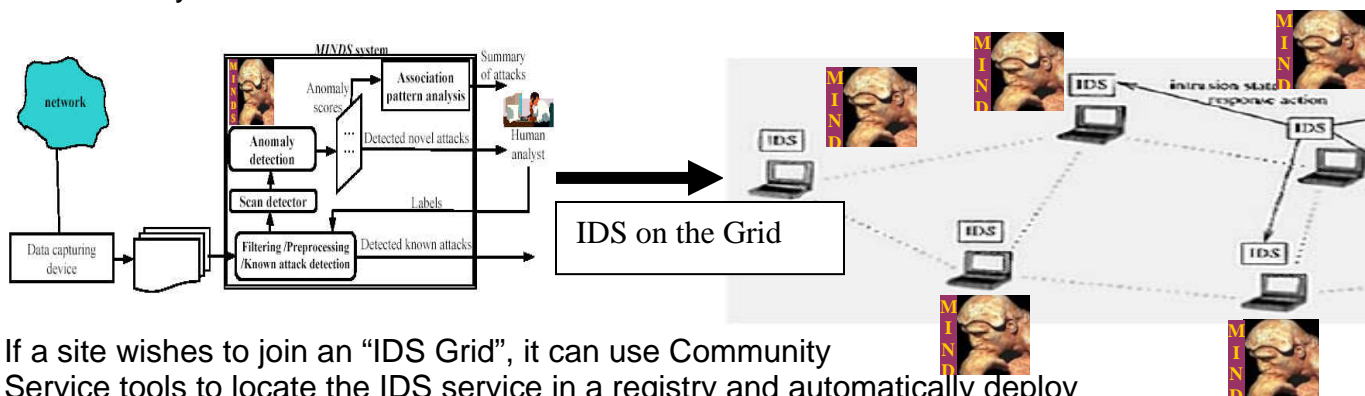


Securing Cyberspace with a little help from my Grids

[reference project: [Community Services, NC middleware project](#)]

Network attacks such as intrusions are increasing with alarming frequency and the discovery of attacks is often done “after-the-fact” by analysis of network logs. Single-site intrusion detection systems such as MINDS (at the University of Minnesota, Kumar, PI) work well but cannot catch sophisticated attacks that involve several sites (using hacked machines to launch subsequent attacks). Researchers at the University of Illinois (Robert Grossman), University of Florida (Sanjay Ranka), and the University of Minnesota (Vipin Kumar), are exploring the concept of distributed network intrusion detection in which network data from multiple sites can be combined and scanned to detect a higher number of attacks, and may be possibly be used to predict future attacks (see below). This kind of collaborative intrusion detection is utilizing middleware technology developed as part of a DOE-funded collaboratory project, Community Services. Community service technology is being used to package existing single-site detection systems (e.g. MINDS) into dynamic Grid services that can be deployed automatically.



If a site wishes to join an “IDS Grid”, it can use Community Service tools to locate the IDS service in a registry and automatically deploy it on a machine in their local network. It can then learn about the other sites (and vice-versa) and subscribe to their intrusion alerts and publish alerts to the IDS Grid. One of the powerful applications is that collective alert information may be used to identify threats that were ignored previously. For example, an event that is below threshold for a single site, but appears at multiple sites, may be signal that it poses a real threat. The Community Service middleware and tools makes it easy for sites to join an IDS Grid. The advantage is that the larger the IDS Grid, the greater the source of shared data that can be used to detect and predict cyber-attacks, as an attack on one site, may presage similar attacks on other sites.

PI, Jon Weissman
Department of Computer Science
University of Minnesota
jon@cs.umn.edu