REGARD: Rules of Engagement for Automated Cyber Defense Agents

Dr. Benjamin Blakely, Argonne National Laboratory

Dr. Sudip Mittal, Assistant Professor, Computer Science & Engineering, Mississippi State University

Damodar Panigrahi, PhD Computer Science & Engineering, Mississippi State University

William Anderson, MS Computer Science & Engineering, Mississippi State University

Joshua Whitman, MS in Cybersecurity, Mississippi State University

Argonne NATIONAL LABORATORY

INSuRE

STATE MISSISSIPPI STATE UNIVERSITY™

Agenda

- Motivation
- Background
- REGARD (Rules of Engagement for Automated Cyber Defense Agents) Preliminary System
    - Framework
    - Architecture
    - Implementation
- REGARD-GNN System
    - Framework
    - Architecture
    - Implementation
- Conclusion & Future Work

Background - Intrusion Response Systems (IRS)

❑ Cyber attacks are increasingly:

  ❑ Polymorphic, Zero-day, Sophisticated, Automated

❑ Disruption increasingly effective

❑ Automated agents increasingly necessary to keep pace

- Designed to identify a proper response to an ongoing attack *automatically*.
- Goal is to identify strategies and compute an Intrusion Response.

○ *How can the system be protected?*

○ *Can the attack be handled in such a way that the damage is minimized?*

○ *How to constrain action? What are the Rules of Engagement?*

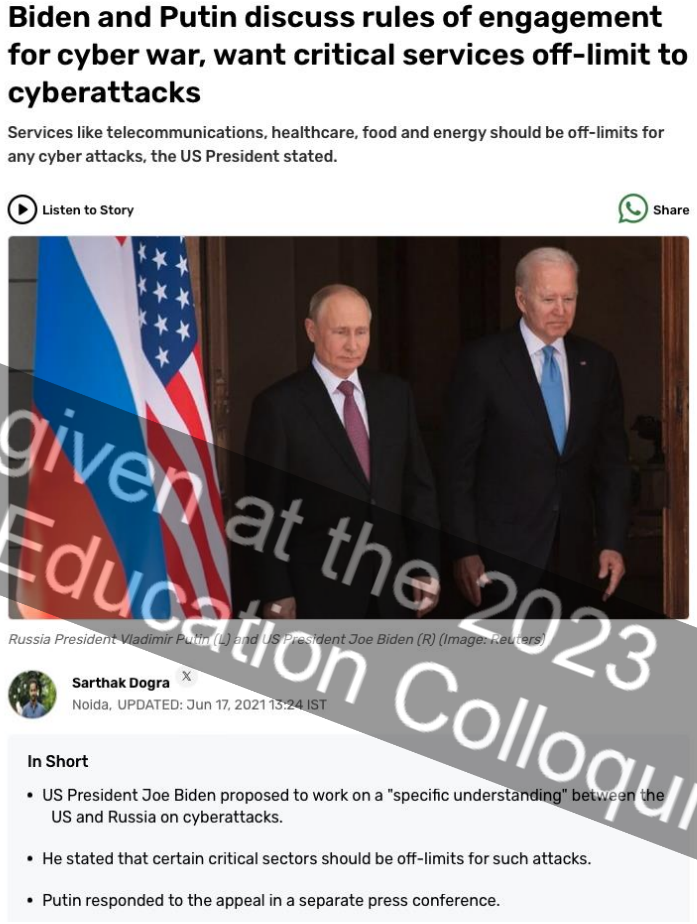
Background - Rules of Engagement (RoEs)

Warfare RoEs are military directives meant to describe the circumstances under which ground, naval, and air forces will enter into and continue combat with opposing forces.

- United Nations Rules of Engagement
- United States Department of Defense’s rules of engagement (both standing peacetime ROE (SROE), and wartime ROE (WROE))

Rules of Engagement for Cyber War

-Still in Development!



Biden and Putin discuss rules of engagement for cyber war, want critical services off-limit to cyberattacks

Services like telecommunications, healthcare, food and energy should be off-limits for any cyber attacks, the US President stated.

Russia President Vladimir Putin (L) and US President Joe Biden (R) (Image: Reuters)

Sarthak Dogra

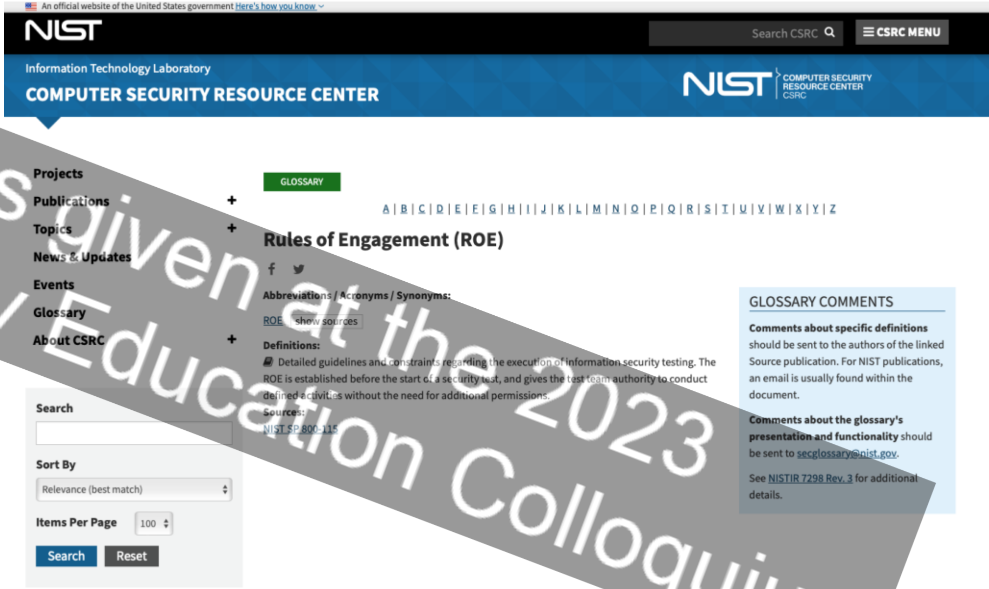
Noida, UPDATED: Jun 17, 2021 13:24 IST

In Short

- US President Joe Biden proposed to work on a "specific understanding" between the US and Russia on cyberattacks.
- He stated that certain critical sectors should be off-limits for such attacks.
- Putin responded to the appeal in a separate press conference.

