CERIAS
The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Secure Configuration of Intrusion Detection Sensors for Changing Enterprise Systems

Gaspar Modelo-Howard, Jevin Sweval, Saurabh Bagchi
Dependable Computing Systems Laboratory

Problem Statement

- We want to know the security state of an enterprise distributed system. For this we need intrusion detection sensors.
- Current state is to treat inputs from individual detectors independently, which misses many distributed multi-stage attacks.

Specific Goals

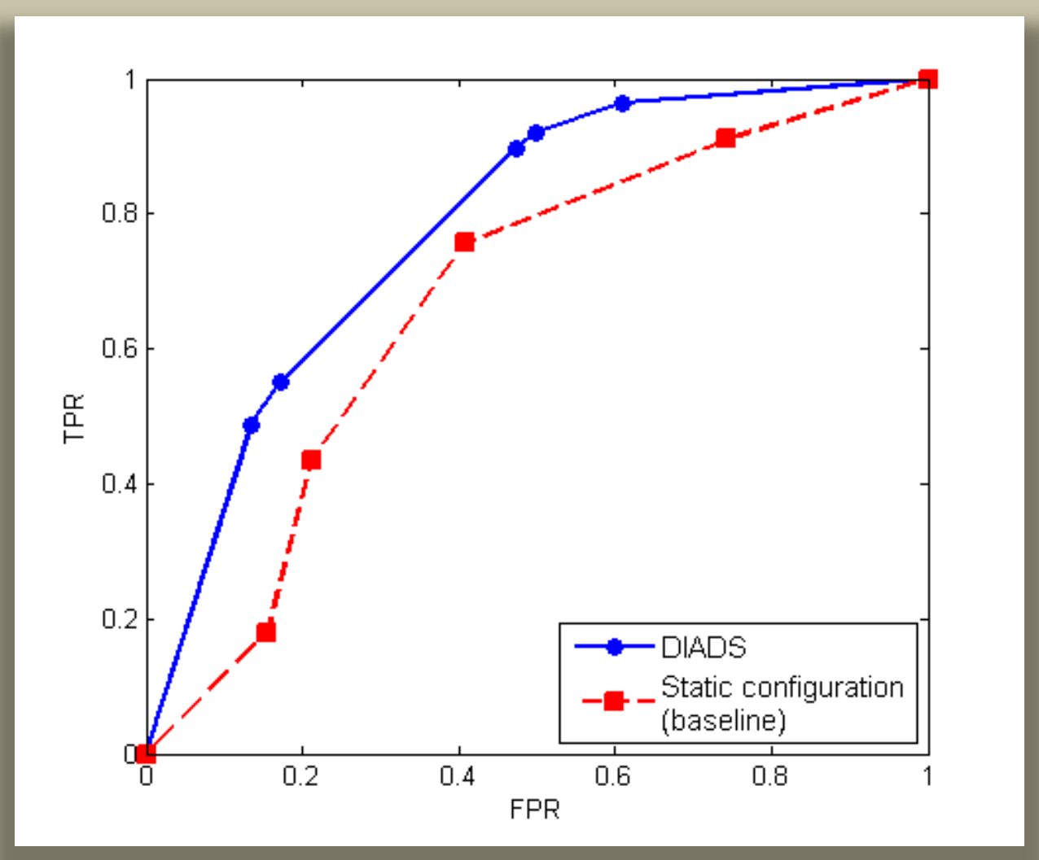
- How to intelligently choose, place, and configure intrusion detection sensors in a distributed enterprise system?
- How to reconfigure initial setup based on runtime information?

Proposed Solution

- Distributed Intrusion Detection System (DIADS) using attack graphs (input) and Bayesian inference (reasoning engine and alert correlation)
- A dynamic programming solution is used for determining the configuration of detection sensors., that can trade off the running time with how close the solution is to the optimal.
- Considers attack origin can be from outside or from inside the periphery.

