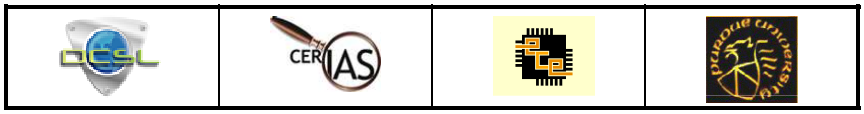
Secure Configuration of Intrusion Detection Sensors for Changing Enterprise Systems

Gaspar Modelo-Howard, Jevin Sweval, Saurabh Bagchi

Presented by Amiya Kumar Maji

Dependable Computing Systems Lab (DCSL) &
Center for Education and Research in
Information Assurance and Security (CERIAS)
School of Electrical and Computer Engineering
Purdue University



PURDUE UNIVERSITY

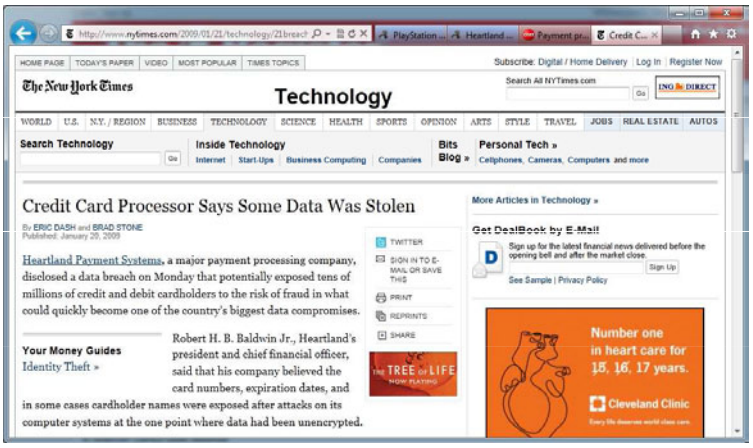
Motivation: MSA

- Current attacks to distributed systems involve multiple steps (**MSA: Multi-Stage Attacks**)
  - Ultimate goal is to compromise a critical asset
  - Prior to compromising the critical asset, multiple components are compromised

PURDUE UNIVERSITY

Motivation: MSA

- Current detection systems are not capable of analyzing MSA scenario
  - Example: breach to Heartland Payment Systems (2009)

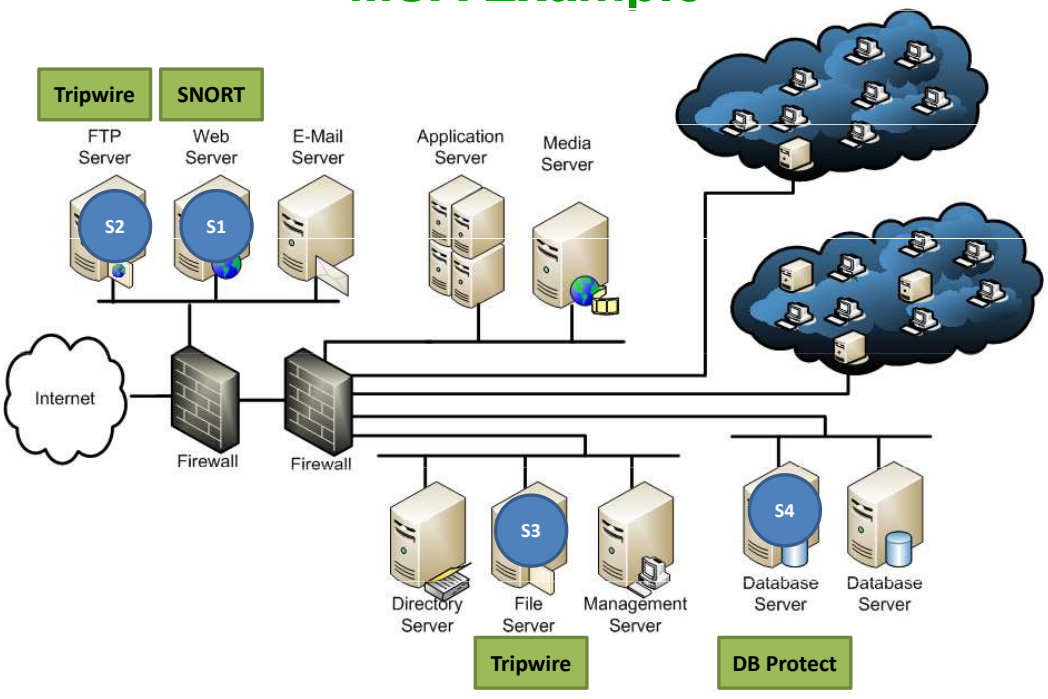


Credit Card Processor Says Some Data Was Stolen

Heartland Payment Systems, a major payment processing company, disclosed a data breach on Monday that potentially exposed tens of millions of credit and debit cardholders to the risk of fraud in what could quickly become one of the country's biggest data compromises.