RoEs for Cyber Defense & Response Systems

"Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions." - NIST


An official website of the United States government Here's how you know
NIST
Search CSRC
☰ CSRC MENU
Information Technology Laboratory
COMPUTER SECURITY RESOURCE CENTER
NIST COMPUTER SECURITY RESOURCE CENTER CSRC
Projects
Publications +
Topics +
News & Updates
Events
Glossary
About CSRC +
Search
Sort By
Relevance (best match)
Items Per Page
100
Search
Reset
GLOSSARY
A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

Rules of Engagement (ROE)

Abbreviations / Acronyms / Synonyms:

ROE show sources

Definitions:

Detailed guidelines and constraints regarding the execution of information security testing. The ROE is established before the start of a security test, and gives the test team authority to conduct defined activities without the need for additional permissions.

Sources:

NIST SP 800-115

GLOSSARY COMMENTS

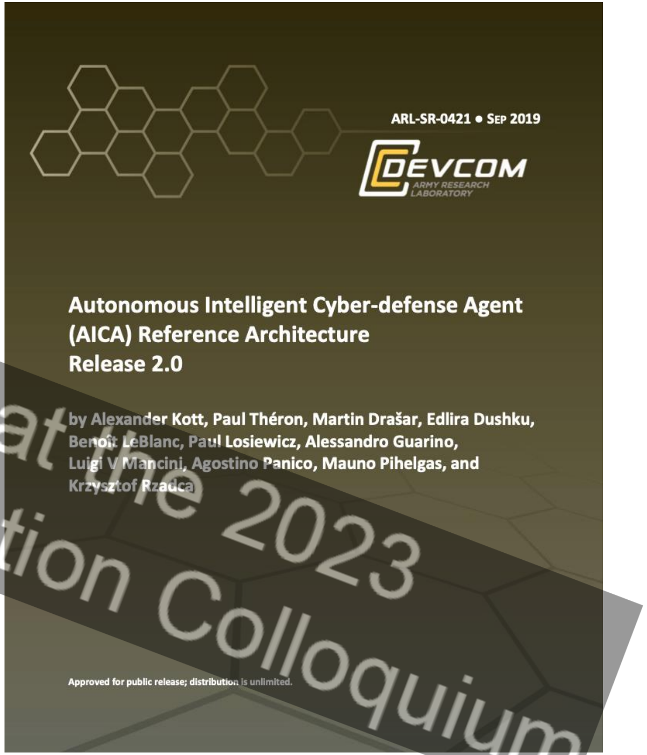
Comments about specific definitions should be sent to the authors of the linked Source publication. For NIST publications, an email is usually found within the document.

Comments about the glossary's presentation and functionality should be sent to secglossary@nist.gov.

See NISTIR 7298 Rev. 3 for additional details.

Background - AICA

- Automated Intelligent Cyberdefense Agents (AICAs)
    - Self-Adaptive Autonomic Computing Systems (SA-ACS)
        - *Kephart, J. and David M. Chess. "The Vision of Autonomic Computing." Computer 36 (2003): 41-50.*
        - MAPE-K Framework (Monitor, Analyze, Plan, Execute, and Knowledge)
- Automated, constrained response based on **Rules of Engagement** (ROE)
    - Inspiration from United States Department of Defense ROE
        - Standing Rules of Engagement (SROE)
        - Wartime Rules of Engagement (WROE)



ARL-SR-0421 • Sep 2019

DEVCOM ARMY RESEARCH LABORATORY

Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture Release 2.0

by Alexander Kott, Paul Théron, Martin Drašar, Edlira Dushku, Benoît LeBlanc, Paul Losiewicz, Alessandro Guarino, Luigi V Mancini, Agostino Panico, Mauno Pihelgas, and Krzysztof Rzadca

Approved for public release; distribution is unlimited.

REGARD: Rules of EngaGement for Automated cybeR Defense to aid in Intrusion Response

Damodar Panigrahi
Mississippi State University
Mississippi State, MS, USA
dp1657@msstate.edu