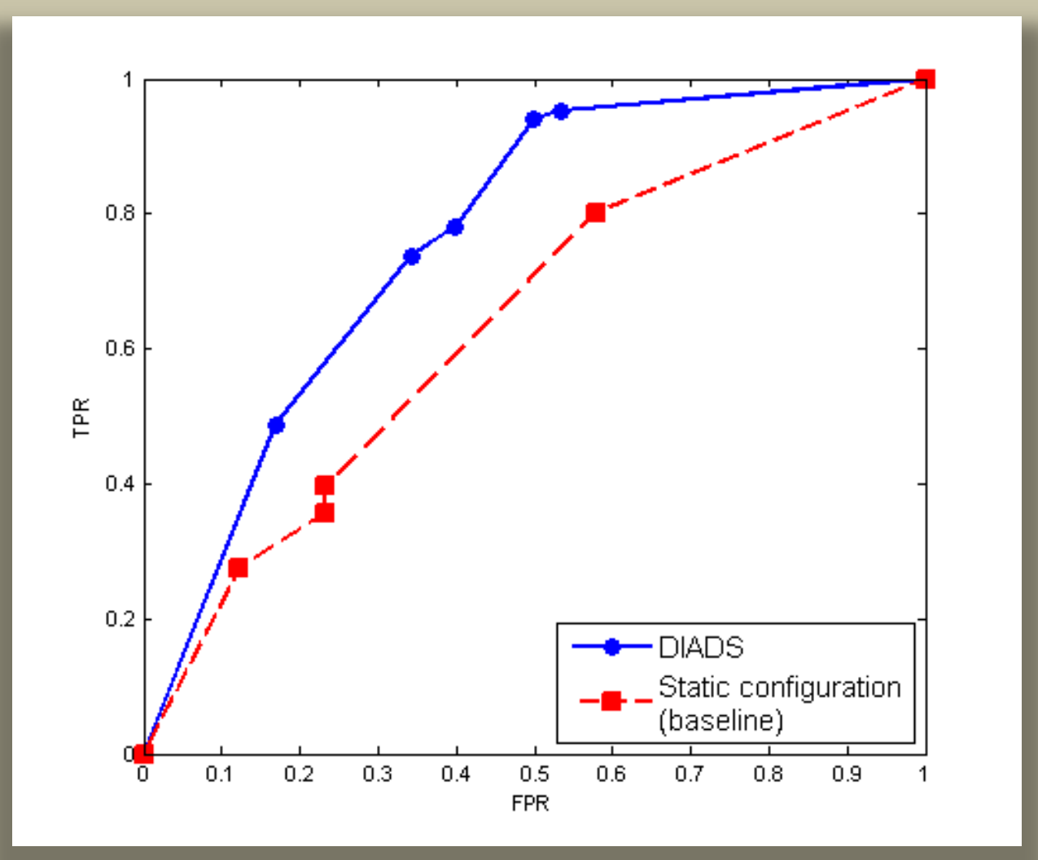
Experimental Results

Dynamic reconfiguration of Detection Sensor



- Comparison between dynamic and static configuration of DIDS, monitoring only database servers. The dynamic setup shows a higher detection rate.