Robert H. B. Baldwin Jr., Heartland's president and chief financial officer, said that his company believed the card numbers, expiration dates, and in some cases cardholder names were exposed after attacks on its computer systems at the one point where data had been unencrypted.

MSA Example



Motivation: Dynamism

- Distributed system **changes over time**
  - Static configuration for detection system could miss new (known) attacks possible in the changed configuration as well as throw off false alarms (FP)
  - Existing knowledge of the IDS needs to be updated
- Attacks **change over time**
  - Static configuration of IDS is not going to be useful

Contributions

- We design a distributed intrusion detection system (DIADS) that can choose and place sensors in a distributed system
- We imbue our solution with the ability to evolve with
  - changes to the protected system and
  - the kinds of attacks seen in the system
- Through domain-specific optimizations, we make our reasoning engine fast enough to perform reconfiguration of existing sensors in light of MSA

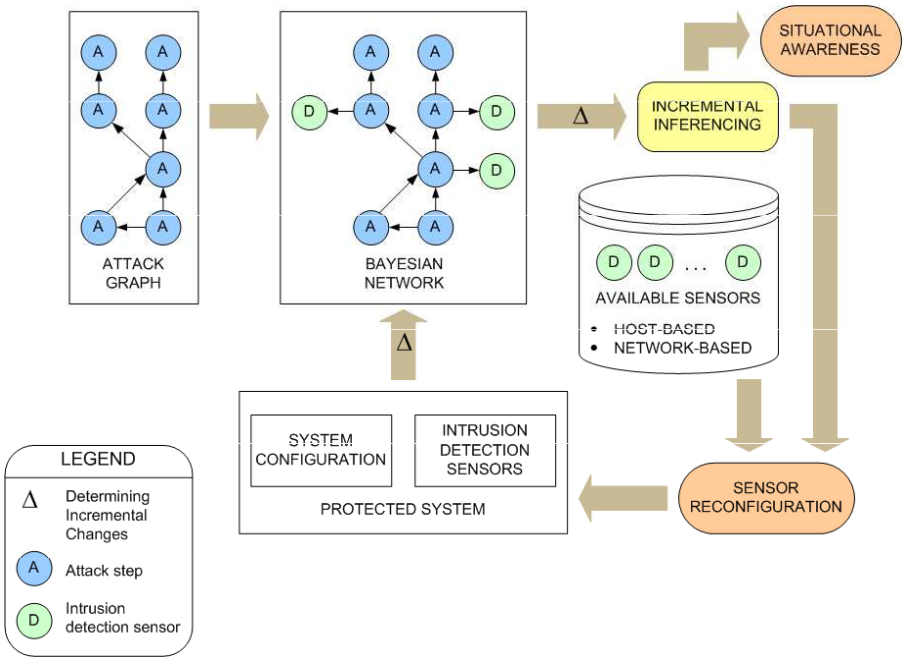
Agenda

- Motivation
- Contributions
- Threat Model
- Proposed Method
- Experiments
- Conclusions and Future Work

Threat and System Model

- Single administrative domain
- Attackers follow a MSA approach to compromise a critical asset
  - Bots/Malware can also follow the MSA approach
  - We do not address physical attacks (using a USB memory stick to steal data)
- We do not preclude having sensors that detect attacks at other assets
  - DIADS incorporates existing ID sensors
  - DIADS provides inference engine to receive input from ID sensors