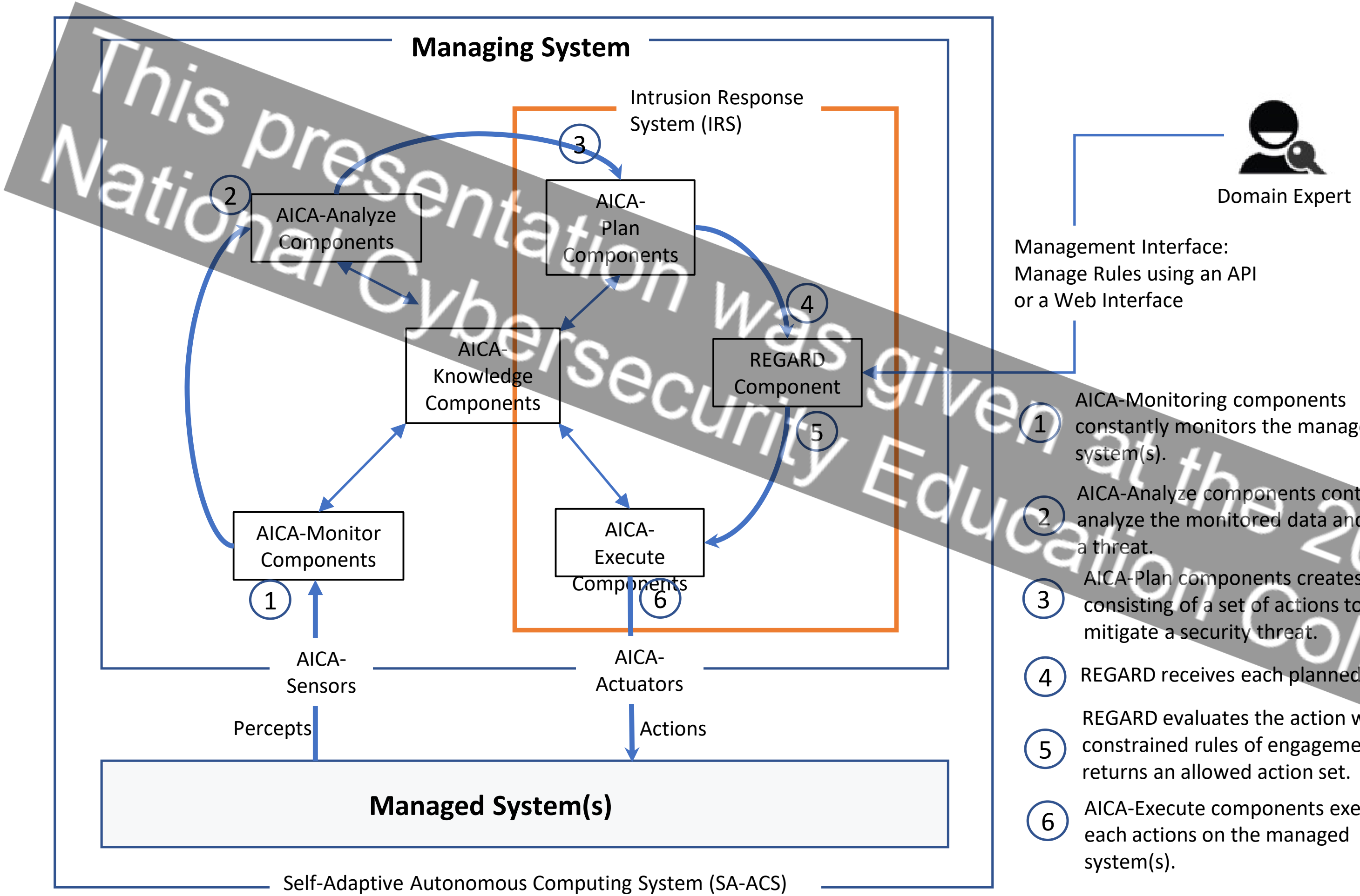
William Anderson
Mississippi State University
Mississippi State, MS, USA
wha41@msstate.edu

Joshua Whitman
Mississippi State University
Mississippi State, MS, USA
jsw625@msstate.edu

Sudip Mittal
Mississippi State University
Mississippi State, MS, USA
mittal@cse.msstate.edu

Benjamin A Blakely
Argonne National Laboratory
Ankeny, IA, USA
bblakely@anl.gov

REGARD - AICA Framework



1 AICA-Monitoring components constantly monitors the managed system(s).

2 AICA-Analyze components continuously analyze the monitored data and detects a threat.

3 AICA-Plan components creates a plan consisting of a set of actions to mitigate a security threat.

4 REGARD receives each planned action.

5 REGARD evaluates the action with constrained rules of engagement and returns an allowed action set.

6 AICA-Execute components executes each actions on the managed system(s).

REGARD - Architecture

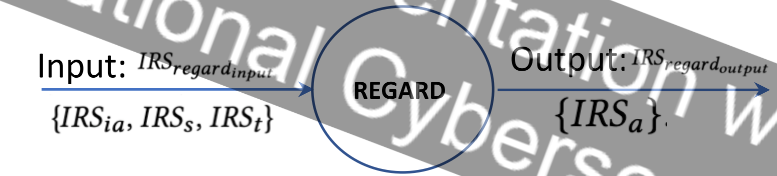

Input: $IRS_{regard_{input}}$
$\{IRS_{ia}, IRS_s, IRS_t\}$
REGARD
Output: $IRS_{regard_{output}}$
$\{IRS_a\}$

Figure A

- REGARD system:
  - Input – Intermediate action from AICA IRS Plan components
  - Evaluates – The intermediate action with RoE
  - Output – Final action to AICA IRS Execute components
- REGARD roles:
  - Domain experts
  - System administrators

