



NSF Campus Cyberinfrastructure PI and Cybersecurity Innovation for Cyberinfrastructure PI Workshop

September 23 – 25, 2019 | Minneapolis, MN

NSF Program (either CC or CICI): CICI

Program Area: OAC

Award Number: 1739025

PI: Matthew Bishop

co-PIs: Dipak Ghosal, Viji Murali

Project Title: CICI:CE: Improving the Security of a Science DMZ



Matthew Bishop

Professor
UCDavis
mabishop@ucdavis.edu



Dipak Ghosal

Professor
UCDavis
dghosal@ucdavis.edu



Viji Murali

CIO and Vice Provost
UCDavis
viji.murali@ucdavis.edu



NSF Campus Cyberinfrastructure PI and Cybersecurity Innovation for Cyberinfrastructure PI Workshop

September 23 – 25, 2019 | Minneapolis, MN

Quad Chart for:

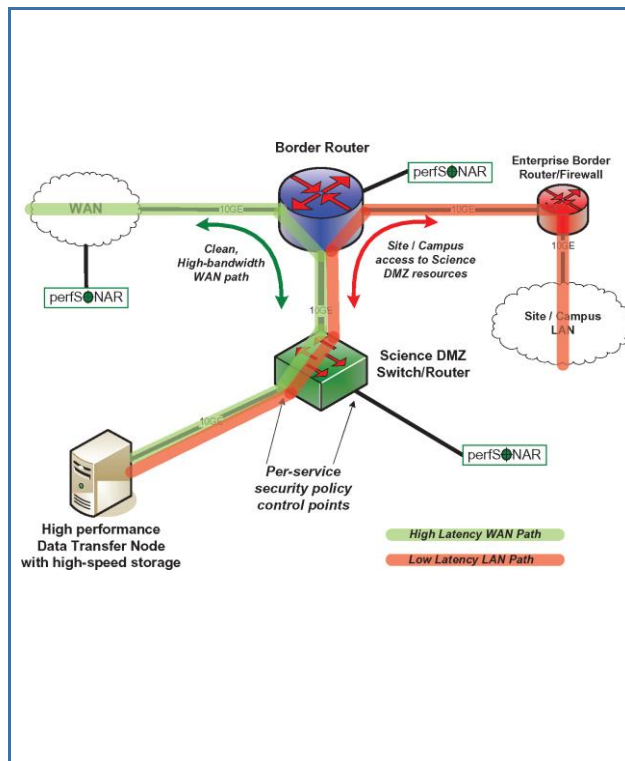
CICI: CE: Improving the Security of a Science DMZ

Challenge Project Seeks to Address:

- Identifying likely threats to a Science DMZ
- Reliably detecting Science DMZ threats using a combination of host and network performance metrics
- Detect malicious network traffic based on inter-packet delay and packet size

Solution(s) or Deliverables:

- Papers analyzing the effectiveness of our detection methods for identifying both common network attacks and insider threats
- Tools for protecting Science DMZs



Scientific Impact or Broader Impact:

- Provide a set of different algorithms to detect attacks on Science DMZ and high speed networks in general
- Reduce the time needed for security analysis
- Provide students with hands-on education

Metadata tag:

- There is lack of Science DMZ traces to build models of benign traffic
- Lack of labelled traces of attack on Science DMZ
- Need collaborators to try out the algorithms that we have developed
- Could always use more funds!!