02 INFORMATION ABOUT PRINCIPAL INVESTIGATORS/PROJECT DIRECTORS(PI/PD) and co-PRINCIPAL INVESTIGATORS/co-PROJECT DIRECTORS

Submit only ONE copy of this form **for each PI/PD and co-PI/PD** identified on the proposal. The form(s) should be attached to the original proposal as specified in GPG Section II.C.a. Submission of this information is voluntary and is not a precondition of award. This information will not be disclosed to external peer reviewers. ***DO NOT INCLUDE THIS FORM WITH ANY OF THE OTHER COPIES OF YOUR PROPOSAL AS THIS MAY COMPROMISE THE CONFIDENTIALITY OF THE INFORMATION.***

PI/PD Name: Bo Yuan

Gender: ☒ Male ☐ Female

Ethnicity: (Choose one response) ☐ Hispanic or Latino ☒ Not Hispanic or Latino

Race: (Select one or more)
- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White

Disability Status: (Select one or more)
- ☐ Hearing Impairment
- ☐ Visual Impairment
- ☐ Mobility/Orthopedic Impairment
- ☐ Other
- ☒ None

Citizenship: (Choose one) ☒ U.S. Citizen ☐ Permanent Resident ☐ Other non-U.S. Citizen

Check here if you do not wish to provide any or all of the above information (excluding PI/PD name): ☐

REQUIRED: Check here if you are currently serving (or have previously served) as a PI, co-PI or PD on any federally funded project ☐

Ethnicity Definition:
Hispanic or Latino. A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race.

Race Definitions:
American Indian or Alaska Native. A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
Asian. A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
Black or African American. A person having origins in any of the black racial groups of Africa.
Native Hawaiian or Other Pacific Islander. A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
White. A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

WHY THIS INFORMATION IS BEING REQUESTED:

The Federal Government has a continuing commitment to monitor the operation of its review and award processes to identify and address any inequities based on gender, race, ethnicity, or disability of its proposed PIs/PDs. To gather information needed for this important task, the proposer should submit a single copy of this form for each identified PI/PD with each proposal. Submission of the requested information is voluntary and will not affect the organization's eligibility for an award. However, information not submitted will seriously undermine the statistical validity, and therefore the usefulness, of information recieved from others. Any individual not wishing to submit some or all the information should check the box provided for this purpose. (The exceptions are the PI/PD name and the information about prior Federal support, the last question above.)

Collection of this information is authorized by the NSF Act of 1950, as amended, 42 U.S.C. 1861, et seq. Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational oppurtunities; and to assess involvement of international investigators in work supported by NSF. The information may be disclosed to government contractors, experts, volunteers and researchers to complete assigned work; and to other government agencies in order to coordinate and assess programs. The information may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records", 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records", 63 Federal Register 268 (January 5, 1998).

02 INFORMATION ABOUT PRINCIPAL INVESTIGATORS/PROJECT DIRECTORS(PI/PD) and co-PRINCIPAL INVESTIGATORS/co-PROJECT DIRECTORS

Submit only ONE copy of this form **for each PI/PD and co-PI/PD** identified on the proposal. The form(s) should be attached to the original proposal as specified in GPG Section II.C.a. Submission of this information is voluntary and is not a precondition of award. This information will not be disclosed to external peer reviewers. ***DO NOT INCLUDE THIS FORM WITH ANY OF THE OTHER COPIES OF YOUR PROPOSAL AS THIS MAY COMPROMISE THE CONFIDENTIALITY OF THE INFORMATION.***

PI/PD Name: Andrew P Meneely

Gender: ☒ Male ☐ Female

Ethnicity: (Choose one response) ☐ Hispanic or Latino ☒ Not Hispanic or Latino

Race: (Select one or more)
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☒ White

Disability Status: (Select one or more)
- ☐ Hearing Impairment
- ☐ Visual Impairment
- ☐ Mobility/Orthopedic Impairment
- ☐ Other
- ☐ None

Citizenship: (Choose one) ☒ U.S. Citizen ☐ Permanent Resident ☐ Other non-U.S. Citizen

Check here if you do not wish to provide any or all of the above information (excluding PI/PD name): ☒

REQUIRED: Check here if you are currently serving (or have previously served) as a PI, co-PI or PD on any federally funded project ☒

Ethnicity Definition:
Hispanic or Latino. A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race.
Race Definitions:
American Indian or Alaska Native. A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
Asian. A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
Black or African American. A person having origins in any of the black racial groups of Africa.
Native Hawaiian or Other Pacific Islander. A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
White. A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

WHY THIS INFORMATION IS BEING REQUESTED:

The Federal Government has a continuing commitment to monitor the operation of its review and award processes to identify and address any inequities based on gender, race, ethnicity, or disability of its proposed PIs/PDs. To gather information needed for this important task, the proposer should submit a single copy of this form for each identified PI/PD with each proposal. Submission of the requested information is voluntary and will not affect the organization's eligibility for an award. However, information not submitted will seriously undermine the statistical validity, and therefore the usefulness, of information recieved from others. Any individual not wishing to submit some or all the information should check the box provided for this purpose. (The exceptions are the PI/PD name and the information about prior Federal support, the last question above.)

Collection of this information is authorized by the NSF Act of 1950, as amended, 42 U.S.C. 1861, et seq. Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational oppurtunities; and to assess involvement of international investigators in work supported by NSF. The information may be disclosed to government contractors, experts, volunteers and researchers to complete assigned work; and to other government agencies in order to coordinate and assess programs. The information may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records", 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records", 63 Federal Register 268 (January 5, 1998).

02 INFORMATION ABOUT PRINCIPAL INVESTIGATORS/PROJECT DIRECTORS(PI/PD) and co-PRINCIPAL INVESTIGATORS/co-PROJECT DIRECTORS

Submit only ONE copy of this form **for each PI/PD and co-PI/PD** identified on the proposal. The form(s) should be attached to the original proposal as specified in GPG Section II.C.a. Submission of this information is voluntary and is not a precondition of award. This information will not be disclosed to external peer reviewers. ***DO NOT INCLUDE THIS FORM WITH ANY OF THE OTHER COPIES OF YOUR PROPOSAL AS THIS MAY COMPROMISE THE CONFIDENTIALITY OF THE INFORMATION.***

PI/PD Name: Rajendra K Raj

Gender: ☒ Male ☐ Female

Ethnicity: (Choose one response) ☐ Hispanic or Latino ☒ Not Hispanic or Latino

Race: (Select one or more)
- ☐ American Indian or Alaska Native
- ☒ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White

Disability Status: (Select one or more)
- ☐ Hearing Impairment
- ☐ Visual Impairment
- ☐ Mobility/Orthopedic Impairment
- ☐ Other
- ☒ None

