FINAL REPORT- Microsoft TWC (Trustworthy Computing) Curriculum Grant

Mehmet Sahinoglu, Ph.D.
Eminent Scholar & Professor,
Computer Science
Gunter AFB Annex, Bldg. 826, Rm: G111
Troy University - Montgomery Campus
Montgomery AL 36103-4419
Tel:(334) 832-7289, Fax: (334)241-9589
E-MAIL: mesa@troy.edu

List of Contents:

1) Introduction:

We are pleased to present this final report to the Microsoft Academic Alliance on the $50,000 grant awarded worldwide in January 2006 along with those of other 13 universities which are St. Petersburg (Russia), Yonsei (S. Korea), CMU, Northeastern, KUL (Belgium), Nothwestern, Purdue/TAMU, U of FL, Michigan State U, U-Mass, NCSU, U of VA and U -Cal at Berkeley. This activity report shows what had been proposed, accomplished and delivered as well as the extent of educational challenges presented and met pursuant to the core of the grant, that being to excel in a curriculum most beneficial for the students in this field and to provide them with the tools they will need in their future careers. Further recommendations and future plans are included. Please see a detailed Appendix presented at the end of this executive summary to help understand some details of the process the PI and project group went through.

2) What is TWC Context?

To aid in understanding TWC I would begin by quoting Microsoft's External Research & Programs "Trustworthy Computing" article. "No issue is currently of greater importance to Microsoft and our industry than trustworthy computing. Amid increasingly frequent and sophisticated networks attacks, users expect their systems to remain resilient and available. They expect data to remain intact and confidential at all times. As they increasingly use computers to manage information important to their everyday lives they expect and demand control over access to and use of their personal information. Ultimately, it is essential that computers perform as expected and that users enjoy a consistently trouble-free computing experience." "Changes in the way software is designed, built and tested are critical. We must better understand the types of failures and threats to which any particular piece of software is vulnerable." "We must effectively train designers and developers of software to focus on trustworthiness and to have the essential knowledge to build consistently trustworthy software. Computer security and cryptography have been subjects of valuable academic research for some time. But this is only a part of the larger set of issues that define trustworthy computing and even computer security often receives only very limited treatment in computing curriculum. Academic research has made valuable contributions to Microsoft through Microsoft

Research's Trustworthy Computing Advisory Board. Now, there is an urgent need to raise awareness of the full range of trustworthy computing issues in academia and begin to develop the kind of innovative approach and materials that can replace trustworthiness at the center of the computing curriculum." **[1]**

By strengthening and updating the CS curriculum with the changing trends at the onset of the 21st century we plan for our graduate students with a degree in CS to be equipped with an appreciation of analytical and quantitative measures to assess, compare and measure trustworthiness of cyber systems. Students must be sensitized and proactive **before** undesirable episodes due to breach of security and poor reliability can occur and act "security-conscious & reliability-literate." Simply stated, our students cannot afford ignorance in terms of software-quality and information-security concerns. TWC is in direct response to this need as well as the following: PITAC's (President's Information Technology Advisory Committee) report to the President of the United States in February of 2005 such as in: "Ubiquitous Interconnectivity = Widespread Vulnerability" (p. 7), and "Fundamentally New Security Models and Methods Needed" (p. 12), or "The Federal government should intensify its efforts to promote recruitment and retention of cyber security researchers and students at research universities" (p. 31) and,

a) Developing security metrics and benchmarks,

b) Economic impact assessment and risk analysis including risk reduction and cost of defense and,

c) Automated tools to assess compliance and /or risk. (p. 45). **[2]**

In addition to offering CS 4451 as an undergraduate course, the need for a more advanced-level graduate course was indicated. The project was intended to and has actually fulfilled the important next step with an update of the existing core of the elective course. The existing course in the Troy University catalog:

CS 4451: Computer Security and Reliability (3): Basic security concepts and principles applied to real-world applications. Introduces the major elements that go into a security implementation, including encryption, authentication, access control lists, execution control lists, vulnerability of operating systems, auditing, performing vulnerability analysis and risk assessment, developing a security plan and protecting data, systems and infrastructure. This course also builds on the fundamentals of reliability and safety engineering, which include software reliability, growth models, testing and stopping-rules, safety methods and redundancy. *Prerequisite:* CS 3330 *(Data Structures and Algorithms),* CS 3332 *(Software Engineering I)*

This is an excerpt from the Troy University Undergraduate Catalog 2005-2006. An electronic link can be found at **[3].**

The summary of the proposal which was awarded by Microsoft along with others **[4]**:

Improving a Trustworthy Computing Curriculum (TCC) for Undergraduate/Graduate Computer Science

Mehmet Sahinoglu, Troy University

The objective of this proposal is to strengthen and validate an already existing course on Reliability and Security in the CS Department of TROY's Montgomery Campus generally serving adult and working students in IT, to meet the most current trends of the academia and IT industry. Other local campuses in Troy, Dothan and Phoenix City, and 62 world campuses including those of Distance Learning will benefit. We aim to provide our students with collaborative guidance by a local IT firm for hands-on-training through the creation of a cyber-security lab. Compensated graduate students will play an active role in the TCC improvement, assisted by the PI's current book writing activity on Reliability and Security.

3) TWC Curriculum Grant (EXECUTION & EVALUATION)

The CS Dept. of Troy University Montgomery had filed a proposal on October 5, 2005 happily resulting in The Microsoft TCC (Trustworthy Computing Curriculum) Grant being awarded to them at the end of January 2006.

