

MARIST

School of Computer Science and Mathematics

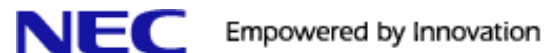


NSF SecureCloud, Year 2: Autonomic Cybersecurity using OODA Loops

PI: Casimer DeCusatis, Ph.D.

Assistant Professor, Marist College @Dr_Casimer

Co-PI: Alan Labouseur, Robert Cannistra, Matt Johnson, Bill Thirsk (CIO)



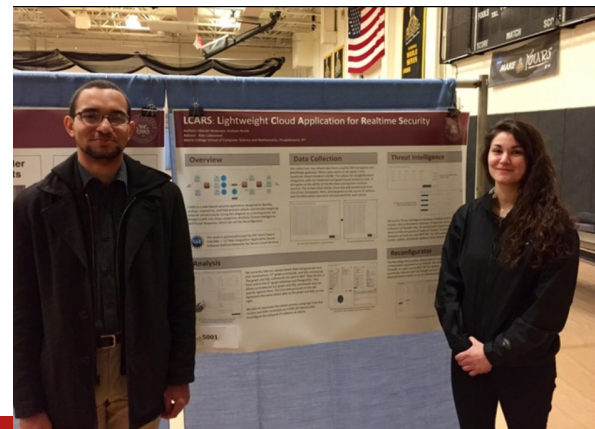
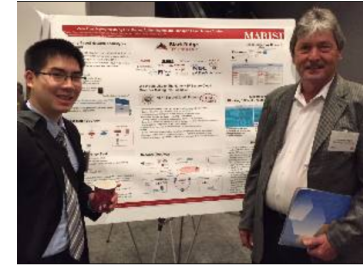
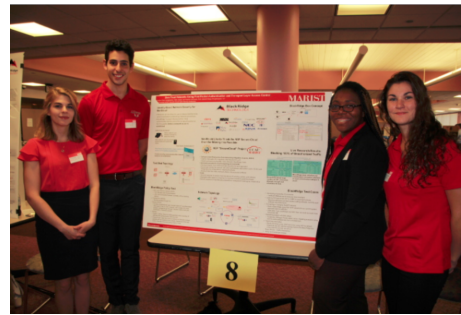
MARIST

School of Computer Science and Mathematics



Student Researchers

Marcos Barbieri
Graham Burek
Michelle Crawley
James Crowley
Thomas Famularo
Dan Jast
Vallie Joseph
G Leaden
Piradon (Tien) Liengtiraphan
Mariah Molenaer





SECTIONS

THE CHRONICLE OF HIGHER EDUCATION

LOG IN

SUBSCRIBE TODAY

SPECIAL REPORTS

Innovations in Cybersecurity Benefit Graduates and the Nation

By Paul Basken | FEBRUARY 26, 2017 PREMIUM CONTENT FOR SUBSCRIBERS. SUBSCRIBE TODAY

Cybersecurity job posting grew 114% from 2011 to 2015, with 86% requiring at least a B.S. degree. 4 year colleges are meeting only about 24% of this demand.

SECTIONS

THE CHRONICLE OF HIGHER EDUCATION

LOG IN

SUBSCRIBE TODAY

SPECIAL REPORTS

Cybersecurity, Rising

Working to meet a national shortage of computer-safety personnel, colleges find customers and complications

By Paul Basken | FEBRUARY 26, 2017 PREMIUM C

Working to meet a national shortage of computer-safety personnel, colleges find customers and complications.

Cybersecurity graduates can anticipate negative unemployment as far as the eye can see...Cybersecurity graduates will find jobs, especially if they come with a solid liberal arts education.

expansive sense of cybersecurity, offering programs that go beyond traditional computer science. These graduates, who may be better positioned to help their graduates find jobs in a world that is increasingly vulnerable to costly or deadly attacks. Following are some of...



