CERIAS

the center for education and research in information assurance and security

Runtime Intrusion Diagnosis Under Uncertainty

G. Modelo Howard, Y. Wu, B. Foo, M. Glause, S. Bagchi, G. Lebanon, E. Spafford

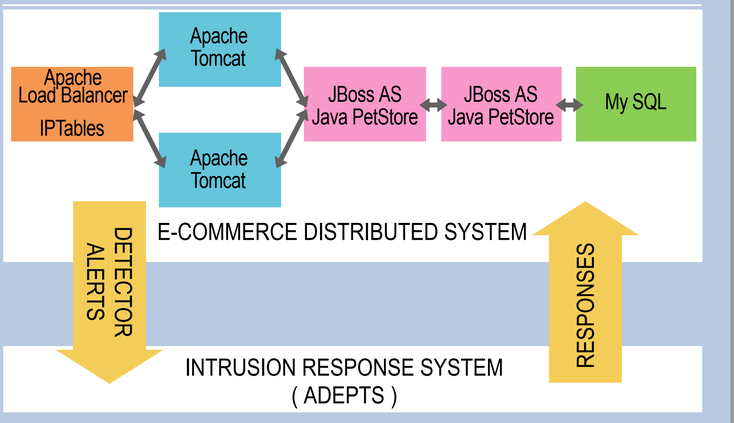
Problem Definition

- **What is diagnosis?**
  - To identify (in runtime) the services that have been affected by an attack
- **Complexity in distributed computing systems and imperfect knowledge of attacks**
- **Necessary to provide runtime diagnosis mechanisms to effectively build robust distributed systems**
- **Based on indeterministic and imperfect properties of systems**

Solution Approach

- **Use the bayesian network model to deal with imperfect detectors and incomplete knowledge base**
- **Organically grow the knowledge representation based on observed attacks**

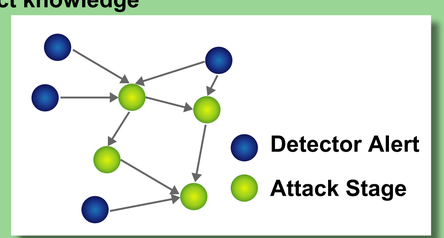
Sample Payload System



- **Web-based e-commerce three-tier server structure**
- **Attacks are performed against the e-commerce system**
- **An intrusion response system, called ADEPTS, provides diagnosis and response mechanism to thwart attacks**

Solution based on Bayesian Networks

- **Bayesian Networks are probabilistic directed acyclical graphs (DAGs) in which:**
  - Nodes represent random variables and
  - Edges represent conditional independence assumptions
- **Application to intrusion diagnosis (and consequential response) with imperfect knowledge**
- **Types of nodes:**
  - Detector Alerts (observed)
  - Attack stages (unobserved)

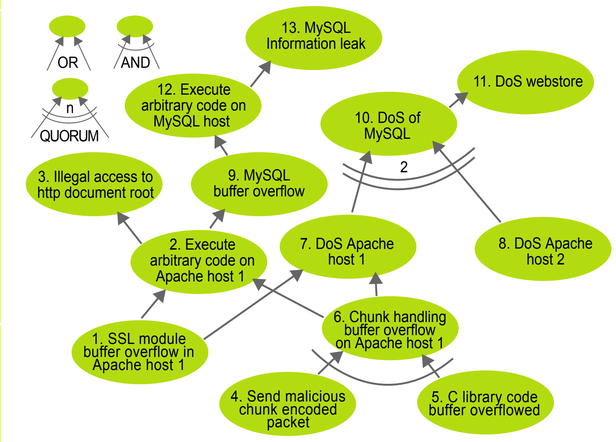


Testbed

- **Bayesian networks are created from**
  - dynamic multi-stage attack scenarios
  - related system detectors
- **Bayesian networks are simulated by using Matlab-based BNT toolkit**

I-Graph

- **Knowledge modeling of multi-stage attacks in the payload system for diagnosis purposes**
- **Each intrusion goal is represented by one node in the graph**
- **Intrusion goals have dependency relationships between one another**
- **Three types of edges**
  - Quorum, defines a minimum number of child nodes to be achieve in order to achieve its parent
  - OR, at least one child node
  - AND, all child nodes