Overview of Approach



Bayesian Network Modeling

Attack Node = <host, port, vulnerability>

Attack Node

pscan
0.1

Detector Node

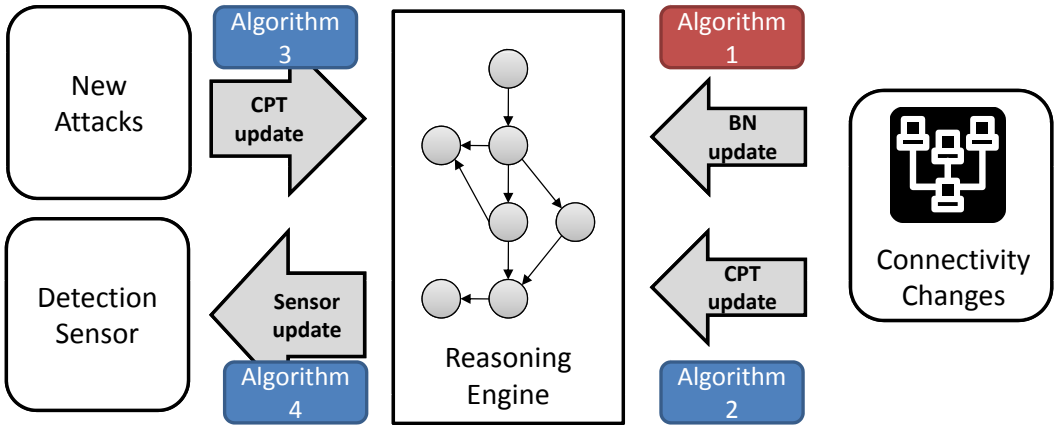
CPT

	snort
SSL	TP
$\overline{\text{SSL}}$	1-TN

CPT

	SSL
pscan	0.9
$\overline{\text{pscan}}$	0.7

Handling Changes to Protected System and Attack Scenarios



CPT = Conditional Probability Table; BN = Bayesian Network

- Our solution fits within the context of a security architecture already deployed in the system, which includes intrusion detection sensors and firewall

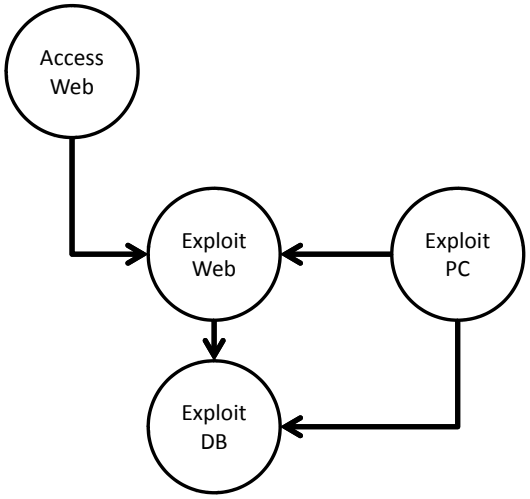
Algorithm 1: Update BN based on Firewall Rule Changes (1)

- INPUT: We use changes to FW rules as proxy for changes to monitored system
  - `Message = < number, srcIPaddr, destIPaddr, portnumber, action, ruletype >`
- OUTPUT: List of nodes and edges that should be added or deleted from Bayesian network
  - Represents changes to monitored system
- Algorithm can be divided into four phases
  - Determine nodes and edges to be added
  - Determine nodes and edges to be deleted
  - Checking for cycles from changes (Depth First Search)
  - Converting `destIPaddr:port` nodes into corresponding BN nodes (`address:port:vulnerability`)

Algorithm 1: Sample Scenario

No.	Source	Destination	Action
1	Any	Web:80	Allow
2	Web	DB:3306	Allow
3	Web	DB:22	Allow
4	DB	Web:22	Allow
5	PC	DB:3306	Allow
6	PC	DB:22	Allow
7	Any	FTP:21	Allow
8	Any	Any	Deny

(a) Firewall rule table



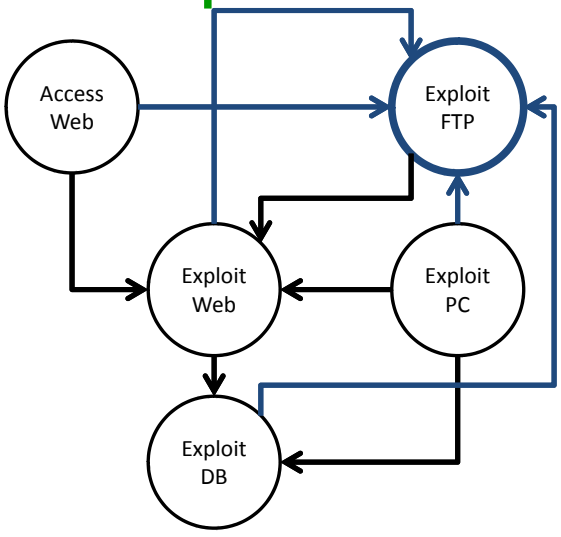
(b) Bayesian Network (1. Previous Network)