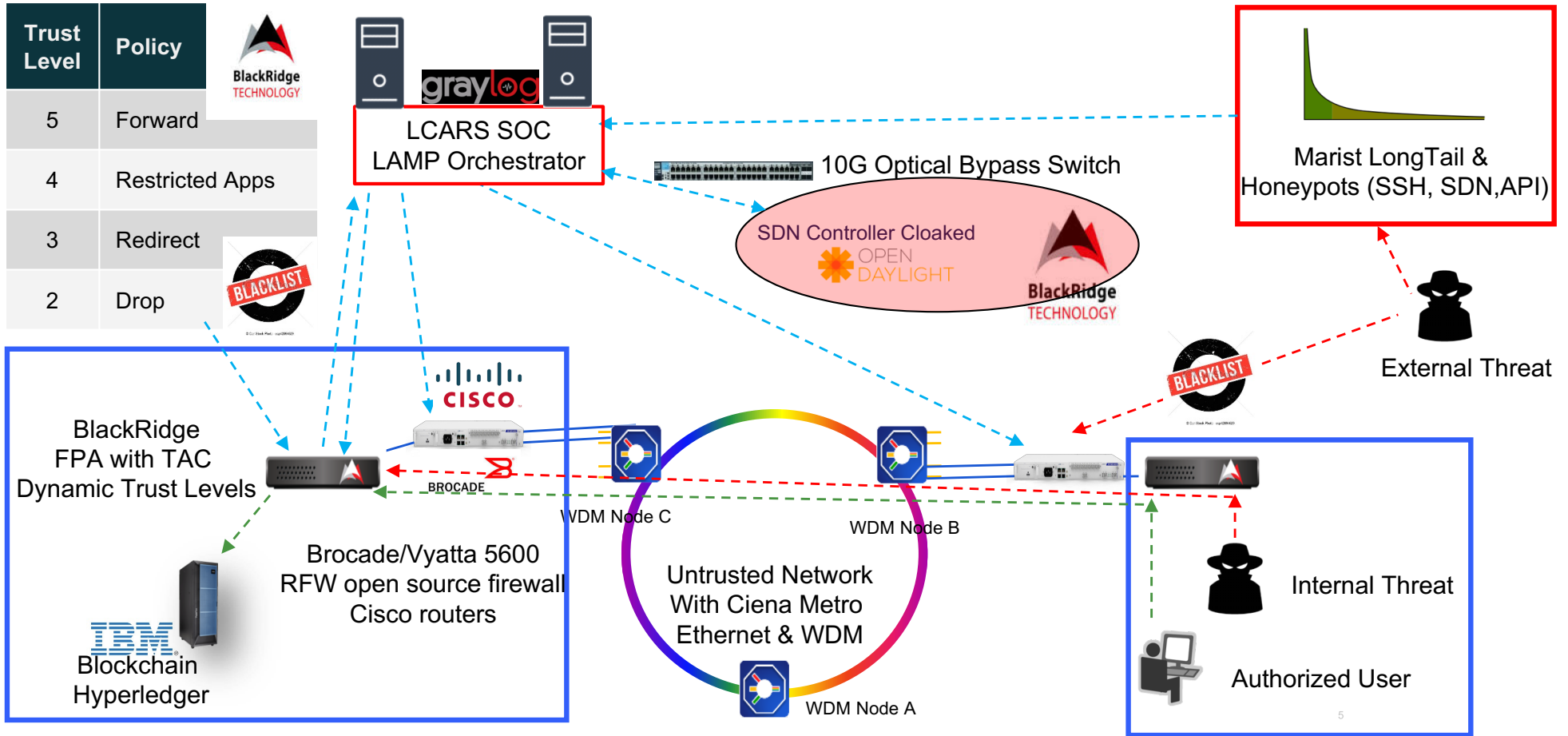
NSF “SecureCloud” Project

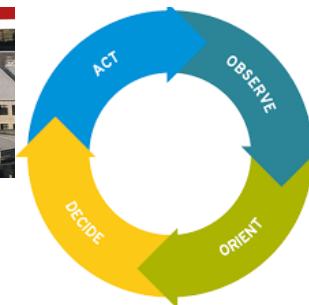
- **Campus Cyberinfrastructure Data Networking Integration (2-3 years, \$690 K)**
 - Casimer DeCusatis (PI), 4 students, 3 other faculty/CIO co-PI
 - Industry partners including IBM, Ciena, Brocade, BlackRidge, Cisco
- **Autonomic security for zero trust cloud computing environments**
 - Develop & deploy novel end-to-end security policy for each application
 - Dynamically monitor the network both within and between data centers (up to 100 km) and change security configuration in response to attacks
 - Prevent DDoS masking attacks, improve traffic visibility & segregation
 - Develop & test new code, eventually deploy into production at Marist