Following this announcement, the PI had an initial meeting, in February, with the Sponsored Programs Coordinator, Troy University Campus and multi-campus Deans, and Vice Chancellors from Montgomery and Troy campuses, at Montgomery about conditional acceptance of Microsoft grant only as a gift with no strings attached. The letter was sent to Microsoft Representative, John Spencer who confirmed that the grant was a gift only for TWCC research and activities (**Appendix**: MICROSOFTletter.jpg).

The same above-mentioned group also had a meeting with the CEO of ICS (Integrated Computer Solutions), a local award winning Software Security Firm who volunteered to build the TCC lab with Troy Univ.'s CS Department at Montgomery, on how to proceed with a letter of intent and joint action on press releases in the coming months. The administrative assistant of the TWC project was also present at this meeting.

Several press releases at the Univ. or local media level were accomplished through Troy University's public relations offices. These releases proved useful to ICS in their Public Relations efforts as well as by Microsoft for promotion of their programs on TCC grants. At the academic level, the PI started teaching the designated course on Security and Reliability during the Spring Semester, starting January 2006, from a newly proposed curriculum, which was the nucleus to the final form. The class followed the PI's draft book, due to publish in July 2007 by J. Wiley. The PI was subsequently able to collect feedback from one A+ student. The same course was scheduled for undergraduate and graduate students in Fall 2006, as well as Spring 2007.

The Cyber-Lab project, a part of this curriculum building project has been initiated with nothing first available on an action plan, consequently advanced to the level of completion at the end of 12 months in February 2007. The hardware activities were completed at the end of July and the software downloading for the Honeynet-project, with collaboration from the partnering company ICS has been concluded at the time of the closing presentation in February 2007.

The Cyber-Lab was scheduled to be completed by January 2007 after having been connected to the Bellsouth network. The goal, as stated in the TCC proposal submitted to Microsoft, purports to familiarize our students with hands-on-education and training. This goal was achieved by January 2007. During the months of April and May, the PI was invited to participate in Microsoft Academic Days on TwC in Redmond WA, and FSU's Information Security Summer School, respectively. These meetings added considerable insight and appreciation observing the state-of-the-art on the overall picture, which has influenced the PI to improve the project's course. **(Appendix**: Redmond.jpg, FSU.jpg, Invitation to Microsoft.eml)

From mid-June to end–December, the PI focused during the new Fall semester's teaching of the same courses (CS 45451-ugrad, CS 6653-grad) as regards with the curriculum improvement based on the past and future feedbacks, and personal experiences gained from the presentation of this course, and lab integration with the said course. The author is presented this course curriculum along with that of a book tutorial, during the IDPT2006 conference **[5, p.17/28]**. The TWC curriculum will be studied in the Education Workshop in 2007 IDPT conference **[6].**

The PI planned -in the second half of the year- to undertake two to three fact finding trips to meet with the other fellow grantees to find out how the other PIs are conducting their TWCC projects. At the end of this project, the PI worked to consolidate and share its findings with Troy Univ's other CS Depts. or those others interested in this project. The proposed and in time improved curriculum was presented to the students, and their curriculum feedbacks were received for a second time in 2006 Fall Semesters after teaching CS 4451: Security and Reliability, through using the author's (PI) bookwith the CD ROM to be published in July 2007 by J. Wiley Inc. **[7].**

The cyber-security lab with a separate DSL internet connection was constructed now with the Honeynet project and others in the near future like those on privacy pending to be incorporated. The lab portion of the curriculum was appended after the completion of the lab to-do-list. Various collaborations through domestic/international invitational seminars with the other grant winners have been arranged for a broader understanding of the TWC concepts and applications, geared towards the core objectives of the TWCC proposal statements proper as in the proposed write-up.

Presentations based on outcomes and target dates were:

<u>a. Conferences:</u>

1) IDPT2006, A Tutorial on the TWC Improved Curriculum, June 23-29, 2006, San Diego, CA

2) DII06, Key Note Seminar on Security and Privacy with Implementations on a Univ. Curriculum, Nov 15, 2006, Seoul, Korea

3) Invited Seminar at U-Mass on Security and Privacy Curriculum, Dec. 8, 2006, Amherst, Mass.

4) Invited Seminar at UAB's CIS Dept on Microsoft TWC Grant for an Improved CS Curriculum , Dec. 1, 2006, Birmingham, AL.

<u>b. Other</u>

1) Attended Microsoft TWC Days in Redmond Washington as an invitee of Miscrosoft in April 2006.

1) Attended Cyber-Security workshop, May 23-25,06 by FSU in Tallahasse,FL

2) Visited UFL on Aug. 7, 2006 at Gainesville FL to meet with Dr. Tao Li, 2005 Microsoft Grant winner, to discuss his initiative on Sim-SODA :A Unified Framework for Architectural Level Software Reliability Analysis for a possible collaboration on the metrification of Imbedded Reliability towards including the topic within the framework of an improved TWC Curriculum.

Planned publications and presentations:

Proc. IEEE Instrumentation and Measurement, June 2007 **(Appendix:** 493_0_Art….pdf**)**

IDPT 2007, SDPS Annual Conference, June 2007 **[6, p. 16]**

Any other important information:

The J. Wiley book-to-be published in June 2007, titled " Trustworthy Computing: Analytical and Quantitative Engineering Evaluation" independently from this Microsoft project(not financially supported by Microsoft Grant) is in works by the PI, and is currently being used as a text book for the TWC curriculum for the course being developed and improved. I am building a new one supported by the new book's chapters to improve on the old curriculum as I proposed in the TWC proposal a year ago. The book is a metric-based quantitative evaluation of the Reliability, Security and Privacy.