- New rule (7) in FW changes topology of Bayesian network
- 2 of 5 potential new edges will not make it to final update since they create a cycle

Algorithm 1: Sample Scenario

No.	Source	Destination	Action
1	Any	Web:80	Allow
2	Web	DB:3306	Allow
3	Web	DB:22	Allow
4	DB	Web:22	Allow
5	PC	DB:3306	Allow
6	PC	DB:22	Allow
7	Any	FTP:21	Allow
8	Any	Any	Deny

(a) Firewall rule table



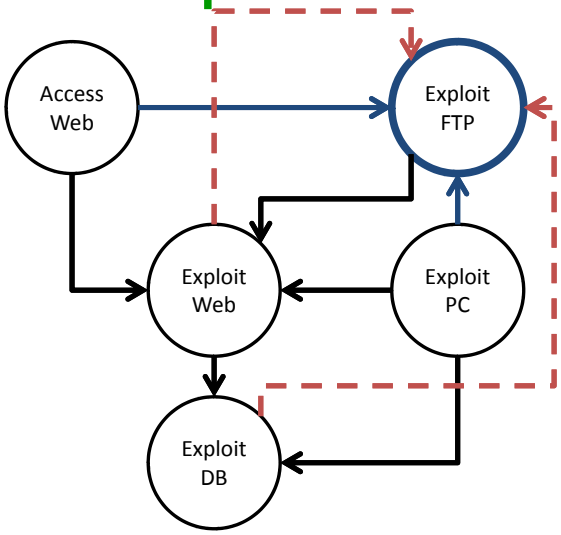
(b) Bayesian Network (2. Add Edges from New Rule)

- New rule (7) in FW changes topology of Bayesian network
- 2 of 5 potential new edges will not make it to final update since they create a cycle

Algorithm 1: Sample Scenario

No.	Source	Destination	Action
1	Any	Web:80	Allow
2	Web	DB:3306	Allow
3	Web	DB:22	Allow
4	DB	Web:22	Allow
5	PC	DB:3306	Allow
6	PC	DB:22	Allow
7	Any	FTP:21	Allow
8	Any	Any	Deny

(a) Firewall rule table



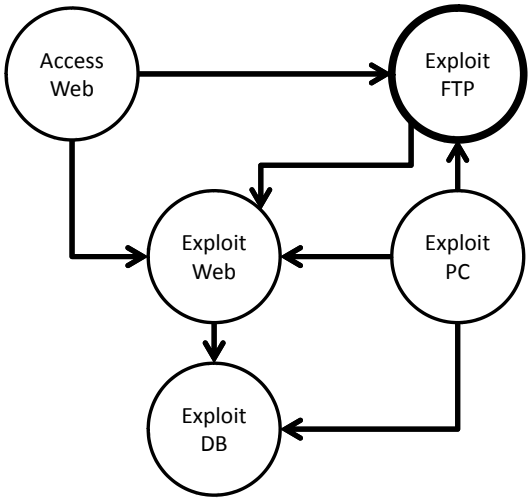
(b) Bayesian Network (3. Identify Cycles using DFS)

- New rule (7) in FW changes topology of Bayesian network
- 2 of 5 potential new edges will not make it to final update since they create a cycle

Algorithm 1: Sample Scenario

No.	Source	Destination	Action
1	Any	Web:80	Allow
2	Web	DB:3306	Allow
3	Web	DB:22	Allow
4	DB	Web:22	Allow
5	PC	DB:3306	Allow
6	PC	DB:22	Allow
7	Any	FTP:21	Allow
8	Any	Any	Deny