Citizenship: (Choose one) ☒ U.S. Citizen ☐ Permanent Resident ☐ Other non-U.S. Citizen

Check here if you do not wish to provide any or all of the above information (excluding PI/PD name): ☐

REQUIRED: Check here if you are currently serving (or have previously served) as a PI, co-PI or PD on any federally funded project ☒

Ethnicity Definition:
Hispanic or Latino. A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race.
Race Definitions:
American Indian or Alaska Native. A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
Asian. A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
Black or African American. A person having origins in any of the black racial groups of Africa.
Native Hawaiian or Other Pacific Islander. A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
White. A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

WHY THIS INFORMATION IS BEING REQUESTED:

The Federal Government has a continuing commitment to monitor the operation of its review and award processes to identify and address any inequities based on gender, race, ethnicity, or disability of its proposed PIs/PDs. To gather information needed for this important task, the proposer should submit a single copy of this form for each identified PI/PD with each proposal. Submission of the requested information is voluntary and will not affect the organization's eligibility for an award. However, information not submitted will seriously undermine the statistical validity, and therefore the usefulness, of information recieved from others. Any individual not wishing to submit some or all the information should check the box provided for this purpose. (The exceptions are the PI/PD name and the information about prior Federal support, the last question above.)

Collection of this information is authorized by the NSF Act of 1950, as amended, 42 U.S.C. 1861, et seq. Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational oppurtunities; and to assess involvement of international investigators in work supported by NSF. The information may be disclosed to government contractors, experts, volunteers and researchers to complete assigned work; and to other government agencies in order to coordinate and assess programs. The information may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records", 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records", 63 Federal Register 268 (January 5, 1998).

List of Suggested Reviewers or Reviewers Not To Include (optional)

SUGGESTED REVIEWERS:
Not Listed

REVIEWERS NOT TO INCLUDE:
Not Listed

COVER SHEET FOR PROPOSAL TO THE NATIONAL SCIENCE FOUNDATION

PROGRAM ANNOUNCEMENT/SOLICITATION NO./CLOSING DATE/if not in response to a program announcement/solicitation enter NSF 13-1

NSF 14-510 **02/11/14**

FOR CONSIDERATION BY NSF ORGANIZATION UNIT(S) (Indicate the most specific unit known, i.e. program, division, etc.)

DUE - SFS-Scholarships

FOR NSF USE ONLY

NSF PROPOSAL NUMBER

1433736

DATE RECEIVED	NUMBER OF COPIES	DIVISION ASSIGNED	FUND CODE	DUNS# (Data Universal Numbering System)	FILE LOCATION
02/11/2014	**1**	**11040000 DUE**	**1668**	**002223642**	**12/22/2014 1:41pm S**

EMPLOYER IDENTIFICATION NUMBER (EIN) OR TAXPAYER IDENTIFICATION NUMBER (TIN)

160743140

SHOW PREVIOUS AWARD NO. IF THIS IS
☐ A RENEWAL
☐ AN ACCOMPLISHMENT-BASED RENEWAL

IS THIS PROPOSAL BEING SUBMITTED TO ANOTHER FEDERAL AGENCY? YES ☐ NO ☒ IF YES, LIST ACRONYM(S)

NAME OF ORGANIZATION TO WHICH AWARD SHOULD BE MADE

Rochester Institute of Tech

AWARDEE ORGANIZATION CODE (IF KNOWN)

0028068000

ADDRESS OF AWARDEE ORGANIZATION, INCLUDING 9 DIGIT ZIP CODE

Rochester Institute of Tech
1 Lomb Memoria Drive
Rochester, NY. 146235603

NAME OF PRIMARY PLACE OF PERF

Rochester Institute of Tech

ADDRESS OF PRIMARY PLACE OF PERF, INCLUDING 9 DIGIT ZIP CODE

Rochester Institute of Tech

NY ,146235603 ,US.

IS AWARDEE ORGANIZATION (Check All That Apply) (See GPG II.C For Definitions)
☐ SMALL BUSINESS ☐ MINORITY BUSINESS ☐ FOR-PROFIT ORGANIZATION ☐ WOMAN-OWNED BUSINESS

☐ IF THIS IS A PRELIMINARY PROPOSAL THEN CHECK HERE

TITLE OF PROPOSED PROJECT **SFS: Preparing Crosscutting Cybersecurity Scholars**

REQUESTED AMOUNT	PROPOSED DURATION (1-60 MONTHS)	REQUESTED STARTING DATE	SHOW RELATED PRELIMINARY PROPOSAL NO. IF APPLICABLE
$ **1,711,626**	**36** months	**09/01/14**	

CHECK APPROPRIATE BOX(ES) IF THIS PROPOSAL INCLUDES ANY OF THE ITEMS LISTED BELOW

☐ BEGINNING INVESTIGATOR (GPG I.G.2)
☐ DISCLOSURE OF LOBBYING ACTIVITIES (GPG II.C.1.e)
☐ PROPRIETARY & PRIVILEGED INFORMATION (GPG I.D, II.C.1.d)
☐ HISTORIC PLACES (GPG II.C.2.j)
☐ EAGER* (GPG II.D.2) ☐ RAPID** (GPG II.D.1)
☐ VERTEBRATE ANIMALS (GPG II.D.6) IACUC App. Date _____
PHS Animal Welfare Assurance Number _____

☐ HUMAN SUBJECTS (GPG II.D.7) Human Subjects Assurance Number _____
Exemption Subsection _____ or IRB App. Date _____
☐ INTERNATIONAL COOPERATIVE ACTIVITIES: COUNTRY/COUNTRIES INVOLVED (GPG II.C.2.j)
_____

PI/PD DEPARTMENT
Computing Security

PI/PD FAX NUMBER
585-475-2181

PI/PD POSTAL ADDRESS
1 LOMB MEMORIAL DR

ROCHESTER, NY 146235603
United States

NAMES (TYPED)	High Degree	Yr of Degree	Telephone Number	Email Address
PI/PD NAME **Bo Yuan**	**PhD**	**1996**	**585-475-4468**	**bo.yuan@rit.edu**
CO-PI/PD **Andrew P Meneely**	**PhD**	**2011**	**585-475-7829**	**axmvse@rit.edu**
CO-PI/PD **Rajendra K Raj**	**PhD**	**1991**	**585-475-2595**	**rkr@cs.rit.edu**
CO-PI/PD				
CO-PI/PD				

CERTIFICATION PAGE

Certification for Authorized Organizational Representative (or Equivalent) or Individual Applicant

By electronically signing and submitting this proposal, the Authorized Organizational Representative (AOR) or Individual Applicant is: (1) certifying that statements made herein are true and complete to the best of his/her knowledge; and (2) agreeing to accept the obligation to comply with NSF award terms and conditions if an award is made as a result of this application. Further, the applicant is hereby providing certifications regarding conflict of interest (when applicable), drug-free workplace, debarment and suspension, lobbying activities (see below), nondiscrimination, flood hazard insurance (when applicable), responsible conduct of research, organizational support, Federal tax obligations, unpaid Federal tax liability, and criminal convictions as set forth in the NSF Proposal & Award Policies & Procedures Guide,Part I: the Grant Proposal Guide (GPG). Willful provision of false information in this application and its supporting documents or in reports required under an ensuing award is a criminal offense (U.S. Code, Title 18, Section 1001).