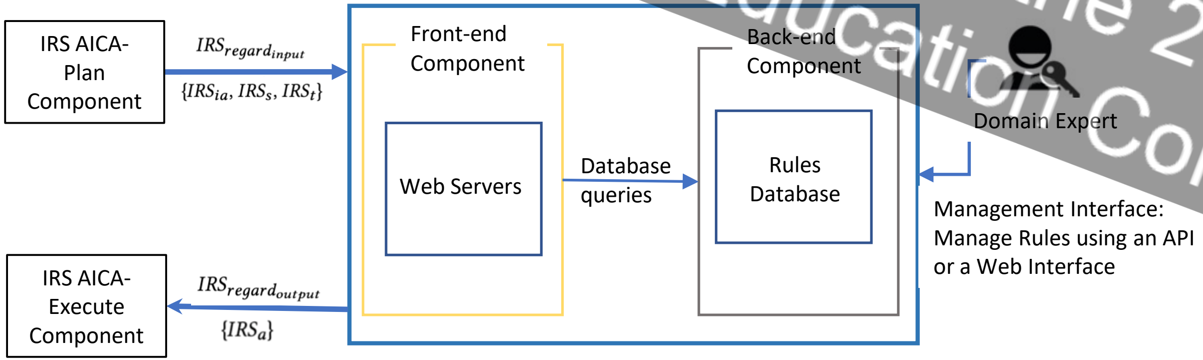
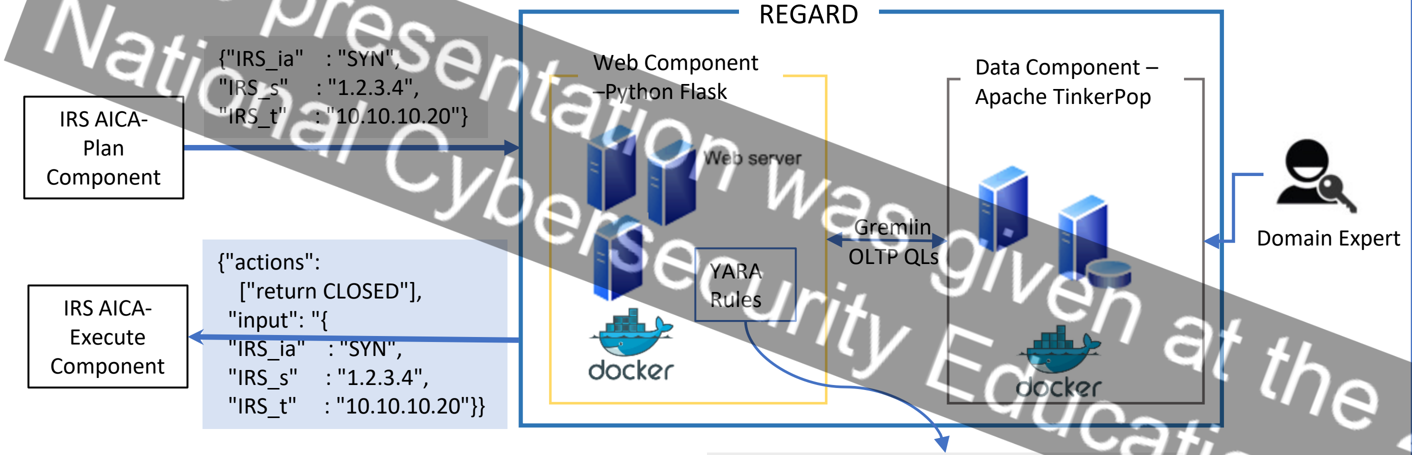


Figure B

REGARD - Implementation

Management Interface:
Manage Rules using an API
or a Web Interface



```
{"IRS_ia"   : "SYN",
"IRS_s"    : "1.2.3.4",
"IRS_t"    : "10.10.10.20"}
```

```
{"actions":
   ["return CLOSED"],
  "input": "{
  "IRS_ia"    : "SYN",
  "IRS_s"     : "1.2.3.4",
  "IRS_t"     : "10.10.10.20"}}
```

```
IRS_res_input{
        "action":"SYN",
        "target":"10.10.10.20",
         "source":"1.2.3.4"}
```

```
IRS_res_output{
   "action":"Return CLOSED",}
```

```
RoE1 {
  "id":"NET-L3-DDOS",
  "source":"any",
  "action":"SYN",
  "scope":"10.10.10.20",
  "constraint":"deny",
  "altaction":"return CLOSED"}
```

```
rule NET_L3_DDOS: NET_L3_DDOS {
  meta:
    created="10/23/2022 09:00:00"
    author="ANL"
    constraint="deny"
    alt_action="return CLOSED"
  strings:
    $source="*"
    $int_action="SYN"
    $scope="10.10.10.20"
  condition:
    $source and $int_action and $scope}
```

Features:

- Follows micro-service architecture & layered architecture patterns
- Provides flexibility to administer the software and rules data
- Uses YARA rules engine

GNN-powered AICA Intrusion Response System with REGARD

Damodar Panigrahi
Mississippi State University
Mississippi State, MS, USA
dp1657@msstate.edu