4) TWC Curriculum Improved

Curriculum for CIS 4451/6653 : COMPUTER SECURITY AND RELIABILITY(Sessions:75 min)

Trustworthy Computing course was developed during a period of seven years (2000-06) while teaching a course for students and practitioners on the recognition of data analytical and metric aspects of security and reliability modeling dealing with measuring software and hardware quality, and security. The course traditionally covered topics on trustworthy computing. However, over the years, I was not able to identify a single book that integrated coverage of applied and quantitative concepts dealing with Security and Reliability. The goal of the text book together with the references, and therefore the course is to establish metrics or indexes to quantify the common enemy - the malicious and nonmalicious risk − so as not to solely qualify the imminent danger within the conventional standards of high or medium or low risk. A cross product of computer security and reliability measures constitutes a concern that dominates today's world, which is now definitely data-driven, no longer verbal. Numerical data on security breaches and chance failures surround us. Innocent and malicious risk data must be collected, analyzed, and processed objectively to convert them into useful information not only to inform, but also to instruct, answer, or aid in decision making as to how to combat the disastrous consequences of the computer-addicted world of industry, commerce, finance, science and technology. The text book CD focuses on helping the reader to solve problems and to gain a sense of industrial experience. The object of the book is to provide an elementary and reasonably self-contained overview of the engineering aspects of trustworthiness in the most general sense of the word, integrating reliability, security and privacy.

Every course must have a solid and clear purpose for coming to life. The purpose of a new course curriculum such as this is to inform senior undergraduate or beginning graduate students across the board in engineering disciplines about new advances in reliability and security modeling with a metric-based quantitative approach as opposed to the more common verbal or qualitative or subjective case histories, which positively form some of the experiential background in the text book. Rather than what this course is about, what is this course not about? This course is not a collection of already available topics that can be found in a multitude of fine books, therefore avoiding repetitious information already available. It is objective, quantitative, empirical, metric-oriented, and data-driven. However, earlier methods that deal with reaching the new frontiers are examined. Therefore in Chapter 1, there is some, but minimal duplication of material widely available such as descriptions of the statistical probability distributions accompanied by their respective random number generations, and hardware reliability methods for components and systems, and software reliability-growth models. There are hyper-links to the book CD to work with projects that provide hands-on-experience.

The course begins with a review to provide the supplemental material necessary to train students with no previous knowledge of the basics of reliability theory as it relates both hardware and software, with practical applications. Although the material is available in many books and tutorials, a general treatment will enable the reader to understand the nomenclature used in the main body of the book without shuffling the pages of other books. In Chapter 1, we also study the simulation alternatives for each statistical probability distribution that exists in the literature, with a few exceptions, to model and calculate system or component availability when the analytical methods have serious shortcomings. The course continues with software reliability modeling of clustered failure data in an effort-based testing environment, taking up the less studied compound Poisson process approach in the first half of Chapter 2. Then, as a follow-up to the first half of the chapter, in the second half we study ways to compare forecast accuracy in a stochastic manner as opposed to the deterministic ways used conventionally. Multi-faceted quantitative modeling of security risk is studied in Chapter 3, from quantitative, qualitative and hybrid perspectives, with data analytical applications and estimation techniques of the risk parameters, as well as how to handle nondisjointness of vulnerabilities or threats, and how to prioritize during the maintenance cycle after assessment. Cost-effective stopping rules in an effort- and time-based failure environment are studied in Chapter 4, where economic rules of comparison are emphasized, with applications not only to software and hardware testing but also in the active business domains. In Chapter 5, we employ the Sahinoglu-Libby probability distribution to model the availability of hardware components in cyber-systems. Chapter 6 takes up the topic of reliability block diagramming to compute source-target reliability using various novel methods for simple and complex embedded systems. Each chapter explains why there is a need for the methods proposed in comparing the material presented with that covered conventionally. All chapters work toward creating mathematical-statistical but engineering-oriented metrics to best quantify the lack of risk, and the reliability of a system.

The improved curriculum will be outlined below
(Appendix: CurriculumCIS6653.pdf, brief.pdf)

Week 1

Session 1: A review of the course outline, rules and regulations. Introduction to reliability and hazard rate functions. Introduction to basic statistical concepts. Refer to Textbook Chapter 1.1 and 1.2.

Session 2: Common statistical distributions and generation of random variates. Refer to textbook Chapter 1.3.

Reading Assignment: Textbook Chapter 1

Week 2

Session 3: Life testing for component reliability in case of complete and incomplete data. Redundancy concepts and limitations in system reliability. Refer to textbook Chapter 1.4 and 1.5.

Session 4: What are software reliability, taxonomy and classifications? What are some of the software reliability growth models and their examples. Software applications. Refer to "PG (Poisson ^ Geometric)" and "NB (Negative Binomial)" radio buttons in T-Solver. Refer to Textbook Chapter 1.6.

Homework 1: Selected exercises from textbook Chapter 1.

Week 3

Session 5: Software reliability modeling using effort-based failure data. MLE (Maximum Likelihood Estimation) method in the Poisson ^ Geometric model. Applications to data sets. Refer to Textbook Chapter 2.1.

Reading Assignment: Textbook Chapter 2

Session 6: NLR (Nonlinear Regression) estimation method in the Poisson ^ Geometric model. SPSS applications to data sets. Comparison of Methods. Refer to textbook Chapter 2.1 and Appendix 2 for SPSS algorithms.