Conflict of Interest Certification

When the proposing organization employs more than fifty persons, the Authorized Organizational Representative (or equivalent) is required to complete the following certification regarding Conflict of Interest:
By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) is certifying that the organization has implemented a written and enforced conflict of interest policy that is consistent with the provisions of the NSF Proposal & Award Policies & Procedures Guide, Part II, Award & Administration Guide (AAG) Section IV.A; that to the best of his/her knowledge, all financial disclosures required by that conflict of interest policy have been made; and that all identified conflicts of interest will have been satisfactorily managed, reduced or eliminated prior to the organization's expenditure of any funds under the award, in accordance with the organization's conflict of interest policy. Conflicts which cannot be satisfactorily managed, reduced or eliminated must be disclosed to NSF.

Drug Free Work Place Certification

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent), is providing the Drug Free Work Place Certification contained in Exhibit II-3 of the Grant Proposal Guide.

Debarment and Suspension Certification

(If answer "yes", please provide explanation.)

Is the organization or its principals presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency? Yes ☐ No ☒

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) or Individual Applicant is providing the Debarment and Suspension Certification contained in Exhibit II-4 of the Grant Proposal Guide.

Certification Regarding Lobbying

This certification is required for an award of a Federal contract, grant, or cooperative agreement exceeding $100,000 and for an award of a Federal loan or a commitment providing for the United States to insure or guarantee a loan exceeding $150,000.

Certification for Contracts, Grants, Loans and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:
(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.
(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, ''Disclosure of Lobbying Activities,'' in accordance with its instructions.
(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Certification Regarding Nondiscrimination

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) is providing the Certification Regarding Nondiscrimination contained in Exhibit II-6 of the Grant Proposal Guide.

Certification Regarding Flood Hazard Insurance

Two sections of the National Flood Insurance Act of 1968 (42 USC §4012a and §4106) bar Federal agencies from giving financial assistance for acquisition or construction purposes in any area identified by the Federal Emergency Management Agency (FEMA) as having special flood hazards unless the:
(1) community in which that area is located participates in the national flood insurance program; and
(2) building (and any related equipment) is covered by adequate flood insurance.

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) or Individual Applicant located in FEMA-designated special flood hazard areas is certifying that adequate flood insurance has been or will be obtained in the following situations:
(1) for NSF grants for the construction of a building or facility, regardless of the dollar amount of the grant; and
(2) for other NSF grants when more than $25,000 has been budgeted in the proposal for repair, alteration or improvement (construction) of a building or facility.

Certification Regarding Responsible Conduct of Research (RCR)
(This certification is not applicable to proposals for conferences, symposia, and workshops.)

By electronically signing the Certification Pages, the Authorized Organizational Representative is certifying that, in accordance with the NSF Proposal & Award Policies & Procedures Guide, Part II, Award & Administration Guide (AAG) Chapter IV.B., the institution has a plan in place to provide appropriate training and oversight in the responsible and ethical conduct of research to undergraduates, graduate students and postdoctoral researchers who will be supported by NSF to conduct research.
The AOR shall require that the language of this certification be included in any award documents for all subawards at all tiers.

CERTIFICATION PAGE - CONTINUED

Certification Regarding Organizational Support

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) is certifying that there is organizational support for the proposal as required by Section 526 of the America COMPETES Reauthorization Act of 2010. This support extends to the portion of the proposal developed to satisfy the Broader Impacts Review Criterion as well as the Intellectual Merit Review Criterion, and any additional review criteria specified in the solicitation. Organizational support will be made available, as described in the proposal, in order to address the broader impacts and intellectual merit activities to be undertaken.

Certification Regarding Federal Tax Obligations

When the proposal exceeds $5,000,000, the Authorized Organizational Representative (or equivalent) is required to complete the following certification regarding Federal tax obligations. By electronically signing the Certification pages, the Authorized Organizational Representative is certifying that, to the best of their knowledge and belief, the proposing organization:
(1) has filed all Federal tax returns required during the three years preceding this certification;
(2) has not been convicted of a criminal offense under the Internal Revenue Code of 1986; and
(3) has not, more than 90 days prior to this certification, been notified of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

Certification Regarding Unpaid Federal Tax Liability

When the proposing organization is a corporation, the Authorized Organizational Representative (or equivalent) is required to complete the following certification regarding Federal Tax Liability:

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) is certifying that the corporation has no unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

Certification Regarding Criminal Convictions

When the proposing organization is a corporation, the Authorized Organizational Representative (or equivalent) is required to complete the following certification regarding Criminal Convictions:

By electronically signing the Certification Pages, the Authorized Organizational Representative (or equivalent) is certifying that the corporation has not been convicted of a felony criminal violation under any Federal law within the 24 months preceding the date on which the certification is signed.

AUTHORIZED ORGANIZATIONAL REPRESENTATIVE	SIGNATURE	DATE
NAME **David Bond**	**Electronic Signature**	**Feb 14 2014 4:43PM**

TELEPHONE NUMBER	EMAIL ADDRESS	FAX NUMBER
585-475-4987	**dmbsrs@rit.edu**	**585-475-7990**

* EAGER - EArly-concept Grants for Exploratory Research
** RAPID - Grants for Rapid Response Research

NATIONAL SCIENCE FOUNDATION
Division of Undergraduate Education

NSF FORM 1295: PROJECT DATA FORM

The instructions and codes to be used in completing this form are provided in Appendix II.