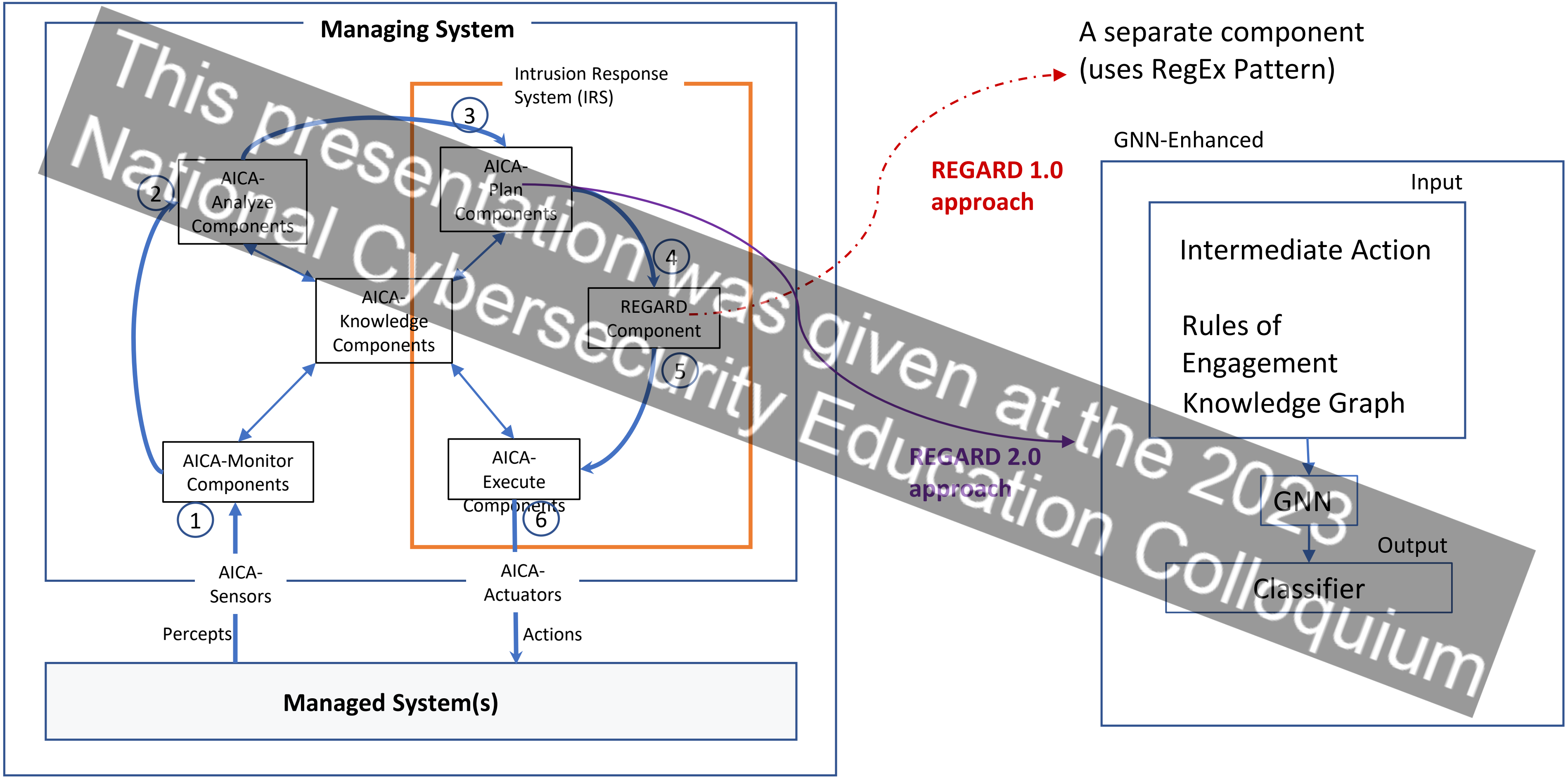
William Anderson
Mississippi State University
Mississippi State, MS, USA
wha41@msstate.edu

Joshua Whitman
Mississippi State University
Mississippi State, MS, USA
jsw625@msstate.edu

Sudip Mittal
Mississippi State University
Mississippi State, MS, USA
mittal@cse.msstate.edu

Benjamin Blakely
Argonne National Laboratory
Lemont, IL, USA
bblakely@anl.gov

REGARD-GNN - AICA Framework



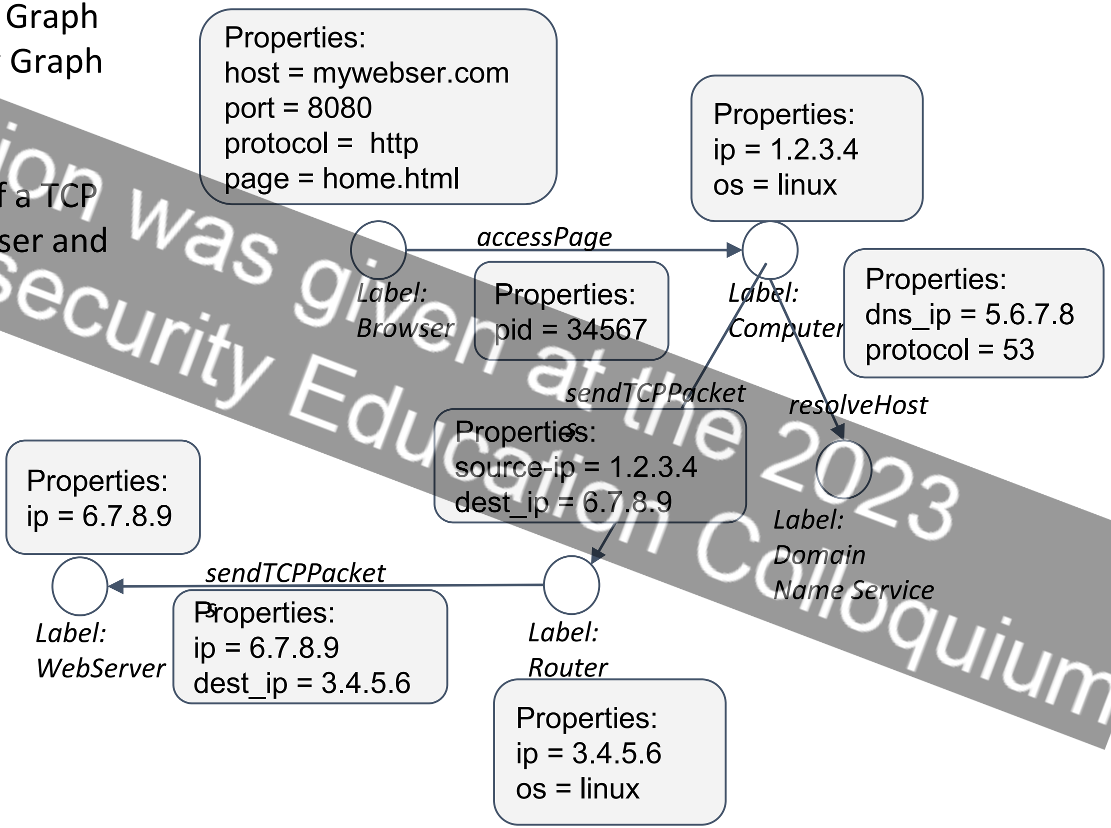
A separate component (uses RegEx Pattern)

REGARD 1.0 approach

REGARD 2.0 approach

Knowledge Graph - Sample

- Graph model built using Property Graph (PG), also called Labeled Property Graph (LPG.).
- A partial, yet simple illustration of a TCP packet flow between a web browser and a web server.