Week 4

Session 7: Statistical measures to compare the predictive accuracy of failure-count models using Bayesian approach. Refer to textbook Chapter 2.2.
Session 8: Software applications. Refer to "Flat", "One Sample t-test" and "Two Sample t-test" radio buttons in T-Solver.

Homework 2: Selected exercises from textbook Chapter 2.

Week 5

Session 9: Various approaches on the quantitative modeling for security risk assessment. Security meter design types. Refer to textbook Chapter 3.1. Software applications. Refer to "Security" radio button in T-Solver.

Reading Assignment: Chapter 3

Session 10: Prioritizing Security Maintenance using Bayesian method. Nondisjoint vulnerabilities and threats. Refer to textbook Chapter 3.2 and 3.3. Software applications. Refer to "Security" radio button in T-Solver.

Week 6

Session 11: Estimation of the Security meter input parameters. Security Risk Management. Simulation of the Risk Model. Refer to Textbook Chapter 3.4. Software applications. Refer to "Security" radio button in T-Solver.

Session 12: Quantification of lack of privacy and risk management. Refer to textbook Chapter 3.5. Software applications. Refer to “Privacy” radio button in T-Solver.

Week 7

Session 13: Introduction to encryption and decryption and types. Refer to Textbook Appendix 3.

Session 14: Cyber-Security laboratory applications on network testing using scanning tools, such as SuperScan and NetBrute scanners and implementing the “honeynet project” for enumerating vulnerabilities on security and privacy, and the breaches as simulated in cyber-space. Refer to reference textbooks for the scanning tools and honeynet.

Homework 3: Selected exercises from Chapter 3.

Week 8

Session 15: Review of Chapters 1, 2 and 3, and assignment of Term Project Part A due by semester’s end.

Session 16: Exam 1 (Textbook Chapters 1, 2 and 3)

Reading Assignment: Chapter 4

Week 9

Session 17: Introduction to Stopping Rule algorithms in hardware and software reliability testing. Effort-based stopping rule. Refer to textbook Chapter 4.1. Software applications. Go to “MESAT-1 and MESAT-2” radio buttons in T-Solver, and click MESAT-1.

Session 18: Study of high assurance testing in Business. Refer to Textbook Chapter 4.2. Software applications. Go to “MESAT 1” in T-Solver.

Week 10

Session 19: Stopping rule in time-domain. Refer to textbook Chapter Appendix 4.
Session 20: Software applications. Refer to textbook Chapter 4.3 and Appendix 4. Go to "MESAT-2" in T-Solver.

Week 11

Session 21: Introduction to Stopping Rule algorithms in hardware and software reliability testing. Effort-based stopping rule. Refer to textbook Chapter 4.1. Software applications. Go to "MESAT-1 – and MESAT-2" radio buttons in T-Solver, and click MESAT -1.

Session 22: Study of high assurance testing in Business. Refer to textbook Chapter 4.2. Software applications. Go to "MESAT-1" in T-Solver.

Homework 4: Selected exercises from Chapter 4. Assignment of Term Project Part B due by semester's end.

Week 12

Session 23: Availability Modeling using Sahinoglu-Libby Probability Model. Bayes estimators for Informative and Noninformative priors and various loss functions. Refer to textbook Chapters 5.1-5.4.

Reading Assignment: Chapter 5

Session 24: Component and system software applications. Refer to Textbook Chapter 5.5 and 5.6. Go to "ERBDC" radio button in T-Solver.

Homework 5: Selected exercises from Chapter 5. Assignment of Term Project Part C due by semester's end.

Week 13

Session 25: Inroduction to reliability block diagramming. Compression algorithm in simple parallel-series systems using Polish notation. Refer to textbook Chapters 6.1, 6.2 and 6.3. Go to “ERBDC” radio button in T-Solver.

Reading Assignment: Chapter 6

Session 26: Hybrid Tool to compute s-t reliability. New Polish-decoding algorithm. Refer to textbook Chapter 6.4 and 6.5. Software applications. Go to “Decoding” radio button in T-Solver.

Week 14

Session 27: Overlap technique and algorithm. Refer to textbook Chapter Appendix 6.7.
Session 28: Examples. Software applications. Refer to textbook Chapter Appendix 6. A-D. Go to “ERBDC” radio button in T-Solver.

Week 15

Session 29: Multistate System Reliability Evaluation. Refer to textbook Chapter 6.8.1 to 6.8.4.

Homework 6: Selected exercises from Chapter 6. Assignment of Term Project Part D due by semester’s end.

Session 30: Software applications. Refer to Textbook Chapter 6.8.5. Go to “ERBDC” radio button in T-Solver.

Week 16

Session 31: Exam II (from Chapters 4, 5 and 6). Term projects A-D due.

Session 32: Final Exam. End-of-semester course evaluation.

CS 6653 : COMPUTER SECURITY AND RELIABILITY (Spring 2007)

1) Instructor: Dr. M. Sahinoglu; TROY Univ.-Gunter Annex #111, Tel.832-7289,mesa@TROY.edu
2) Class Time and Location: T-Th 17.30-18:45pm., Gunter Annex 215
3) Office Hours: Tuesday: 13.00-15.00pm., Thursday 12.30-14.30
4) Prerequisite: As listed in TROY Univ. catalog
5) Exams, Homeworks, Grading/Make-Up Policy
   a) 4 HWs : 25 points each & mini-project: 25 bonus points. Total: 125
      No late submissions please!
   b) Exam 1 : April 12, 2006, Thurs ; Class-time, 125 points worth
      c) Exam 2(Term-Project): April 24, 2006, Tues; 125 points worth
   c) Final Exam : May 2, 2005, Tues. Class time, 150 points worth
   d) For exams, homeworks, only official hospital & police statements and documents are valid for make-ups, or preliminary permission is required from the instructor for any must-have absence.
   e) Grades will be be based on the following scale(curved):
      525<A<425<B<350<C<300<D<250