1. **Program-track** to which the Proposal is submitted: **SFS-Scholarships**
2. Name of **Principal Investigator/Project Director** (as shown on the Cover Sheet):
   Yuan, Bo
3. Name of submitting **Institution** (as shown on Cover Sheet):
   Rochester Institute of Tech
4. **Other Institutions** involved in the project's operation:

Project Data:

A. Major Discipline Code: **35**
B. Academic Focus Level of Project: **GU**
C. Highest Degree Code: **D**
D. Category Code: **--**
E. Business/Industry Participation Code: **NA**
F. Audience Code: _ _ _ _ _ _ _ _
G. Institution Code: **PRIV**
H. Strategic Area Code: **IT**
I. Project Features: **4** _ _ _ _

Estimated number in each of the following categories to be directly affected by the activities of the project during its operation:

J. Undergraduate Students: **12**
K. Pre-college Students: **0**
L. College Faculty: **3**
M. Pre-college Teachers: **0**
N. Graduate Students: **12**

PROJECT SUMMARY

Overview:

Rochester Institute of Technology plans to establish a three year CyberCorps Scholarship for Service (SFS) program to support six exceptional students annually: two students from each of three BS+MS programs in Computing Security, Computer Science, and Software Engineering. These students will receive an MS degree in Computing Security in addition to a BS in their respective programs upon graduation. In the BS+MS program, students will take three graduate-level courses during their undergraduate study, which will allow completion of graduate work within one year. The scholarship program will recognize talented students from the three outstanding undergraduate computing programs at RIT, who will then be given the opportunity to join their respective BS+MS programs and receive the scholarship for the last two years of study.

This proposal aims to leverage the well-established Computing Security, Computer Science, and Software Engineering programs to foster and educate next generation cybersecurity professionals and leaders to secure and protect our national infrastructures and interests.

Intellectual Merit :

The intellectual merit of this proposal is based on a cohort experience of students from multiple disciplines in a practical setting. More specifically:

Like the three PIs, students in each cohort will be from three different computing majors, thus enabling faculty and students to shape one another's differing perspectives on the crosscutting discipline of cybersecurity.

The cohort experience will be facilitated by common coursework, monthly seminars, work on research projects, and travel to security conferences.

SFS scholars placed on federal internships will build on RIT's well-established undergraduate cooperative education (co-op) model that yields students, thus will be able to contribute to cybersecurity operations before and immediately after graduation.

This proposal leverages RIT's infrastructure, diverse programs, faculty resources, and industry/military relationships to support a pool of qualified candidates who might not otherwise be able to pursue graduate study in cybersecurity.

Broader Impacts :

RIT's SFS graduates will secure, protect and improve our nation's cyberinfrastructure.

With their crosscutting breadth of knowledge and experiences, these SFS graduates will be ready to adapt to a variety of cybcersecurity challenges at diverse federal agencies.

Scholarly contributions made by the SFS scholars will be disseminated at professional conferences relating to cybersecurity.

Building on their prior record of disseminating educational issues, the PIs will discuss lessons learned in running this SFS program at appropriate venues in educational and federal settings.

Working with RIT's K-12 office, the PIs and the SFS scholars will visit the City of Rochester schools with a large population of underrepresented groups in computing. Student scholars will promote awareness of cybersecurity issues facing to the nation and teach students basic knowledge about how to protect themselves online.

TABLE OF CONTENTS

For font size and page formatting specifications, see GPG section II.B.2.

*Proposers may select any numbering mechanism for the proposal. The entire proposal however, must be paginated. Complete both columns only if the proposal is numbered consecutively.

Preparing Crosscutting Cybersecurity Scholars

1 Overview

Rochester Institute of Technology plans to establish a three-year Scholarships for Service (SFS) program to support two cohorts, each with 6 exceptional students, for a double BS+MS degree.

We anticipate each cohort to have students from three undergraduate programs: Computer Science (CS), Software Engineering (SE), and Computing Security (CSEC). These students will receive an MS degree in CSEC in addition to a BS in their respective programs upon graduation. Students will take three graduate-level courses from the CSEC department during their undergraduate study, which will allow completion of their graduate work with only one extra year. This scholarship program will recognize talented students who will then be given the opportunity to join the respective BS+MS degree programs (BS in their major and MS in Computing Security) and receive the SFS scholarship to complete their last two years of study.

At the B. Thomas Golisano College of Computing and Information Science, we have a wide range of students from various computing backgrounds with interest in cybersecurity. Each computing discipline views cybersecurity differently, so we believe students will benefit from the cohort experience of interacting across the three departments. With the help from this SFS program, we will facilitate this cohort experience by providing:

- A **common curriculum** so the students remain in the same classes
- A series of **monthly seminars** for supported students
- Multiple sessions of **professional training** with the help from the RIT Office of Cooperative Education and Careers
- Student travel to **security conferences**

1.1 NSF Merit Review Criteria

Intellectual Merit

The intellectual merit of this proposal is based on a cohort experience of students from multiple disciplines in a practical setting. More specifically:

- Like the three PIs, students in each cohort will be from three different computing majors, thus enabling faculty and students to shape one another's differing perspectives on the crosscutting discipline of cybersecurity.
- The cohort experience will be facilitated by common coursework, monthly seminars, work on research projects, and travel to security conferences.
- SFS scholars placed on federal internships will build on RIT's well-established undergraduate cooperative education (co-op) model that yields students, thus will be able to contribute to cybersecurity operations before and immediately after graduation.
- This proposal leverages RITs infrastructure, diverse programs, faculty resources, and industry/military relationships to support a pool of qualified candidates who might not otherwise be able to pursue graduate study in cybersecurity.

Broader Impacts

There are multiple impacts of the proposed SFS program:

- RIT's SFS graduates will secure, protect and improve our nation's cyberinfrastructure.

- With their crosscutting breadth of knowledge and experiences, these SFS graduates will be ready to adapt to a variety of cybcersecurity challenges at diverse federal agencies.
- Scholarly contributions made by the SFS scholars will be disseminated at professional conferences relating to cybersecurity.
- Building on their prior record of disseminating educational issues, the PIs will discuss lessons learned in running this SFS program at appropriate venues in educational and federal settings.
- Working with RIT's K-12 office, the PIs and the SFS scholars will visit the City of Rochester schools with a large population of underrepresented groups in computing. Student scholars will promote awareness of cybersecurity issues facing to the nation and teach students basic knowledge about how to protect themselves online.

2 Motivation

Our society is currently experiencing a rapid development in technology. Most notably the Internet is becoming an increasingly important backbone for the nation's economic engine and a necessity for human interaction. Cyberspace will continue to grow to be the most important platform for many activities in our daily lives.

Great benefits come with great danger. The Internet has also become a fertile ground for criminal activities destined to inflict harm to customers, patients, citizens, and America's national interests. Critical information stored on a computing device could be stolen. Communications could be eavesdropped and/or altered during transit. System functionality could be processed mistakenly and could be intentionally distorted to mislead the user.

