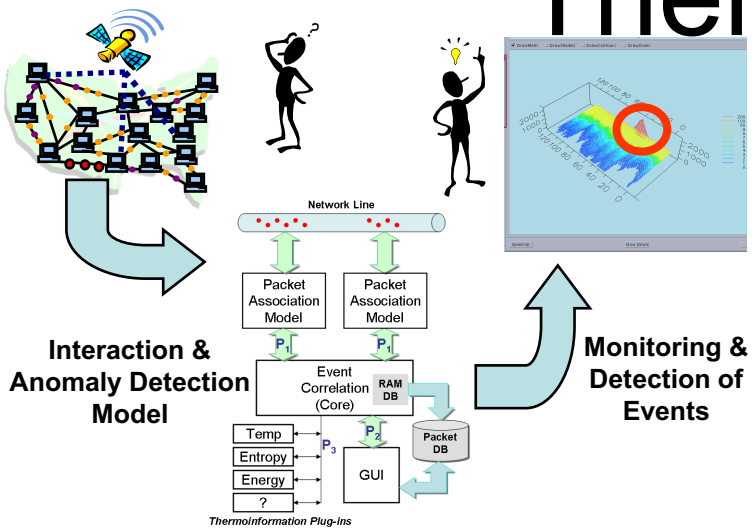
2005-01-05

Therminator

McEachen, John

Therminator



Operational Capability:

- **A radically different approach to DoD's hard Computer Network Defense problem**
- Using real traffic from operational DoD networks this system has identified anomalous patterns associated with network intrusions and multi-pronged network probes
- Thermodynamics-inspired model of conversation exchanges in large-scale distributed networks with high degree of unpredictable interaction patterns
  Novel data reduction attacks a notoriously unsolved problem
- Holistic visualization of large-scale network interaction activity with the ability to trace back to specific host/packet events
  Allows human to see the forest *and* the trees
- Intuitive user interface provides immediate feedback to network admin, analyst, and decision maker **w/ low processing overhead**
  Decreases *data→information→knowledge→decision* loop time

Proposed Technical Approach:

Task 1: Normal Baseline Model Production

- Adapt existing software system for robust and accurate normal network baseline models to permit dynamic adaptation of boundary conditions to normal variations in Internet conditions
- Continue developing analytic framework of thermo-information-based host interaction model compared to classic information theoretic and combinatorial stochastic models

Task 2: Robust System Development and Validation

- Validate and verify the thermoinformation model of virtual entity interaction against real-world threats and anomalies (e.g., MIT LL IDS data set)
- Implement and validate a hardware-based subsystem for monitoring/detection in 1+ Gb/s networks

Rough Order of Magnitude Cost and Schedule:

Task 1: 12 months / ROM cost of $350k
Task 2: 8 months (2 months concurrent w/ Task 1) / ROM cost of $250k
Total ROM schedule/costs: 18 months / $600k

Deliverables:

- Robust network monitoring and anomaly detection software system
- Installation, User, and Programmer Documentation
- Monthly and final technical/progress reports of analytical model, normal baseline model, and verification and validation studies

Contact Information:

Associate Professor John McEachen, Ph.D.
Naval Postgraduate School, Dept. of Electrical and Computer Eng.
Phone: (831) 656-3652, Fax: (831) 656-2760,
Email: mceachen@nps.navy.mil