Text Book : "Trustworthy Computing" by M. Sahinoglu, J. Wiley
Reference : Intro. to Reliability Engineering, 2^{nd} Ed. by E. E. Lewis
Reference : Information Security Manual-Hands On, 2^{nd} Ed., by M. Whitman, H. J. Mattord and David M. Shackleford

TOPICS (SEE Text Book)

Week Dates	Tues	Thurs	Comments
(1) Jan 9, 11	S/Chap1	Chap1	*S:Syllabus*
(2) Jan 16, 18	Chap1	Chap1	
(3) Jan 30, Feb1	Chap2	Chap2	
(4) Jan 23, 25	Chap2	Chap2	
(5) Feb 6, Feb 8	Chap3	Chap3	
(6) Feb 7, 9	Chap3	Chap3	
(7) Feb 13, 15	Chap3	Chap3	
(8) Feb 20, 22	R,PrA	Exam1	*R: Review, PrA: Project A*
(9) Feb 27, Mar1	Chap4	Chap4	
Mar 6, Mar8	SPRING BREAK		
(10)Mar 13, 15	Chap4	Chap4	
(11)Mar 20, 22	Chap4	Chap4,PrB	*PrB: Project B*
(12)Mar 27, 29	Chap5	Chap5,PrC	*PrC: Project C*
(13)Apr 3, 5	Chap6	Chap6	
(14)Apr 10, 12	Chap6	Chap6	
(15)Apr 17, 19	Chap6	Chap6,PrD	*PrD: Project D*
(16)Apr 24, 26	Exam2	R,Proj due	*R: Review*
May 1	FINAL		

5) Budget Report

The initial report (A) and final conclusive (B) reports are summrized respectively below.

A) Initial budget report at the beginning:

memorandum

TO: Leigh Ann Paramore, Sponsored Program Accounting

FROM: Mehmet Sahinoglu, Computer Science
Judy Brighton-Enfinger, Sponsored Programs

RE: **Microsoft Research Trustworthy Computing Curriculum**

DATE: Wednesday, February 08, 2006

The **Microsoft Research Trustworthy Computing Curriculum** grant has been approved for funding. The budget commences January 1, 2006 and ends December 31, 2006. Please budget the following accounts for this project:

The following account number (123-202262) should be entitled (Microsoft Trustworthy Computing). All references to this account should include this exact title.

Revenue

Revenue	
123-202262-5337-33	50,000.00

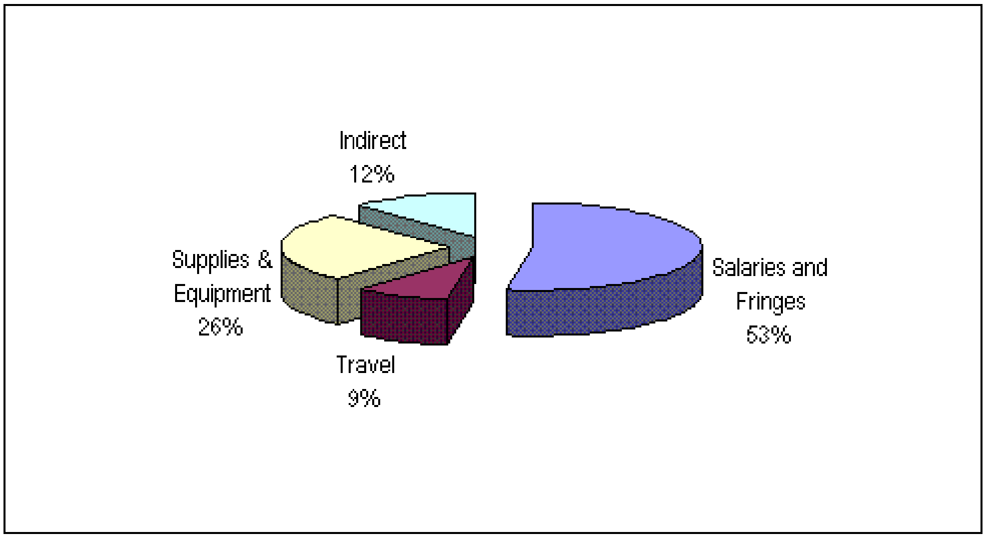
Expenditures

Salaries--Teaching	
123-202262-6011-33	18,430.00
Graduate Assistants Research	
123-202262-6033-33	4,875.00
Wages—Secretary	
123-202262-6041-33	2,091.00
Printing	
123-202262-6111-33	214.00
Travel	
123-202262-6115-33	2,500.00
Non Capitalized Equipment	
123-202262-6197-33	12,504.00
Social Security	
123-202262-6303-33	1,570.00
Retirement	
123-202262-6308-33	1,676.00
Indirect Cost	
123-202262-8106-33	6,140.00
Total	50,000

B) FINAL BUDGET REPORT at the conclusion of the grant

	2005-2006	2006-2007	Total Spent	Balance
Microsoft Award (50,000)				
Salaries	13,822.47	4,607.49	18,429.96	0.04
Graduate Assistants Teaching	400.00		400.00	4,475.00
Wages--Secretary	1,400.00		1,400.00	691.00
Wages--Other, Part-Time	725.61	2,306.79	3,032.40	(3,032.40)
Printing				214.00
Travel		4,506.74	4,506.74	(2,006.74)
Instructional Supplies	266.40		266.40	(266.40)
Non Capitalized Equipment	12,181.61	631.46	12,813.07	(309.07)
Social Security	1,101.64	234.74	1,336.38	233.62
Retirement	1,243.80	431.25	1,675.05	0.95
Indirect Costs	4,359.81	1,780.19	6,140.00	-
	35,501.34	14,498.66	50,000.00	0.00

Salaries and Fringes	26,273.79
Travel	4,506.74
Supplies & Equipment	13,079.47
Indirect	6,140.00
Total	50,000.00



Note that Troy University contributed with tables, chairs and classroom gadgets including some of the teaching equipment like projector and screen, and some peripherals.