Properties:
host = mywebser.com
port = 8080
protocol = http
page = home.html

accessPage

Label:
Browser

Properties:
pid = 34567

Properties:
ip = 1.2.3.4
os = linux

Label:
Computer

Properties:
dns_ip = 5.6.7.8
protocol = 53

sendTCPPackets

resolveHost

Properties:
source-ip = 1.2.3.4
dest_ip = 6.7.8.9

Label:
Domain
Name Service

Properties:
ip = 6.7.8.9

sendTCPPackets

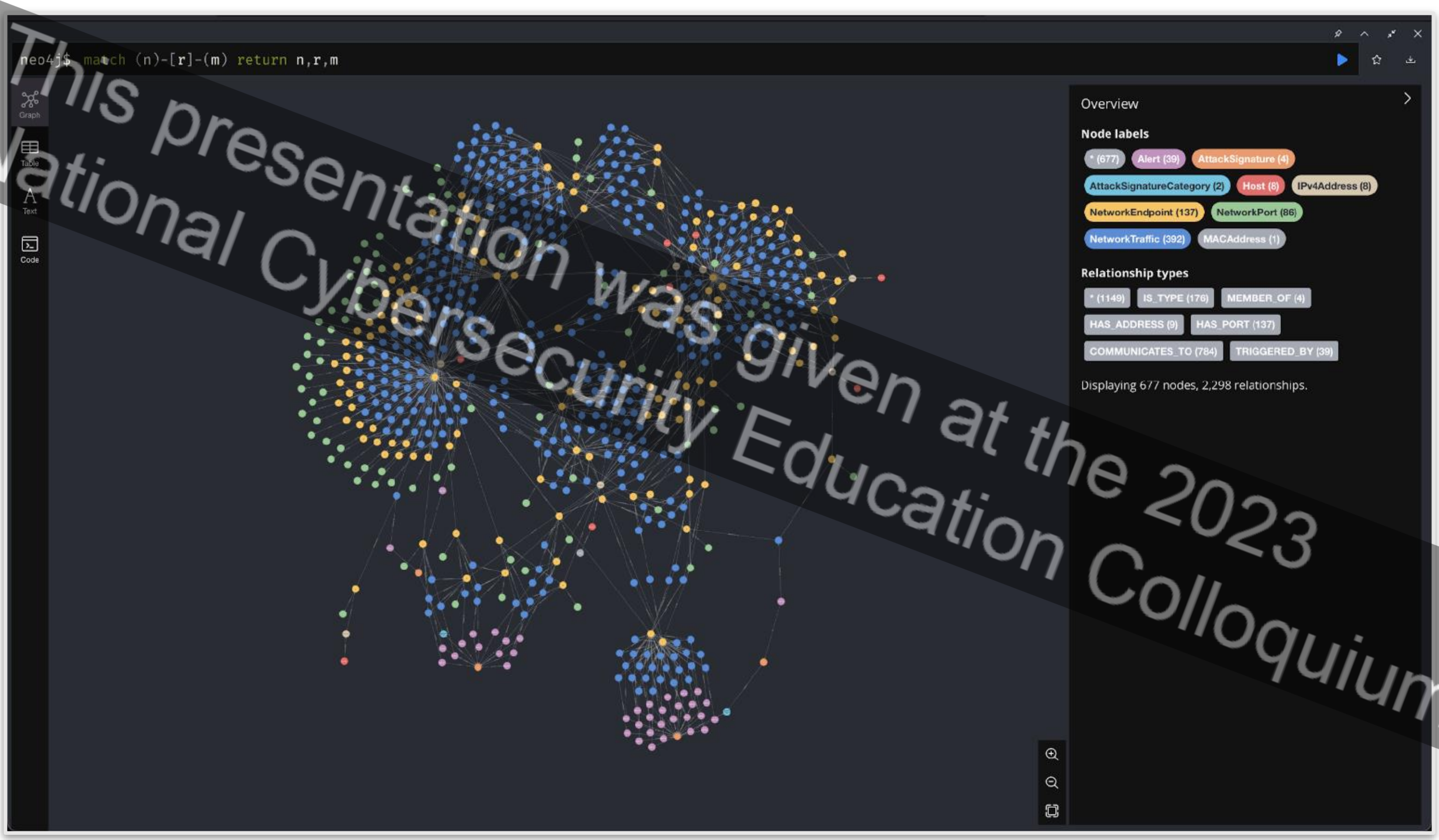
Label:
WebServer

Properties:
ip = 6.7.8.9
dest_ip = 3.4.5.6

Label:
Router

Properties:
ip = 3.4.5.6
os = linux

