Engineering Student Technology Committee

http://www.engr.colostate.edu/ESTC

College of Engineering

Colorado State University

1. **Title of Proposal:**
   Standalone computer network for laboratory experiments and multiyear senior projects isolated from the CSU intra net and focused on hands on **Cyber Security Training**.

2. Proposal Participants:

Primary Contact for Proposal

Name: george collins _____E-Mail: gcollins@engr.colostate.edu

Department/Major: Electrical and Computer Engineering _____

Check One: __x___ **Faculty** _____ **Staff** _____ **Student**

Additional proposal participants

Name: _____E-Mail: _____

Department/Major: _____

Check One: _____ **Faculty** _____ **Staff** _____ **Student**

Additional proposal participants

Name: _____E-Mail: _____

Department/Major: _____

Check One: _____ **Faculty** _____ **Staff** _____ **Student**

3. Proposal Abstract (limit to 100 words):

Cyber-attacks are becoming more sophisticated, more numerous and more serious. Almost every PC on the internet is tested for vulnerabilities on a daily basis. Most of these attacks are not staged by professionals and usually not serious. However, if your computer has marketable information then the game changes. Two of the most serious questions are who has attacked you and how. If you know who you can report them to law enforcement and if you know how you can reconfigure your computer to seal off the vulnerability. Honeypots, computers specially configured to look like ordinary computers that an attacker should be interested in are one of the primary techniques for capturing the IP address and code injected by an attacker. Student familiarity with these issues helps students achieve a post CSU job. All materials developed by senior project teams and in a dedicated network for cyber security hands on experiences will be used in

both existing and a new course that “deep dives” into cyber security. The new 500 level course will be 4 credits (3 lecture and 1 laboratory) and will entitled **“Cyber Security for the Electric Grid, Educational Institutions and Industrial Networks”.**

Student senior projects are multi-year with a new team every year building on prior student efforts and efforts are associated both with Prof Collins’s new and existing courses in ECE. The ECE department will contribute 25% of the total cost of 2400 dollars for establishing a cyber-security network testing set up. I have donated two PC’s from my laboratory, for a total of six computers in an isolated cyber security test network. ENS has agreed to help senior students set up the isolated cyber-attack test network.

4. Proposal Budget: 2400 dollars (ECE Dept. $600 and ESTC $1800)

Four computers at $600/ each for parts and construction and testing will be done by ECE senior project students with help from ENS . Honeypot software will be provided gratis by both Fireeye and IBM, which are both security leaders have already met with Prof. Collins and both have offered honey pot both software and teaching materials. In addition for a base line we will run web based cyber security free ware.
Since this material and secure and isolated cyber-attack testing network will be employed in three courses and a similar number of senior projects, we cannot use a special course fee, since it benefits a wide variety of students from ECE and other departments.

5. Full description of proposal:

Over the next two years I am creating a new 500 level course in ECE entitled **“Cyber Security for the Electric Grid, Educational Institutions and Industrial Networks”**. This will consist of lectures for 3 credits and 8-10 laboratory assignments for 1 credit. A key component of the “ deep Dive” cybersecurity course will be a computer laboratory for hands on work with simulated cyber-attacks and responses. This small network needs to be isolated from the CSU intranet. In this isolated network students will utilize one of the open source honeypots and configure and modify a set of three of them to record and analyze the external traffic coming into the machine. Since the machine isn’t accessing the net on its own, then any

traffic is more or less malicious. Students will review all the incoming traffic to the honeypots, determine the source and determine what type of attack is being used. Newer techniques permit traffic from three adjacent machines to be analyzed to digitally triangulate the source. Malware analyzers will be used to identify the type of attack, although newer attacks don't fit previously detected patterns. Upon completion of the project students will be familiar with the problems of cyber defense and security which will provide them with a marketable skill.

Simplified portions of this cyber security course will also be employed and incorporated into three existing ECE courses Prof. Collins teaches.

My existing course in "Power Systems", ECE 461/462, with an enrollment of 20-25 students will be the first beneficiary with a focus on electric grid security threats in existing laboratory assignments. Three new laboratory experiments will be added to ECE 461/462.

My 562 Power Electronics (enrollment 15) and 569 (enrollment 28 ECE and 6 ME) courses will also benefit from cyber security via 10 quizzes with cyber security questions set in industrial settings, taking 10-20 % of each quiz assignment, including hands on monitoring of hacking logs.

Finally my new " deep dive" course, entitled **"Cyber Security for the Electric Grid, Educational and Industrial Networks"**, for 4 credits 3cr lecture and 1cr for laboratory) will have more in depth cyber security coverage for industry, universities and for the electric grid.

A key element of the course is the use of "honey pots to identify and neutralize attackers. In addition we will have labs, demonstrations and lectures by Steven Lovaas the CSU head of Cyber security. Steven has also offered to allow students in all my courses to view cyber logs of attacks on CSU's system.This will use Fireeye gateway moats already deployed by CSU ACNS. Both IBM and Fireeye will provide course materials on cyber security as well.

The course lectures and laboratories will also feature contributions Dr. Joel Dubow covering his extensive experience with cyber security in industrial settings. Steven Lovaas of CSU ACNS will contribute materials on cyber-

attacks on universities. Finally, Joe Liberatore of WAMPA (Western Area Power Authority) will provide materials on electric grid attacks.

We request from ESTC monies for four PC's to be built by ENS at a parts count of 600/ each. ECE will cover $600 and we request ESTC cover the remaining $1800. ENS will put together the isolated networked system of the cyber laboratory computers, to be used in the laboratory portion of the new cyber security course. All other lab construction and cyber testing will be done by an existing team of SENIOR PROJECT STUDENTS and 695 special project MS students. This senior project effort will be yearly for the next 2-3years.