Dynamism from Firewall Rules Changes

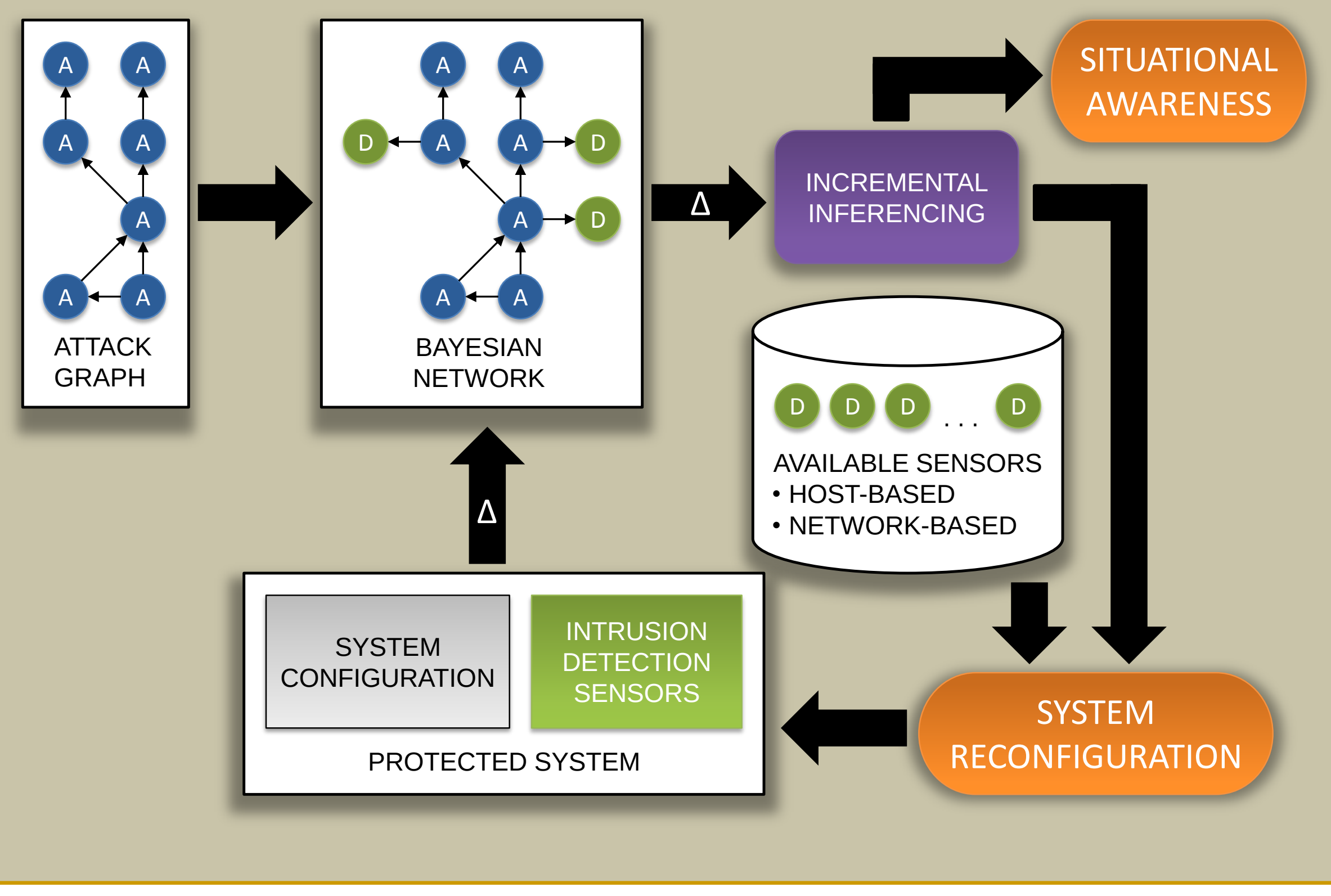


- Impact of topology changes on dynamic and static detection systems after allowing direct access between consultant and database server

Work Ahead

- Generalization of Bayesian network nodes to increase detection scope
- Implementation of DIDS using open-source Bro IDS

