REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
21-03-2023	Final Report	15-Mar-2019 - 30-Jun-2020

4. TITLE AND SUBTITLE
Final Report: Computers and Networks for Cybersecurity Experiments and Education

5a. CONTRACT NUMBER
W911NF-19-1-0177

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Davis
Sponsored Programs
1850 Research Park Drive, Suite 300
Davis, CA 95618 -6153

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
73964-NC-RIP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Matthew Bishop
UU	UU	UU	UU		19b. TELEPHONE NUMBER 530-752-8060

RPPR Final Report
as of 22-Mar-2023

Agency Code: 21XD

Proposal Number: 73964NCRIP **Agreement Number: W911NF-19-1-0177**
INVESTIGATOR(S):

Name: Matthew A Bishop
Email: mabishop@ucdavis.edu
Phone Number: 5307528060
Principal: Y

Organization: **University of California - Davis**
Address: Sponsored Programs, Davis, CA 956186153
Country: USA
DUNS Number: 047120084 EIN: 946036494

Report Date: 30-Sep-2020 Date Received: 21-Mar-2023
Final Report for Period Beginning 15-Mar-2019 and Ending 30-Jun-2020
Title: Computers and Networks for Cybersecurity Experiments and Education
Begin Performance Period: 15-Mar-2019 **End Performance Period:** 30-Jun-2020
Report Term: 0-Other

Submitted By: Matthew Bishop Email: mabishop@ucdavis.edu
Phone: (530) 752-8060

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: **STEM Participants:**

Major Goals: The goal of this project was to establish a network testbed with commercial off-the-shelf (COTS) systems and a high assurance, high security systems that could be used to test and evaluate methods for monitoring and protecting networks of systems of varying levels of assurance and security.

The design of the testbed is to have two subnets connected by a gateway/firewall. One subnet would have the high assurance, high security GEMSOS system and COTS computers, and the other would have COTS computers. The testbed would not be connected to the Internet, except for one system that would serve as a "switch" -- it can be connected to either the testbed or the Internet, but not both. This can be used to transfer data and programs from one network to another.

This would support several Department of Defense projects and proposed projects.

Accomplishments: Unfortunately, COVID-19 interfered with this work, as UC Davis closed the campus in early 2020 and did not reopen until late 2021, and did not require in-person class (and other) attendance until late 2022.

* Set up and began using the GEMSOS system
* Attended training, recorded it so others could learn
* Developed small controller for stop sign to test its use controlling CPS and IoT systems
* Designed network; began implementation, which was delayed due to COVID-19

Training Opportunities: The GEMSOS system, which is a high assurance, high security system uses a different model than Linux, BSD, Windows and Macintoshes use. It very much resembles the Multics programming environment, treating files and memory as segments, and programs manipulate segments, and indeed execute in segments. The GEMSOS ring access control mechanisms work exactly as do the Multics rings. This means users of the GEMSOS system have to be trained on how to use it and, in particular, learn a completely different programming model. So AESEC, the company developing GEMSOS, provided a two-week tutorial on the architecture of GEMSOS, how to use it, and how to program it. With AESEC's permission, we recorded the tutorial so incoming graduate and undergraduate students could learn about the system, use it, and program it. This contributed to their training and education because it showed them the constraints and architecture that a high security, high assurance system provides.

Results Dissemination: Nothing to Report

RPPR Final Report
as of 22-Mar-2023

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to report -- no patent applications, inventions, licenses, or interactions with DoD laboratories

PARTICIPANTS:

Participant Type: PD/PI
Participant: Matt Bishop
Person Months Worked: 1.00
Project Contribution:
National Academy Member: N

Funding Support:

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Matt Bishop
Signature Date: 3/21/23 7:19PM

Final Report on DURIP Award W911NF1910177

Matt Bishop
Dept. of Computer Science
University of California at Davis
1 Shields Ave.
Davis, CA 95616-8562
email: mabishop@ucdavis.edu

Abstract

The objective of this project was to obtain a high assurance, secure system and create a testbed around it That would enable researchers to test attacks, defenses, malware, worms, and other inimical actions and programs against the high assurance system, and from the high assurance system. We completed procuring and training on the system, and designed the network.

Objectives

This was a one-year project. The objectives were:

- Establish a network testbed with commercial off-the-shelf (COTS) systems and a high assurance, high security systems;
- Train students and faculty in the use of such a system; and
- Implement a testbed hat could be used to test and evaluate methods for monitoring and protecting networks of systems of varying levels of assurance and security.

Findings

We accomplished the following:

- Procured, set up, and began using the GEMSOS system;
- Attended training, recorded it so others could learn;
- Developed a small controller for stop sign to test the computer's use controlling CPS and IoT systems; and
- Designed network; began implementation, which was delayed due to COVID-19

The GEMSOS system, which is a high assurance, high security system uses a different model than Linux, BSD, Windows and Macintoshes use. It very much resembles the Multics programming environment, treating files and memory as segments, and programs manipulate segments, and indeed execute in segments. The GEMSOS ring access control mechanisms work exactly as do the Multics rings. This means users of the GEMSOS system have to be trained on how to use it and, in particular, learn a completely different programming model. So AESEC, the company developing GEMSOS, provided a two-week tutorial on the architecture of GEMSOS, how to use it, and how to program it. With AESEC's permission, we recorded the

tutorial so incoming graduate and undergraduate students could learn about the system, use it, and program it. This contributes to their training and education because it showed them the constraints and architecture that a high security, high assurance system provides.

Unfortunately, COVID-19 interfered with this work, as UC Davis closed the campus in early 2020 and did not reopen until late 2021, and did not require in-person class (and other) attendance until late 2022.