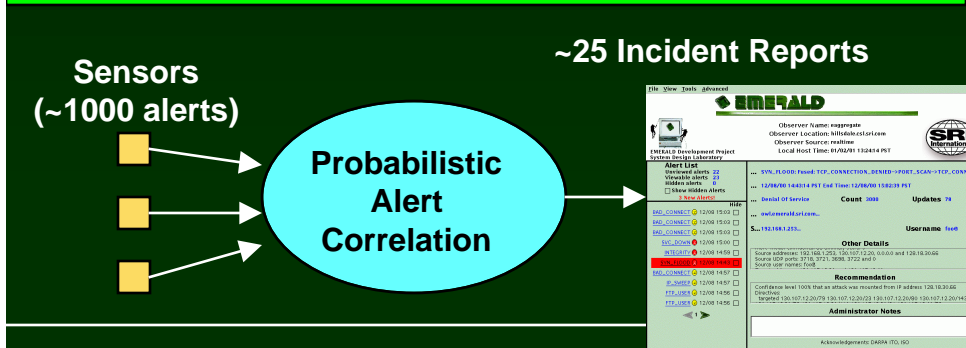
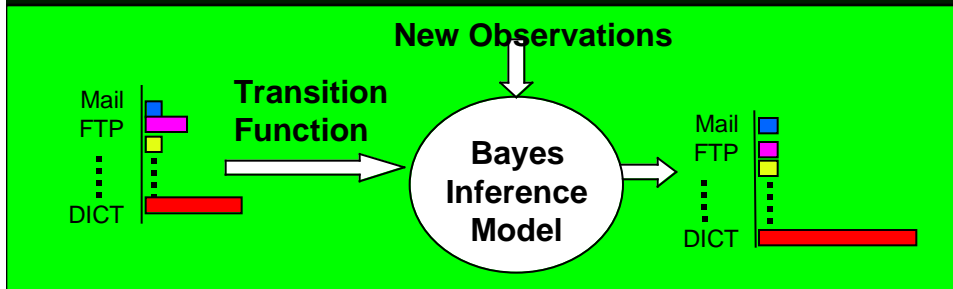


Adaptive Model-Based Monitoring And Threat Detection (EBAYES)



Impact

- Captures desirable features of signature systems (model based) and statistical systems (generalization potential)
- Usable “out of the box”, but adapts to dynamic environment
- Thread, incident, or scenario reconstruction. Up to 50x reduction in alert volume
- Transfer to DARPA ISO, DARPA ITO, DARPA CC2, NSA, etc.



New Technical Ideas

(<http://www.csl.sri.com/intrusion.html>)

- TCP Session monitor encodes knowledge base as Bayes models
- System availability sensor monitors asset distress
- Coupling sensors improves sensitivity at a lower false alarm rate
- Probabilistic alert correlation (new capability in year 2) demonstrates a mathematically rigorous but practical approach to comprehending heterogeneous sensors

Schedule