Knowledge Graph - Comprehensive



```
neo4j$ match (n)-[r]-(m) return n,r,m
```

Overview

Node labels

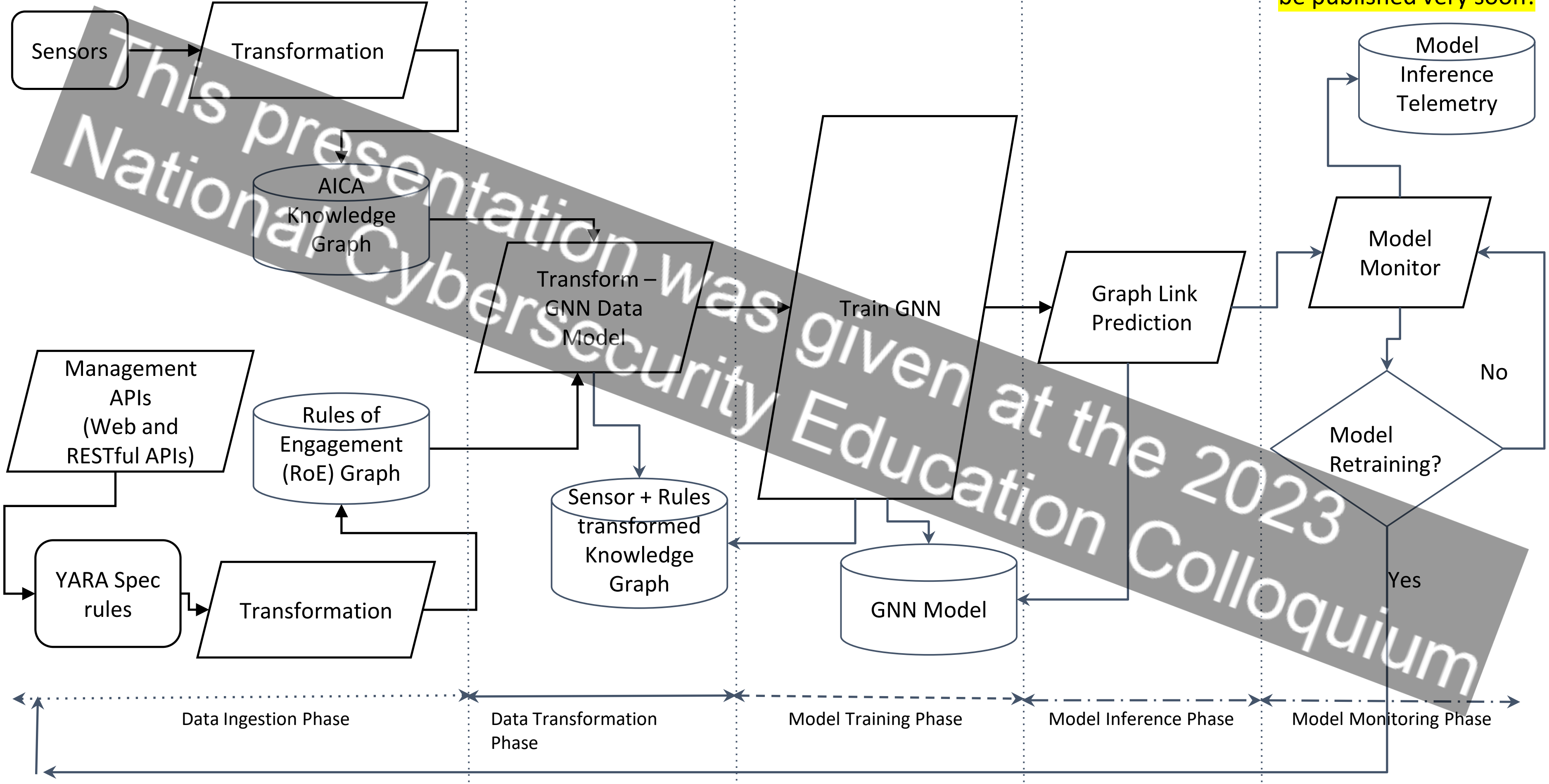
* (677) Alert (39) AttackSignature (4) AttackSignatureCategory (2) Host (6) IPv4Address (8) NetworkEndpoint (137) NetworkPort (86) NetworkTraffic (392) MACAddress (1)

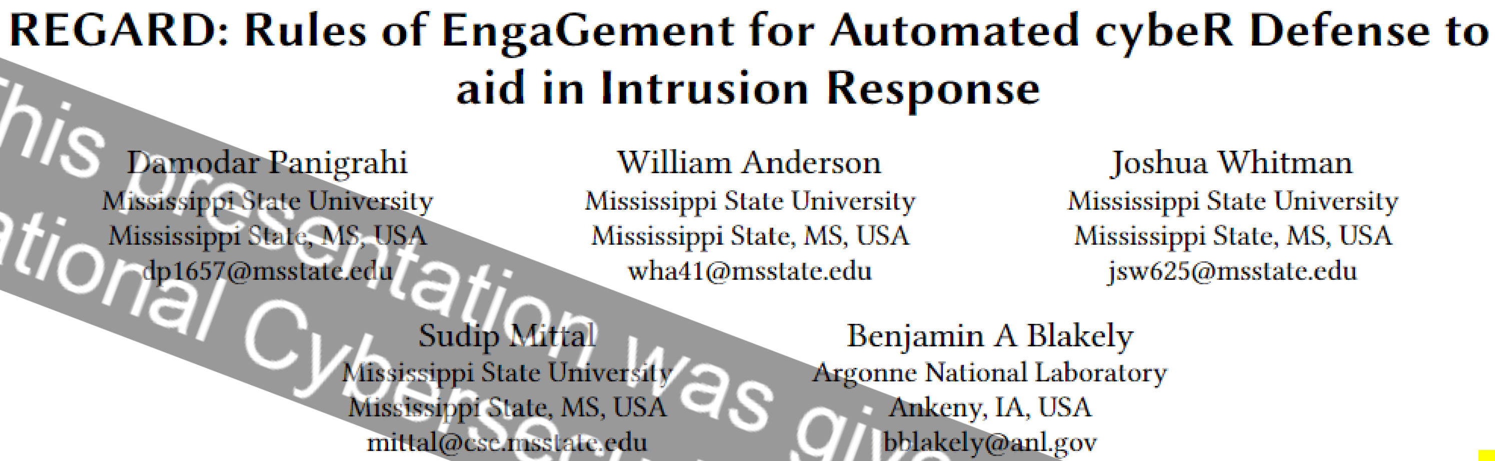
Relationship types

* (1149) IS_TYPE (176) MEMBER_OF (4) HAS_ADDRESS (9) HAS_PORT (137) COMMUNICATES_TO (784) TRIGGERED_BY (39)

Displaying 677 nodes, 2,298 relationships.