Security is a property that impacts all levels of computing abstraction: from the low-level networking protocols, to sofware architecture, to fundamental algorithms that drive all computing. The next generation of cybersecurity professionals will be a heterogeneous collection of experts who have collectively mastered the many different facets of computing. These scholars must be able to fortify computing systems using methods from many computing sub-disciplines, such as: system administration, networking, cryptography, authentication, web applications, mobile, cloud, operating systems, software design, software development processes, database management, data mining, and many others.

Understanding how to protect systems from malicious attack is not only an important skill set, but a career that is currently highly in demand, from government agencies in particular. As the demand for cybersecurity careers coninues to ramp up, we anticipate the need for highly talented, highly skilled technical personnel. The CyberCorps®SFS program will help RIT provide top students with well-balanced backgrounds to be recruited into government agencies, into the private sector, or into academia. RIT is positioned to provide our nation with well-balanced cybersecurity professionals for the following reasons:

- RIT has formed the nation's first **Department of Computing Security** (CSEC) with nine faculty members. Section 4.1 discusses this department in detail.
- The CSEC department has five extended faculty to balance the computing perspective in such a crosscutting discipline. Co-PI Meneely from SE and Co-PI Raj from CS are both extended faculty to the CSEC department. All PIs have proven track records of both teaching and research in the field of cybersecurity. See Section 5.1 for qualifications.
- RIT provides cooperative education (co-op) where students can apply their skills in a practical, "real world" setting. See Section 3.6 for more on co-op.

3 CyberCorps®: Scholarship for Service at RIT

We propose a three-year SFS program for BS+MS students from three different undergraduate programs. We will create two cohorts with 6 students in each cohort.

Table 1: RIT SFS Three Year Plan

Year	Student
1	6 undergraduate seniors
2	6 graduate students 6 undergraduate seniors
3	6 graduate students

3.1 Curriculum

To ensure students will be able to complete the MS in Computing Security within one year, we will require students to take three graduate courses from the MS in Computing Security program while they are undergraduates. These three courses are recommended to be taken as undergraduate students.

- GCCIS-CSEC-731 Web Server and Application Security Audits
- GCCIS-CSEC-733 Information Security and Risk Management
- GCCIS-CSEC-742 Computer System Security

The pre-requisites of these courses are easily satisfied by undergraduates from the three programs involved. The content of these three courses also matches well with the undergraduate CSEC program. We anticipate that, in their final year of undergraduate study, BS+MS students will first take CSEC-731 in the fall semester, then CSEC-733 and CSEC-742 in the spring semester (see Table 2).

Table 2: Cohort courses of last year of undergraduate study

Fall (3 credits)	Spring (6 credits)
CSEC-731 Web Server and Application Security	CSEC-733 Information Security and Risk Management CSEC-742 Computer System Security

For Computing Security students, these three courses count as CSEC electives; for Computer Science students, they count as free electives; for Software Engineering students they count as two application domain electives and one free elective. These three courses with 9 credits in total will be double-counted for undergraduate credits towards students' respective undergraduate degree programs, and also as graduate credits towards the graduate program in computing security. We have communicated with undergraduate program coordinators of the respective programs; all have agreed the three courses recommended will be acceptable to their undergraduate programs.

With 9 credits already completed, the last year of their graduate study schedule will be as follows (see Table 3). Graduate electives are designed to broaden students' interests and skill sets. Students in the program will take three courses together in the fall of the final year, and take the capstone project course together in the spring of the final year.

3.2 Cohort Experience Plan

As the cohort experience is fundamental to the success of our SFS scholarship program, we have developed several elements to our cohort experience plan:

Table 3: Cohort courses of graduate study

Fall (12 credits)	Spring (9 credits)
CSEC-601 Research Methods	CSEC Graduate Elective Two
CSEC-603 Enterprise Security	CSEC Graduate Elective Three
CSEC-604 Cryptography and Authentication	CSEC-793 Capstone Course
CSEC Graduate Elective One	

- **First year common courses.** Students will take three courses together (see Table 2. Since computer science advanced elective courses are also advanced electives for computing security and software engineering majors, there will be more common courses for the cohort.
- **Final year all same courses.** During the last of the program, scholars will take exactly the same required courses, and possibly electives. The capstone course will provide scholars an opportunity to work on large scale team projects where scholars can exercise their team building and working skills.
- **Monthly seminars.** Each month, the PIs will host a seminar with all of the scholars to update each other on the current news and research in cybersecurity. During these seminars, PIs and students will exchange experiences in learning and research in cybersecurity. Students may take these opportunities to ask for help on virtually anything that is related to their study and campus life; students can exchange project ideas during these meetings. Cybersecuirty experts from industry and government agencies may be invited to give a talk or presentation to the scholars. We may arrange some field trips to local industries and law enforcement sites that are related to cybersecurity for the meeting time slot.
- **Visits to local City of Rochester K-12 schools to promote cybersecurity.** The cohort will visit a local K-12 school annually to promote awareness of cybersecurity and as a way to contribute back to society. It will be a good experience for the scholars to help grow minority participation in future cyberseurity workforce.
- **Security conference attendance first year or second year**. Conferences are one way to keep students knowledge up to date. It is especially important for cybersecurity students to learn the trends and future developments in security knowledge and technology. Attending conferences together will be a great bonding opportunity for students to help each other and learn together.
- **Team building capstone projects.** The last year capstone project is another opportunity for the cohort students work on teams to solve real world problems. Students will apply knowledge learned in the program to devise security solutions, create new security tools, identify new systems and network vulnerabilities, and establish new theoretical foundations for computing security.
- **Membership in the local Infragard Chapter.** As part of the cohort experience, we will recommend that SFS scholars join the local Infragard Rochester chapter, which is a partnership between the FBI and the private sector to share information and intelligence to prevent hostile acts against the US. One benefit to a student joining Infragard is that the student has to go through a basic background check process, which prepares them for extensive background checks for employment in government agencies.

As we gain further experience with the SFS Scholarship program, we will continue to identify additional mechanisms to improve the overall cohort experience.

3.3 Student selection

Student selection is critical to the success of the program. We have a large pool of students from which we can recruit qualified students. The B. Thomas Golisano College of Computing and Information Science is one of the largest computing colleges in the nation with an enrollment of over 3,400 in Fall 2013. Approxi-

mately 250 undergraduates are enrolled in Computing Security, over 400 in Software Engineering, and 800 in Computer Science. Over 90% of these students are US citizens, which provides us with a large poll of qualified students to draw from.

The PIs will host annual information sessions to promote the SFS program to junior students who are interested in the BS+MS options, to inform them about requirements, benefits, and commitments to be a part of the program.