MARIST

School of Computer Science and Mathematics





Bad Actors / Attack Surface

OBSERVE

Raw Data Telemetry Collection
(big data + metadata)

Cloaked Resources

ORIENT

Data Analysis

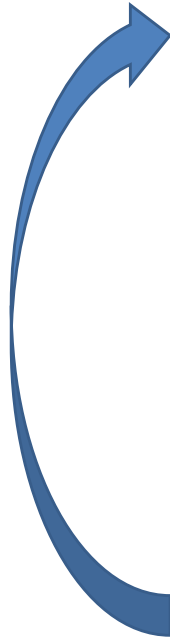
Classification
Attribution
Visualization
Analytics (Predictive & Otherwise)

DECIDE

Actionable Threat Intelligence
(attack profile, response recipe)

ACT

Autonomic Defense
(Reconfigurator / Orchestrator)





Conference Presentations

- M. Molenaer, M. Barbieri, V. Joseph, M. Crawley, and P. Liengtiraphan, “Zero Trust Networks using Transport Access Control Techniques” Proc. IBM TechConnect (Best of Solutions Award, Early Tenure Category), IBM Poughkeepsie/Yorktown Heights, NY (September 22, 2016)
- P. Liengtiraphan and C. DeCusatis, “Zero Trust Networks using Transport Access Control and First Packet Authentication”, Proc. NYIT 6th Annual Cybersecurity Conference, New York, NY, student poster session (Sept. 22, 2016) http://www.nyit.edu/events/annual_cybersecurity_conference
- C. DeCusatis, “Cloudy with a chance of SDN Part II”, BRKCRT-2603, Cisco Live, Las Vegas, NV (July 10-15, 2016)
- C. DeCusatis, “The NSF SecureCloud project: cybersecurity for enterprise class data centers”, Proc. NSF Enterprise Computing Conference (ECC), Marist College, Poughkeepsie, NY, June 12-14, 2016
- C. DeCusatis, “Zero trust cybersecurity architectures for software defined data centers”, Proc. NYSERNET (Internet 2) Tech Summit, Vassar College, Poughkeepsie, NY June 16-17, 2016
- R. Cannistra, P. Liengtiraphan, and V. Joseph, "Securing SDN and NFV Enabled Campus Environments through Orchestration and Automation", Proc. Internet 2 Technology Exchange, Miami, FL (September 2016)
- P. Liengtiraphan and V. Joseph, “How to make a honeypot”, lightning talk presented at Internet 2 Technology Exchange, Miami, FL (September 2016)



Research Papers

- S. Nanda, F. Zafari, C. DeCusatis, E. Wedaa and B. Yang, “Predicting Network Attack Patterns in SDN using Machine Learning Approach”, Proc. IEEE 2016 Conference on Network Function Virtualization and Software Defined Networks (SDN/NFV 2016), Palo Alto, CA (Nov. 7-9, 2016) <http://nfvsdn2016.ieee-nfvsdn.org/>
- C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, “Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication”, Proc. IEEE International Conference on Smart Cloud (SmartCloud 2016), New York, NY (Nov. 18-20, 2016) <http://csis.pace.edu/CSCloud/sc2016/>
- C. DeCusatis, A. Carranza, “Modeling software defined networks using Mininet”, Proc. 2nd International Conference on Computer and Information Science and Technology (CIST), Montreal, Canada (May 20-21, 2016) (Best Paper Award)
- C. DeCusatis, P. Liengtiraphan, A. Sager, IEEE/ACM REV 2017 (to be published)

MARIST

School of Computer Science and Mathematics



Thank You



Follow @Dr_Casimer or <http://www.ofcconference.org/en-us/home/about/ofc-blog/>