(a) Firewall rule table

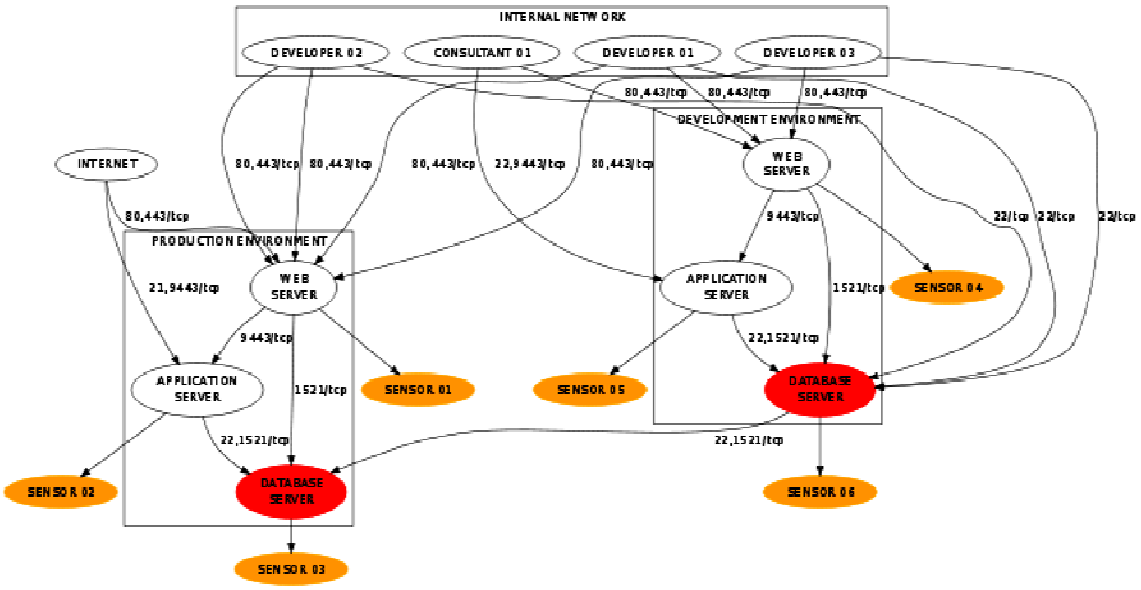


(b) Bayesian Network (4. Remove Cyclic Edges)

- New rule (7) in FW changes topology of Bayesian network
- 2 of 5 potential new edges will not make it to final update since they create a cycle

Experimental Setup (1)

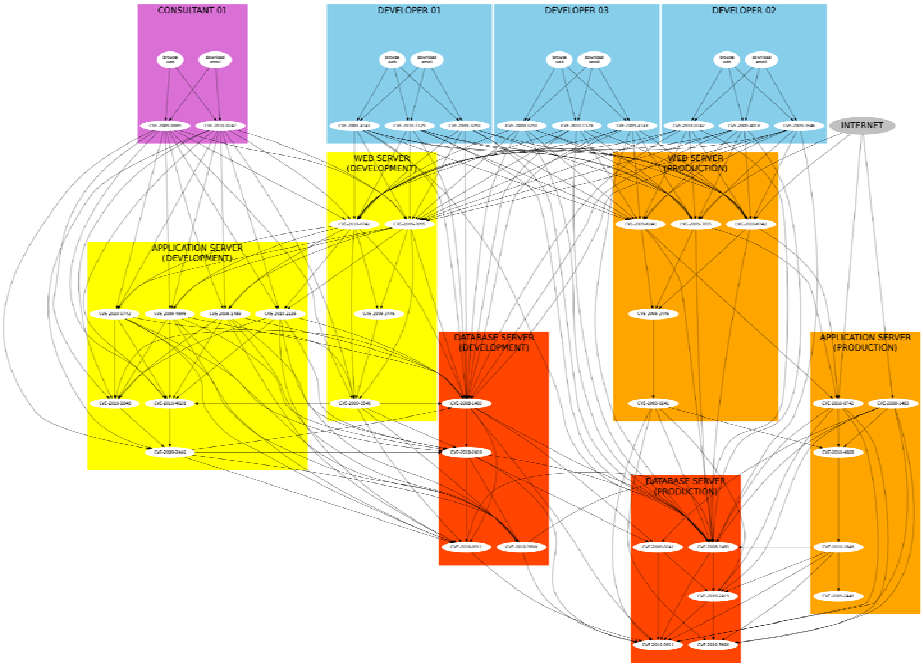
- Used real-world distributed system which is part of an NSF Center at Purdue



Experimental Setup (2)

- Bayesian network was created from real-world distributed system which is part of an NSF Center at Purdue
  - Corresponding vulnerabilities generated from using the OpenVAS (old Nessus) vulnerability scanner
  - BN was pruned to include high risk vulnerabilities
  - Final BN had 90 nodes and 582 edges
  - 18 possible detectors, constrained algorithm to pick 6
- Compared results between DIADS and a static/heuristic driven choice of sensors
- DIADS' goal is to improve performance of set of detectors