In addition to the requirements specified in the SFS program solicitation, we would also require candidate students meet the following minimum requirements:

- Students must be full-time, matriculated undergraduate students in the BS in Computing Security, Computer Science, or Software Engineering programs.
- Students must have completed the co-op requirements within their respective programs. Preferences will be given to those who have completed co-op with federal, state, or local government agencies and/or those who have acquired clearance to work for government agencies.
- Students must submit an up to date resume, a transcript, and two letters of recommendations.
- Students must have an overall GPA at least 3.5.
- Students must commit to monthly meetings with peers and the PIs.
- Students must commit to attending the SFS job fair, participating in the mandatory summer internship, and working for a least two years with a federal agency, as defined in the SFS solicitation.

The PIs will form an admission committee to review application materials including grades, recommendation letters, and co-op evaluation reports.

3.3.1 Possible Targeted Student Groups

- **Security Practices and Research Student Association (SPARSA)**

  SPARSA is RITs premiere cybersecurity student club. Its members are comprised of students studying a range of different computing disciplines and who share a common interest in the study of cybersecurity. Founded in the wake of the terrorist attacks of September 11th, 2001, SPARSA now has an alumni base that ranges in membership from positions within the intelligence community, to Fortune 500 companies and private security research firms. The club hosts weekly meetings to keep members up to date about the most recent news in cybersecurity, organizes many presentations by members, invited speakers from the club, and alumni who are working at the forefront of cybersecurity in government agencies and in industry.

  SPARSA members organize an open, annual cybersecurity competition: Information Security Talent Search (ISTS). Each year the competition hosts about five teams from other universities and colleges. Teams of five competitors ("blue teams") are given a simulated corporate network, featuring a number of misconfigured and intentionally vulnerable systems, which must be secured and defended from outside attacks. Competitors face constant aggression from the "red team", who represent a dedicated attacking force that seeks to break into their networks and maintain their presence as long as possible, while seeking to exfiltrate any sensitive information that they can find. The red team is comprised of volunteers from the security industry around the nation, representing companies or agencies, who are often interested in recruiting the students participating in the event. Competitors also have the opportunity to gain additional competition points by completing challenges, ranging in subjects from web application testing, to reverse engineering and cryptography.

  Members of SPARSA are highly sought by recruiters. The students are technically up to date with trends in industry, and have strong communication and leadership skills. Many current or past IASP

scholarship recipients are or were SPARSA members. PI Yuan is the faculty advisor for the SPARSA club. He works with the club leadership group and members constantly. The PI will actively promote this scholarship to the group and help identify promising candidates personally.

- **Collegiate Cyber Defense Competition (CCDC) Team.** RIT has been involved in CCDC since 2008. In the past four out of six years, RIT made to the national final, and RIT won the national championship in 2013. PI Yuan has been the coach for RIT CCDC team since 2011. He instigated a rigorous selection process for team members. In addition to strong technical skills, excellent academic standing and strong team work skills are required for team members. Blind peer review by applicants is employed to identify cybersecurity talents. The team has an excellent track record in terms of employment. Team members are often offered multiple employment contracts. The PI Yuan will actively promote this scholarship program to team members.

- **Honor Societies.** Each department with in the B. Thomas Golisano College of Computing and Information Science has student honor society. Membership in an honor society is purely merit based. Students need to maintain a grade point average above "B" to remain in the society. Students in a honor society are offered RIT scholarships for extra curricular activities. These students are among the best academically in all computing majors.

  The PIs will frequently participate in honor students' activities, will promote the SFS scholarship to honor students, and will identify and encourage qualified students to apply for the SFS scholarship.

3.3.2 Application Process

All three PIs will actively promote and identify outstanding students in their respective programs and encourage those excellent students to apply for the scholarship. The PIs will also actively involve in the college honor student program, open only to outstanding students. All students in the college will be notified of the NSF SFS program at RIT by a website, email, classroom notification, electronic display announcements, and paper postings throughout the college building. The PIs will personally contact department chairs and student advisors about the program.

The PIs will hold two information sessions, one at the beginning of the fall semester; the other will be held at the beginning of the spring semester, so that students can consider a BS+MS and plan their coursework accordingly. One scheduling factor that we will manage on a case-by-case basis is the required cooperative education component where students work off-campus in their industries. (More information on RIT's cooperative education can be found in Section 3.6).

Students will be asked to submit their most recent resume, transcript, and at least two recommendation letters. Students' application materials will be reviewed by the PIs, who will jointly make the final admission decisions.

3.4 Student mentoring and engagement

Students at RIT are afforded a wide array of advising support. The three PIs for the RIT NSF SFS program serve as the faculty advisors to all NSF SFS scholarship recipients. Personal meetings to review academic progress as well as research and career direction will be scheduled throughout the semesters. The CSEC department currently employs two staff members dedicated to advising students about course selection, career choices, and degree completion audits. The department also supports three graduate assistants to work with students on their domain-area subject materials. These students host office hours in the lab facilities and are available by appointment to tutor and mentor students. RIT also supports an early alert

systems whereby faculty are able to report when a student is not performing up to expectations in a course. Such reports are emailed to the student, as well as the staff and faculty advisors for follow-up.

The PIs will supervise students in the program on various research projects. All PIs have extensive experience in advising students on their theses or capstone projects. Research topics in cybersecurity areas will be identified for students if they do not have one. Research results will be disseminated via conference publications and presentations.

3.5 Student Travel to Security Conferences

Each year we plan to send students to a security-focused conference to learn and explore the latest development in the field of computing security. In the first year, students will, most likely, just attend security conferences as they will have not done any research. In the second year, we expect some students in the program will be able to present their research results at a security conference. Targeted security conference are ShmooCon, Washington, DC; RSA Conference in San Francisco, CA; Black Hat, Las Vegas, NV, etc.

3.6 RIT Co-Operative Education

For over 100 years, the hallmark of an RIT education has been the practical, paid work experience provided through cooperative education. RIT was among the first universities to begin cooperative education back in 1912, and today the RIT co-op program is the fourth oldest and one of the largest in the world.

More than 3,600 RIT students completed more than 5,300 work assignments last year and were employed by nearly 2,000 employers coast to coast and abroad. Co-op is one of the most effective means for employers to identify and acquire key talent. Few institutions have done it as well and as long as RIT. RITs extensive experience and resources allow us to successfully meet the needs of nearly all types of employing organizations.

3.6.1 RIT Office of Cooperative Education and Career Services

The RIT Office of Cooperative Education and Career Services provides outstanding job search services to students seeking cooperative education. The Career Services Office is a centralized campus support service with staff of 30 members to work collaboratively in delivering services and programs as well as unified messaging to all our constituents. Every degree program at RIT is assigned a Career Services Program Coordinator to work with directly with their assigned disciplines, and to assist those students in securing their co-op employment.