ICS donated the rack equipment as follows:

(9) Cisco 2500 routers @ $200 = $1800

(1) Cisco 2900 Series Switch @ $500= $500

(1) Cisco Internet Access Device @$250 =$250

(1) Cisco PIX Firewall @ $500= $500

(1) Cisco Voice Gateway @ $350=$350

(1) Cisco Content Engine 507 @ $1700=$1700

(2) Netscreen 100 Firewalls @$750= $1500

(2) Netscreen 5XT Firewalls@ $600 =$1200

(2) Sun Enterprise 250 Servers @ $2000= $4000

For a grand total of $11800.00.

6) Present and Future Challenges:

a) The most important challenge next to the curriculum development following the teaching of this course in two different terms (with its challenges of feedback inputs from the participating students) was the establishment of the security laboratory to connect with the requirements of those of the course. The lab was designed with two main parts. One part was the rack to contain all the routers and firewalls etc. and the other was the production and independent PCs for the Honeynet project, both illustrated in Figures 1 and 2 respectively. Figure 3 proposes a new lab formation for future studies outlined in the next Section as a follow-up to this grant activitiy.

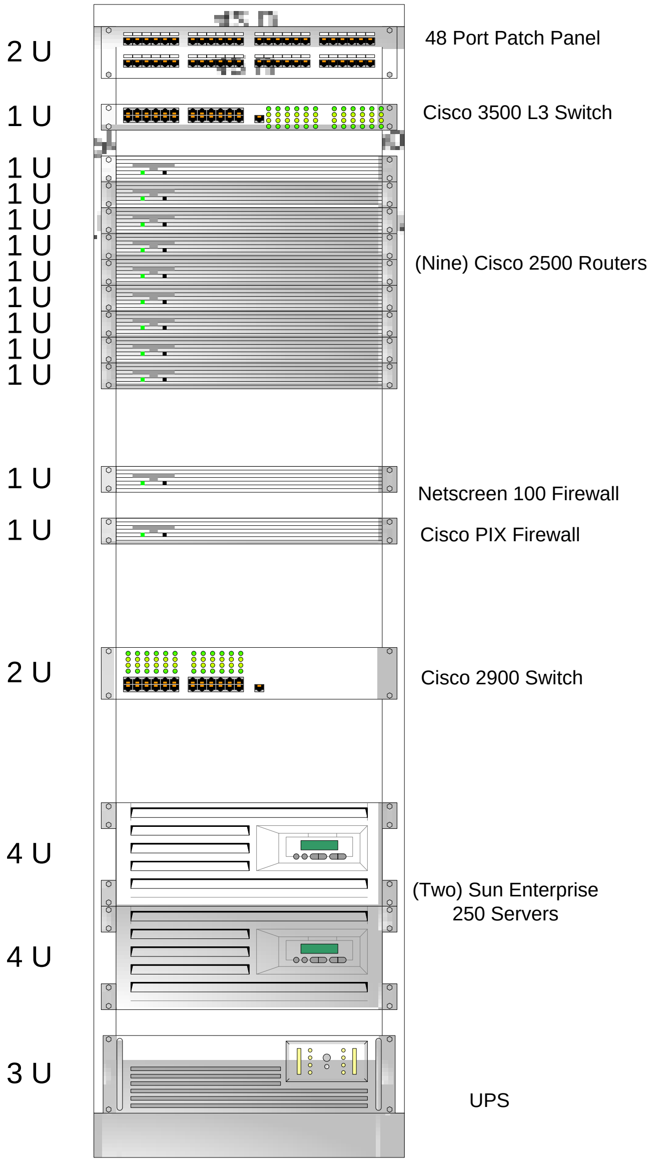


Figure 1: Troy Univ. Computer Science Security Lab's Rack Layout (donated by ICS)