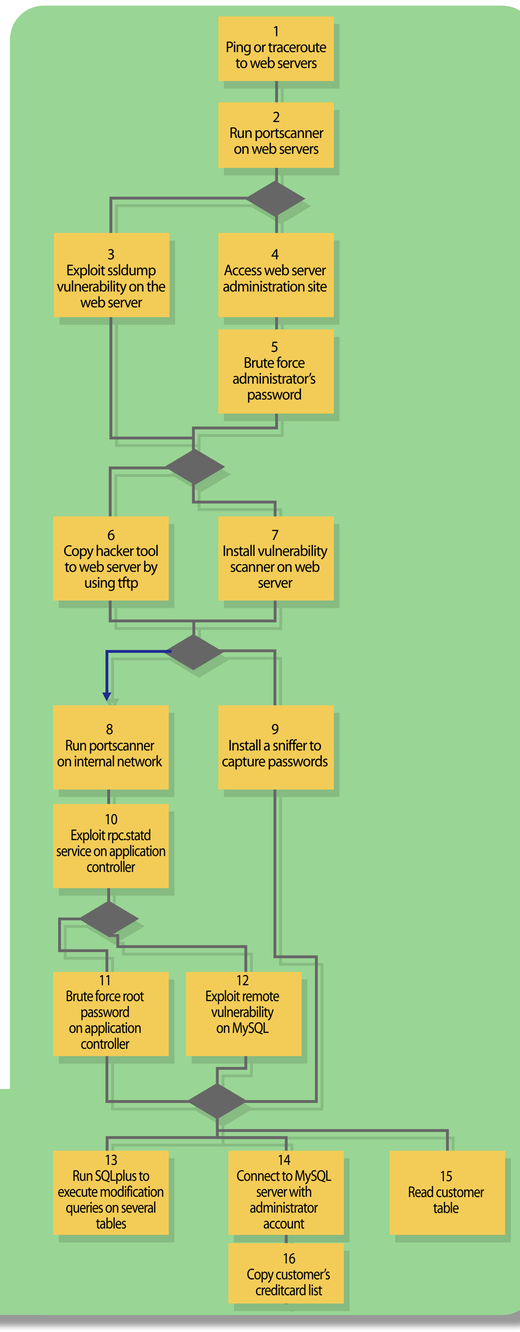


Solution based on I-Graph

- ***Compromised Confidence Index (CCI)***
  - A computation algorithm developed to determine probability of which I-Graph nodes have been achieved
  - Each detector has a confidence value for its alerts
  - A candidate mathematical formulation for the CCI of a node is

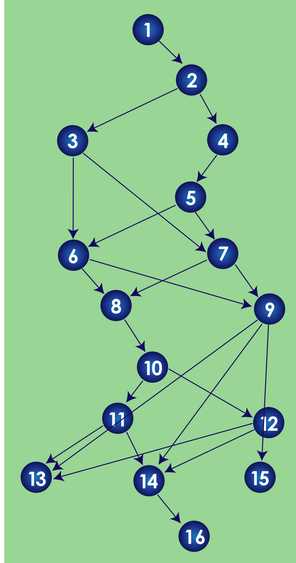
$$CCI = \begin{cases} alertconfidence & \text{,no child} \\ f'(CCI_i) & \text{,no detector } f' = \\ f(f'(CCI_i, alertconf.) & \text{,otherwise} \end{cases} \begin{cases} \max(CCI_i) & \text{,OR edge} \\ \min(CCI_i) & \text{,AND edge} \\ mean(CCI_i) \mid (CCI_i > \tau) & \text{, Quorum edge and quorum met} \\ o & \text{, Quorum edge and quorum not met} \end{cases}$$

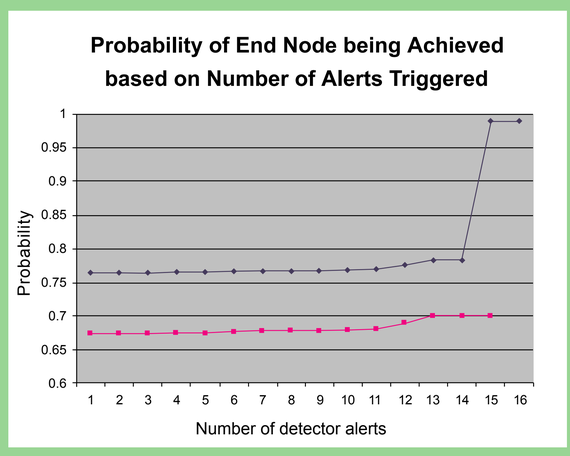
where CCI_i corresponds to the CCI of the i^{th} child and is a per node threshold



Sample Results for Scenario 1

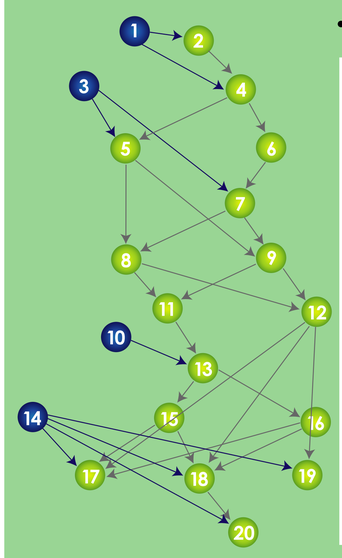
- **All attack nodes have (perfect) detectors**

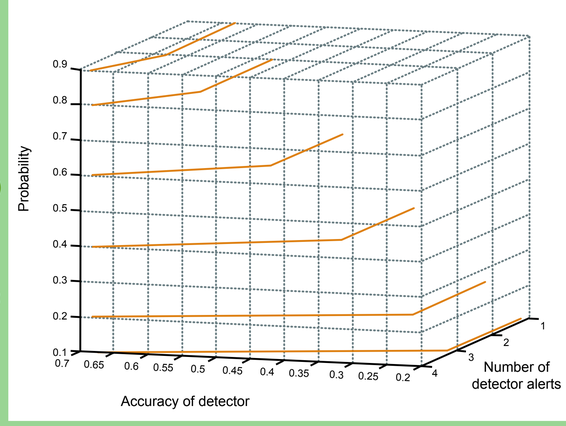




Sample Results for Scenario 2

- **Some attack nodes have (imperfect) detectors**





PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center