Program Coordinators in this office support specific academic departments and are available to meet on a one-to-one basis with students and alumni on career and employment matters. These sessions are critical to developing individual job search plans and addressing the many questions and issues that arise during the job search process.

All three bachelors programs require co-op experience before graduation. BS in Computing Security requires at least two terms of co-op experience, while both BS in Computer Science and Software Engineering require at least three terms of co-op experience. Preference in admission to the scholarship program may be granted to CSEC students who have three terms of co-op experience over those with only two terms of co-op experience.

The RIT co-op requirements mesh well with the NSF SFS requirements and opportunities for student internships and will yield a seamless experience for students graduating from the programs.

3.6.2 Career Fairs

RIT hosts two huge career fairs each year. All federal, state, and local government agencies are invited to the RIT Career Fairs. Through the RIT Job Zone, nearly 100 federal, state, and local government agency job opportunities are posted. More than 150 students complete a co-op each year with nearly 100 Federal, State, and local government agencies.

We will require students in this program to attend RIT job fair each year in addition to Office of Personnel Management job fair before they are ready to make a commitment so that they will gain experience in interviewing and resume writing, and understand the federal job landscape.

Program Coordinators conduct numerous job search and career-related workshops, seminars, co-op prep classes, and other preparation programs such as mock interviews and etiquette dinners. The Office of Co-op and Career Services works with over 10,000 employers throughout the country and around the world to identify and develop corporate partnerships for hiring RIT co-op students, new graduates and alumni. RIT is also focused on developing international work abroad assignments and has been successful in expanding these opportunities for co-op students in many countries and with new and existing corporate partnerships.

4 Computing Security at RIT

RIT has a wide range of computing security capabilities. In response to the demand for cybersecurity professionals and the rapid progress made in the computing security discipline, RIT has established the nation's first Department of Computing Security, discussed in Section 4.1

The study of security is not limited to CSEC Department, however, as security is a property that cuts across many computing disciplines. Undergraduate programs such as those in the CS and SE departments focus on, and in some cases require, security expertise as a part of their program. Sections 4.2 and 4.3 discuss this further.

All three departments are housed in the B. Thomas College of Computing and Information Science, one of the largest computing colleges in the nation.

4.1 Department of Computing Security

Established in 2012, the CSEC department consists of nine full time faculty and five extended faculty members whose primary appointments are in the Departments of Computer Science, Software Engineering, and Information Science and Technologies. In addition, there are two full time staff and a system administrator who are dedicated full time to the department.

RIT awards both a Bachelor of Science and a Master of Science in Computing Security. The first security degree program at RIT was the Master of Science in Computing Security and Information Assurance, established in 2005. It was a cross department degree program with a curriculum taught by faculty from SE, CS, and Information Technology. In the following year, the Bachelor of Science in Information Security and Forensics was established in 2006. It was seen as one of the first undergraduate degree programs focusing on cybersecurity in the nation at that time.

As the both programs grew and the discipline of computing security expanded, a new department was established in 2012 to host both degree programs with a goal to better serve students and foster research and curriculum development in security. Currently there are approximately 300 full time undergraduate and graduate students registered in the programs.

RIT is a Center of Academic Excellence for Information Assurance Education designated by the National Security Agency in 2006, re-designated in 2009. With this designation, RIT was able to successfully receive 12 DoD ISAP scholarship awards over the years. Many graduates from DoD ISAP scholarship pro-

gram now diligently serve the nation in many government agencies. Some of them received awards and honors in their line of duty. It has been praised by NSA for the quality of our graduates.

As a CAE-IAE center, RIT has worked with the NSA Security Education Academic Liaison (SEAL) representative closely in promoting computing security education and research. RIT has successfully completed a thorough curriculum mapping between its computing security degree and the NSA requirements for summer interns. RIT's BS in Computing Security degree has been certified by the NSA as one of degree programs, other than traditional computer science, computer engineering degree programs, where NSA can employ summer internships directly. With this assurance, our students have more opportunities to learn and work for the NSA or other government agencies early and can nurture their interest in and commitment to work for government agencies.

The Master of Science in Computing Security is two-year and 30 credits graduate program. Thanks to the recent dramatic increase in demand for highly skilled cybersecurity professionals in industry, many outstanding undergraduate students have received multiple employment offers before graduation; very few of them even consider post-graduate education. By reducing graduate study to one year, the program is more feasible to many students who are interested in continuing their study.

Post graduate study is important to cybersecurity professionals who may take on leadership roles in their organization. It provides a broader overview of the cybersecurity field, a opportunity to learning project leadership skills, and more depth in knowledge. Those professionals with a leadership role within an organization are critically important to agencies. They will influence the policy, culture, rules of engagement, and development of a team in cybersecurity operations for agencies and organizations.

4.2 Computing Security in the Department of Computer Science

The Department of Computer Science offers a B.S. degree in Computer Science. The degree produces computer scientists who are well rounded, not only in computing, but also mathematics and science. In addition, students must satisfy a general education framework designed to provide students with a strong foundation, exposure to multiple models of inquiry across a wide range of disciplines, and an opportunity to immerse themselves within a specific area through deeper learning. This extensive general background will serve to prepare Computer Science majors to think thoughtfully and critically about the numerous security-related computing problems facing our society.

Students in the B.S. program become competent programmers. Through required Computer Science courses, students develop a broad understanding of a modern computing environment as well as gaining skills and mastery of both theoretical and applied concepts in such diverse areas as data management, intelligent systems, and analysis of algorithms.

One of the hallmarks of the degree is the requirement that students complete at least four Computer Science electives, of which at least two electives are chosen from the same cluster. The CS department identifies each Computer Science elective as belonging to one or more clusters based on the main themes developed in each course. One such cluster that we currently support is titled *Security*. The CS department currently has ten courses at the undergraduate level that are classified in the Security cluster, with an additional eleven courses at the graduate level also classified in the Security cluster. Undergraduates are permitted to take graduate-level courses provided that have the proper prerequisites. Selected Computer Science courses classified in the Security cluster are: *Principles of Computer Security*; *Foundations of Cryptography*; *Secure Data Management*; and *Secure Coding*.

Outstanding Computer Science majors who might be chosen to pursue the MS degree in Computing Security would be highly encouraged to select graduate-level Computer Science courses from the selections in our Security cluster to satisfy their undergraduate Computer Science electives and facilitate their completion of the MS degree with one additional year of study.