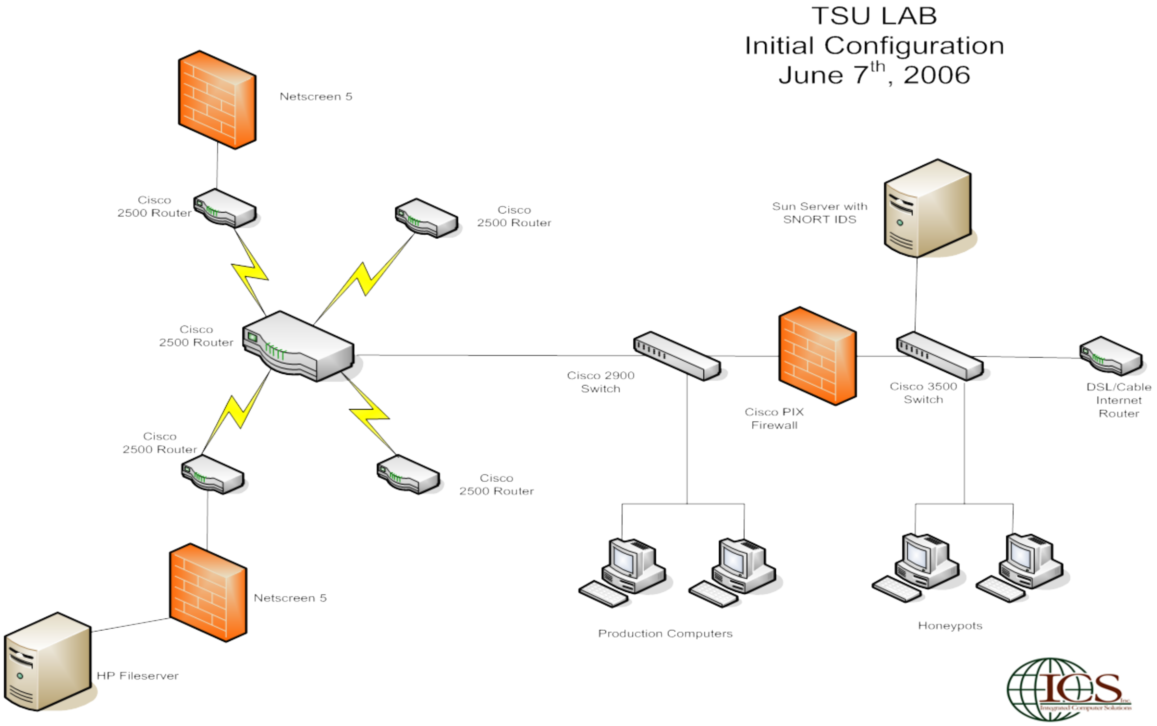


Figure 2. The Established TWC Curriculum Lab per Microsoft Grant Proposal (2006)

b) For future planning, the following topology is proposed. The future work is described.

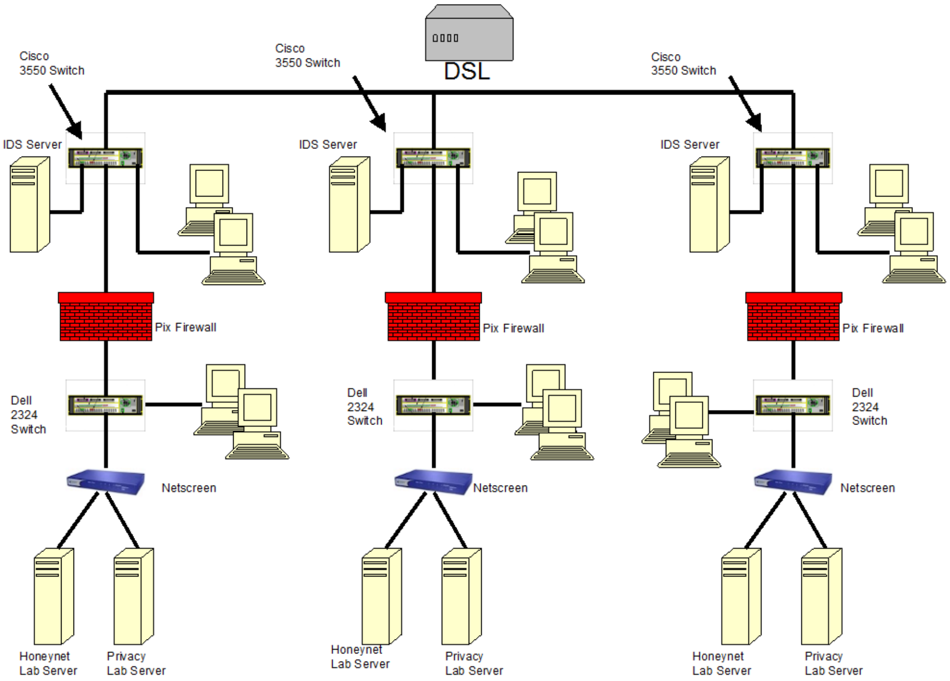


Figure 3. A Proposed Lab Topology for A Future Study

Trustworthy Computing through Quantitative Risk Assessment and Management with proposed Security and Privacy-Meter Models & Lab-Environment Simulation:

This research aims at a paradigm of transitions from conventional discrete risk levels such as "high, mild or low" to a framework of formulating and computing the continuous quantitative indices of lack of security and privacy. This objective lends to a cost-benefit based improvement in security-privacy risk mitigation of computer systems&components.

Several security risk templates employ non-quantitative attributes to express a risk's severity. This approach is highly subjective, and void of actual figures. The PI's design provides a quantitative and hybrid technique with an updated repository on vulnerabilities, threats, and countermeasures to calculate risk. A simulation study will be undertaken to verify the theoretical results.

On the privacy side, given a set of data to indicate privacy invasions, such as in the case of phishing, spam, spoofing, tampering, bots, worms, trojans and other social engineering sorts of malicious malware, a probability distribution function is proposed to conduct statistical inference. The objective is to estimate the probability (likelihood) of the number of breaches within a given period of time under the conditions encountered. Once the pdf is accomplished, then the cumulative and survival probability functions can be estimated to respond to questions such as what is the probability of encountering less than or more than a given number of privacy breaches or incidents. Then once the countermeasures are taken and improvements are made, one can compare the new with the status-quo in terms of cost and benefit dollars in a strictly quantitative manner. Monte-Cartlo simulation studies will also verify the theoretical results.

Finally, for both objectives, a laboratory environment will be established to conduct experimentations on emulating and mimicking the real life scenarios. For security risk studies, projects like honeynet etc. will be applied for enumeration purposes to use in the mathematical model suggested. For privacy experimentations, aside from software projects live human subjects may be used to see the effect of identity thefts. Stopping rules through cost-effective testing to decide on the security and privacy approvals will be determined.