Experimental System: Structure of Bayesian Network

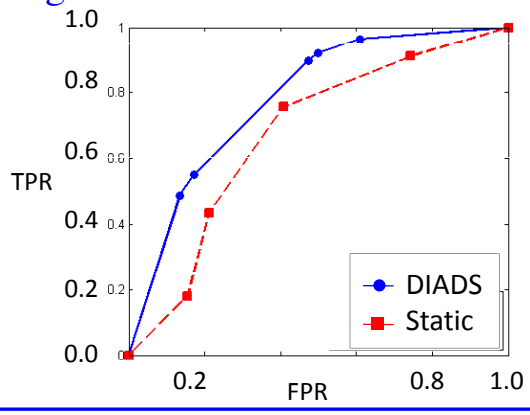


Multi-Stage Attack Scenarios

- Five attack scenarios were used for the experiments
  - Each step in an attack scenario corresponds to a node in the Bayesian network
  - Each attack scenario has an end goal (node) representing a vulnerability in the critical asset of the testing system
  - Each node has a code (CVE-year-number) corresponding to the code assigned for the particular vulnerability, as defined in NVD
- Examples of attack scenarios
  1. Internet → Web Prod (CVE-2010-0742) → App Prod (CVE-2010-0742) → App Prod (CVE-2010-4028) → App Prod (CVE-2010-1848) → DB Prod (CVE-2010-2419)
  2. Developer 01 (download email) → Developer 01 (CVE-2009-4143) → Web Develop (CVE-2010-0742) → App Develop (CVE-2009-3546) → DB Develop (CVE-2010-2419) → DB Develop (CVE-2010-0911)

Experimental Results

- Dynamic reconfiguration of Detection Sensor
  - Compare performance between dynamic reconfiguration and a static set of detectors (all around the critical asset)
  - Set of alerts for first three attack steps given to DIADS for reconfiguration of sensors

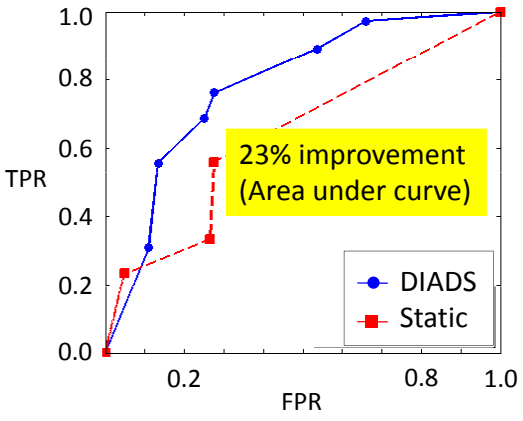


16% improvement
(Area under curve)

Experimental Results

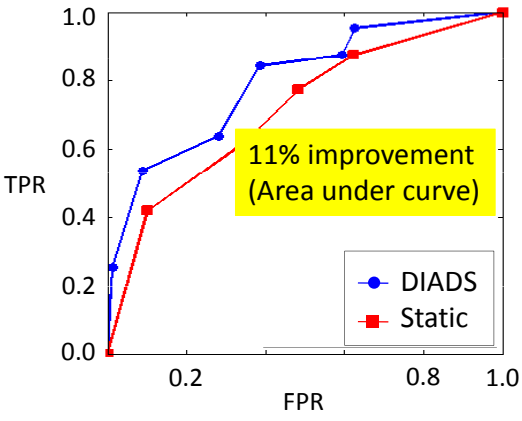
- Dynamism with Attack Spreading
  - Reconfigure sensors on the fly
  - Tested performance of DIADS and static setups

(1) Attack from the Internet



23% improvement
(Area under curve)

(2) Opening ports to DB server



11% improvement
(Area under curve)

Conclusions and Future Work

- Design of a distributed intrusion detection system (DIADS) that detects MSA and tunes sensors according to changing environment of system monitored
  - Reconfiguration of sensors allows to detect attacks that take advantage of changing environment
- Experiments show reduction in number of FP when considering dynamism of monitored system
- Future work will include experimenting further with size of Bayesian network and exploring impact of evasion techniques targeted against DIADS

THANK YOU! QUESTIONS?