Model Evaluation Results to be published very soon!





REGARD: Rules of EngaGement for Automated cybeR Defense to aid in Intrusion Response

Damodar Panigrahi
Mississippi State University
Mississippi State, MS, USA
dp1657@msstate.edu

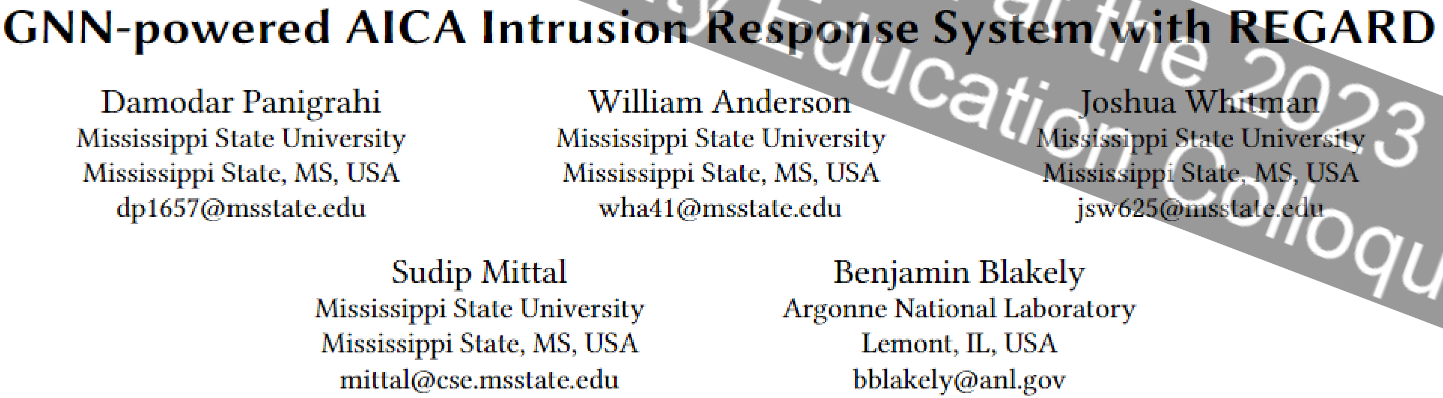
William Anderson
Mississippi State University
Mississippi State, MS, USA
wha41@msstate.edu

Joshua Whitman
Mississippi State University
Mississippi State, MS, USA
jsw625@msstate.edu

Sudip Mittal
Mississippi State University
Mississippi State, MS, USA
mittal@cse.msstate.edu

Benjamin A Blakely
Argonne National Laboratory
Ankeny, IA, USA
bblakely@anl.gov

2 publications!



GNN-powered AICA Intrusion Response System with REGARD

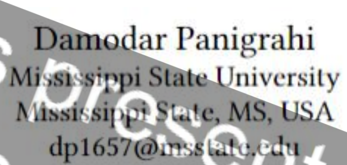
Damodar Panigrahi
Mississippi State University
Mississippi State, MS, USA
dp1657@msstate.edu

William Anderson
Mississippi State University
Mississippi State, MS, USA
wha41@msstate.edu

Joshua Whitman
Mississippi State University
Mississippi State, MS, USA
jsw625@msstate.edu

Sudip Mittal
Mississippi State University
Mississippi State, MS, USA
mittal@cse.msstate.edu

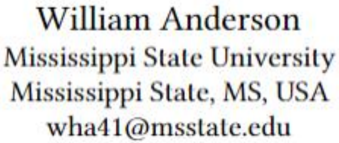
Benjamin Blakely
Argonne National Laboratory
Lemont, IL, USA
bblakely@anl.gov



Damodar Panigrahi
Mississippi State University
Mississippi State, MS, USA
dp1657@msstate.edu

Future Development of REGARD-AICA proposed as PhD dissertation topic.

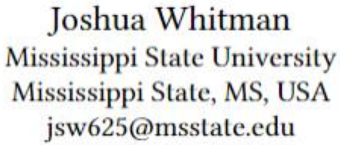
Dr. Blakely part of the PhD committee



William Anderson
Mississippi State University
Mississippi State, MS, USA
wha41@msstate.edu

Joined the Computer Science & Engineering PhD Program at MSU.

Looking at AI Security problems.



Joshua Whitman
Mississippi State University
Mississippi State, MS, USA
jsw625@msstate.edu

Completing his MS, and taking a cybersecurity job with a government agency.

Conclusion

- Rules of Engagement
- AICA
- REGARD
  - AICA-Based ROE Enforcement Framework
  - ROE Enforcement:
    - Strict Rule-Based Application
    - GNN-Based Intelligent Rule Application
- Future Work
  - Explainability!
  - On system testing!

Thank you!

Dr. Benjamin Blakely, Argonne National Laboratory

Dr. Sudip Mittal, Assistant Professor, Computer Science & Engineering, Mississippi State University

Damodar Panigrahi, PhD Computer Science & Engineering, Mississippi State University

William Anderson, MS Computer Science & Engineering, Mississippi State University

Joshua Whitman, MS in Cybersecurity, Mississippi State University

Argonne NATIONAL LABORATORY

INSuRE

MISSISSIPPI STATE UNIVERSITY