The combined hardware/software proposal to improve trustworthiness will also enable the PI and Co-PI to integrate with the educational content of the related course materials on Software Engineering, and Security/Reliability themed courses in the Computer Sciences at Troy University. This is in alignment with the President's committee (PITAC) guidelines to raise the computer security and privacy awareness in Higher Education.

The multidisciplinary project team will accomplish goals by (a) Formulating the modeling objectives by PI and Co-PI. (b) Establishing a quasi-real life laboratory environment to collect data and evidence from this lab and other sources over the cyberspace. See: Power Point diagram attachment-no new lab space needed. The 6-rack lab of Figure 1 will now be dedicated solely for the dual purpose of security and privacy breaches. (c) Activating the proposed cyber-security models towards a prototype software product.

7) Conclusion and Acknowledgements

This report is made from a collection of chronological events documented from the inception of the idea to its finalization. As outlined above, the two core objectives have been met, a) The curriculum has been improved from what it has been before b) A security lab has been established in connection with the curriculum objectives c) Pertinent academic and scholarly activities for the present and future research have been listed.

The closing presentation took place on February 8, 2007 before the Troy University's interim Vice-Chancellor of Montgomery Campus (Ray White), Dean of Science (Dr. D. Jeffrey), Associate Dean of Science (Dr. W.S. Richardson), Chairperson of the Department of Computer Science (Dr. I. Ozkarahan), Vice Chancellor for Undergraduate Studies (Dr. H. Fulmer), Director of Sponsored Programs (Judy Enfinger), Montgomery Campus Computer Services Director (Charles Weaver) and Professor of Computer Science (Dr. Sunil Das). We owe thanks for their attendance and support from A to Z.

This report was presented in the form of PowerPoint slides on February 8, 2007 and at the end the TWC curriculum was proposed in detail along with a lab presentation.

This grant research plan would not be a reality without the relentless efforts and assistance of Dr. William Richardson, Judy Enfinger, Leigh Ann Paramore and Kristy Franklin at Troy University's sponsored programs in Troy; USAF Capt. Rob Barclay (Network and Lab Coordinator from June 2006 on) Angela Crooks (Project Administrative Asst. until Sept. 2006), not to forget CS System Admin (John F. Cole until Dec. 2006), Mindy Kramer of the College of Arts and Sciences, Bob Biersack at the Help Desk, Jim Davis and Sharon Gantt all from Computer Services, Scott Morton and Debbie Harlan-Brooks (both since Jan. 2007) all at Montgomery campus.

Our thanks go to Steve Goldsby, CEO of the ICS in Montgomery for his gracious help in leading the laboratory to its present day status. The entire ICS personnel (Will Millar and many other valuable names) did all they could to make this lab a working machine.

The report shows, beside the chronological events, the deliverables such as

1) The curriculum for the TWC
2) The laboratory element to accompany the curriculum
3) The activities during the grant year in terms of invited conferences, trips and progress reports.

Last but certainly not least, my deep appreciation goes to Microsoft TWC Consortium for providing the grant, and guidance with contact person John Spencer (retired) and others from Microsoft. It has been a year of learning, experience and brainstorming. Many thanks to Professors Ganz (U-Mass), Li (U of FL) and Kim (Yonsei - Korea) - fellow grantees for their academic collaborations- and all of the unsung important heroes who helped my team and the PI to make this research a successful scientific journey, and a reference for future.

May I finally present many thanks to all those involved from A to Z in this project.

ELECTRONIC APPENDIX (See Folder)

2005 RFP Awards and Project Summaries.

Local Press releases.

Invitation by Microsoft to Academic Days on TWC in Redmond, WA April 7-9 2006.

Information Security summer school on May 22-24, 2006 at FSU, Tallahassee, FL.

Research trip to the University of Florida, Gainesville, to meet and discuss with Tau Li, a 2006 TWC grant recipient.

Invitation to Yonsei University, Korea by B. Kim, a 2006 TWC grant recipient, to speak as a keynote at an International Digital Technology

Invitation to CIS at UAB to present a talk on TWC topics.

Invitation to ECE Dept at University of Massachusetts in Amherst, MA to present a talk on TWC topics by a 2006 TWC grant recipient.

Presentation of PowerPoint slides.

REFERENCES

[1] **Trustworthy Computing Curriculum**: Microsoft Research will fund a variety of projects to create, test, and disseminate new curriculum introducing advanced topics of Trustworthy Computing such as Security, Privacy, Reliability, Business Integrity, or Secure Software Engineering. The total amount available under this RFP is $750,000.00 (US). Microsoft Research anticipates making approximately fifteen awards with a maximum of $50,000 (US) for any single award. All awards will be in US dollars. More information on this topic is available at: http://research.microsoft.com/ur/us/fundingopps/RFPs/TWC_Curriculum_2005_RFP.aspx

[2] http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf

[3] http://www.troy.edu/catalogs/0506undergrad/U16CS.htm#COMPUTER%20SCIENCE%20COURSES%20(CS).

[4] http://research.microsoft.com/ur/us/fundingopps/RFPs/TWC_Curriculum_2005_RFP_Awards.aspx

[5] http://www.sdpsnet.org/images/2006proc.pdf

[6] http://www.sdpsnet.org/images/2007proc.pdf

[7] http://www.wiley.com/WileyCDA/WileyTitle/productCd-0470085126,descCd-tableOfContents.html