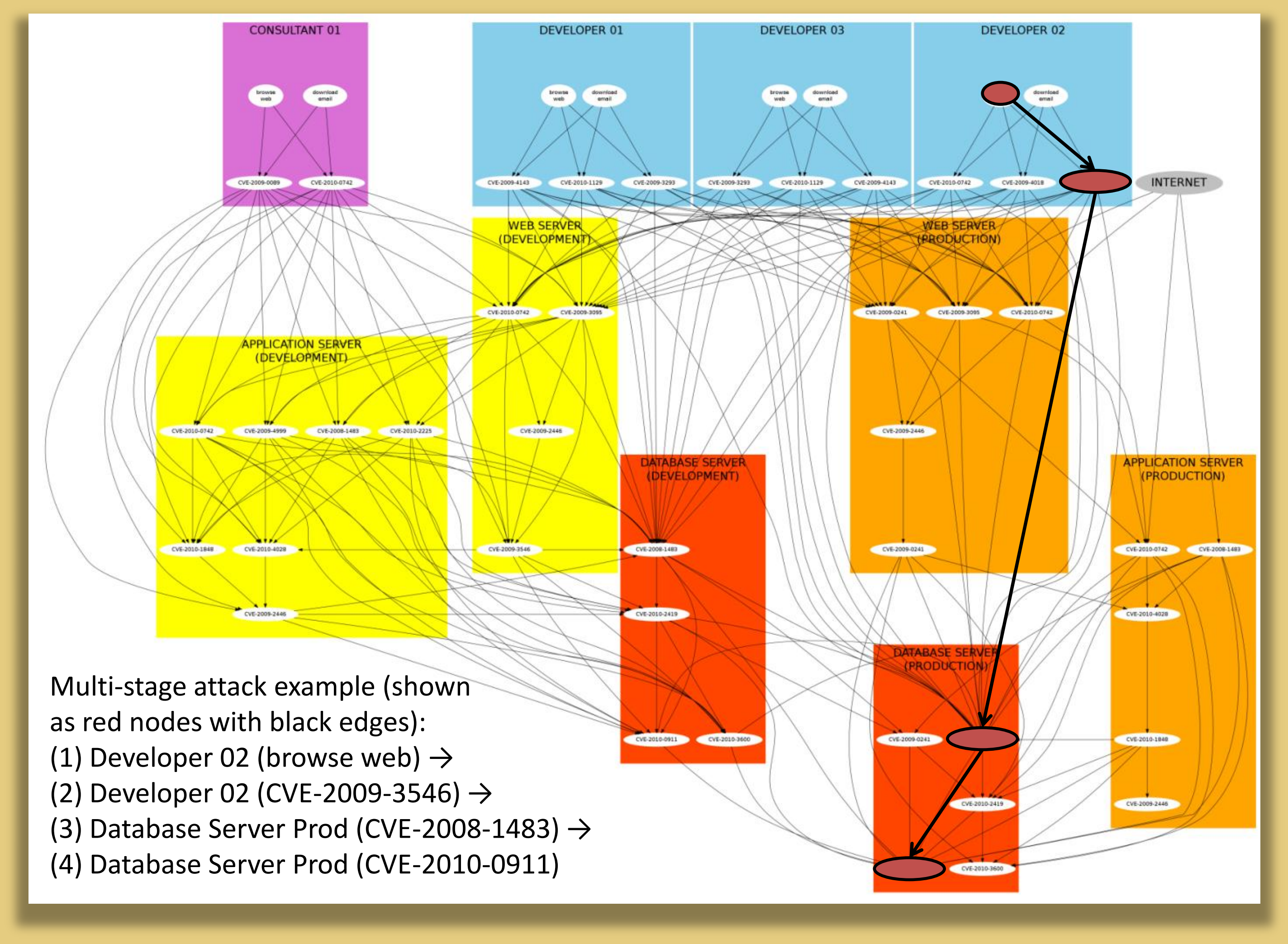
Framework Diagram



Bayesian Network Example

Bayesian network built from real-world distributed system, part of an NSF Center at Purdue

- Communication between hosts is controlled by firewalls
- Database servers are the critical assets to protect


CONSULTANT 01
DEVELOPER 01
DEVELOPER 03
DEVELOPER 02
INTERNET
WEB SERVER (DEVELOPMENT)
WEB SERVER (PRODUCTION)
APPLICATION SERVER (DEVELOPMENT)
DATABASE SERVER (DEVELOPMENT)
APPLICATION SERVER (PRODUCTION)
DATABASE SERVER (PRODUCTION)

Multi-stage attack example (shown as red nodes with black edges):
(1) Developer 02 (browse web) →
(2) Developer 02 (CVE-2009-3546) →
(3) Database Server Prod (CVE-2008-1483) →
(4) Database Server Prod (CVE-2010-0911)

Reference

Modelo-Howard, G., Sweval, J., Bagchi, S.: *Secure Configuration of Intrusion Detection Sensors for Changing Enterprise Systems.* SecureComm 2011.

Project has been conducted under partial funding by Northrop Grumman Information Systems under the Northrop Grumman CyberSecurity Research Consortium.

CERIAS
Discovery Park
e-Enterprise Center