4.3 Computing Security in the Department of Software Engineering

The Department of Software Engineering at RIT currently offers BS and MS degrees in Software Engineering (SE). In 1996, RIT became the first university in the US to offer the bachelor's degree in SE. In this program, students learn the many aspects of the software development lifecycle, such as design, implementation, requirements, testing, process, project management, and security.

One feature of the program that helps facilitate this cross-cutting project is the application domain. Software does not exist in isolation, rather it exists to fill specific needs to a specific domain. In the SE BS program, undergraduates are required to take three courses that focus on an area outside of traditional software engineering. One of those application domains is CSEC, which is approved to include the courses required for the undergraduate side of the BS+MS degree.

Furthermore, SE undergraduates will have an introductory background in security. As of Fall 2013, every SE major is required to take a new course in the curriculum, *Engineering Secure Software*. Developed by Co-PI Meneely as a part of NSF grant (0837656), the course provides a foundation of software security principles as it applies to software engineers. Todays software engineering students will need to deal with software security in their professions. However, these students will also not be security experts. Rather, they need to balance security concerns with the myriad of other draws on their attention, such as reliability, performance, and delivering the product on-time and on-budget. The course takes principles and software security engineering practices and applies them to each step of the software development lifecycle. As a part of this effort, Co-PI Meneely has developed original material and published the results [13, 10, 14]. Topics covered include: security in requirements engineering, secure designs, risk analysis, threat modeling, deployment of cryptographic algorithms, defensive coding, penetration testing, fuzz testing, static analysis, and security assessment.

5 Project Management

5.1 Experience and Capabilities of the PIs and Senior Personnel

PI Bo Yuan is an Associate Professor of Computing Security at RIT since 2003. He has been primarily teaching in computing security related areas. Dr. Yuan has an extensive publication record with students [9, 28, 8, 26, 30, 4, 6, 7]. Dr. Yuan is also the current director for the Center for the Advancement of Research and Education in Information Assurance (CARE-IA) which was established in compliance with the NSA CAE/IAE designation requirement. Dr. Yuan has also been the coach for the RIT CCDC team that won the national champion since two year ago.

Co-PI Rajendra K. Raj is a Professor in Computer Science at RIT and an affiliated member of the Computing Security department. His current research interests include secure software and secure data management in distributed and cloud settings, most recently in healthcare and critical infrastructure protection [1, 2, 23, 25, 27]. Prior to RIT, he was a software designer, developer, and manager in the Information Technology Division at Morgan Stanley, where he led projects in secure worldwide data infrastructures (private clouds) [24]. Dr. Raj developed and taught graduate courses in Secure Coding and Secure Database Systems for RITs MS program in Computer Security and Information Assurance since its inception. He served as the Computer Science Assessment Chair responsible for assessment of the departments MS and ABET-accredited BS programs. Dr. Raj has also been an external program evaluator for several computing programs, and has provided consulting advice within the US and abroad on program assessment and evaluation.

Co-PI Andrew Meneely is an Assistant Professor of Software Engineering at RIT since 2011 and an affiliated member of the Computing Security department. Dr. Meneely's research is in areas of empirical software engineering as it applies to security [17, 19, 29, 13, 21, 20, 16, 22, 15, 21, 18, 14, 10]. Co-PI

Meneely has provided empirical research to several software companies, including Cisco, Nortel, Applied Research Associates, and Red Hat.

External Evaluator Trudy Howles is a Professor of Computer Science at RIT. Dr. Howles current research areas include secure software and privacy preserving data mining (PPDM). Dr. Howles is a senior member of the American Society for Quality (ASQ) and has been active at the national level with the ASQ Software Division. She is an Editor-In-Chief for the *Software Quality Professional*. Dr. Howles is an active researcher on student educational and retention strategies with presentations at IEEE and ACM conferences, and publications in ACM Inroads, Software Quality Professional, and Computer Science Education.

5.2 Roles and Responsibilities

PI Yuan will assume primary responsibility and management of the project. The PIs will form an admission committee to promote the SFS program in their respective degree programs, and to identify and recruit talented scholars. The three PIs will also unction as faculty mentors for the SFS scholars and will be responsible for working with and guiding them. They will host monthly seminars and supervise SFS students' research projects. At least one of the PIs will travel with students to security conferences every year.

Co-PI Raj will assume responsibility for internal assessment and evaluation processes, and will be guided by External Evaluator Howles, described in Section 6

5.3 Project Timeline

Assuming the project is approved in the fall semester, PIs will start to recruit in the spring semester. The first year of SFS scholar cohort starts in the following fall semester.

The following Table 4 illustrates the whole project timeline and activities.

6 Project Assessment and Evaluation

As assessing project success is crucial for a major scholarship-granting proposal, the project has the following overarching goals.

Goal 1: Quantity Goal. *To increase the number of qualified students graduating with an MS degree in Computing Security*. This goal has two sub-goals: (a) increase the number of well-qualified B.S. students in Computer Science and Software Engineering pursuing an MS degree in Computing Security, and (b) increase the number of talented BS Computing Security students pursuing an MS in Computing Security.

Goal 2: Quality Goal. *To increase the quality of SFS students graduating with an MS in Computing Security*. The intention is to provide a variety of curricular and extra-curricular experiences to the SFS graduates to ensure they graduate with the knowledge and skills needed to advance to leadership positions in federal or military agencies, and continue to progress in their careers.
All project activities stem from these goals and need to be carried out in a meaningful way to ensure project success.

We outline some elements of the evaluation plan for our two goals in Table 5 and Table 6. As shown in these tables, the first goal focuses on improving the quantity of students admitted to the program and efforts made to retain these students. The second goal focuses on improving the quality of the curricular, non-curricular and extra-curricular activities for the students so that they graduate with skills needed from an SFS graduate.

Table 4: Project Timeline

Academic Year	Fall term	Spring term	Summer term
2014-2015	• Promote The SFS program	• Promote The SFS Program • Accepting applications • Making admission decisions for Cohort A	
2015-2016 **Cohort A** (6 undergrads)	• Monthly group meetings • Attend RIT fall career fair • Visit a local minority K-12 school • Promote The SFS Program	• Monthly group meetings • Attend RIT Spring career fair • Promote The SFS Program • Accepting applications • Making admission decisions for Cohort B	• Intern at a government agency • Attend a security conference • Initial assessment
2016-2017 **Cohort A** (6 grads)	• Monthly group meetings • Attend RIT fall career fair • Visit a local minority K-12 school	• Monthly group meetings • Capstone project • Attend RIT Spring career fair	• Start to work for a government agency • Attend a security conference • Exit assessment
2016-2017 **Cohort B** (6 undergrads)	• Monthly group meetings • Attend RIT fall career fair • Visit a local minority K-12 school	• Monthly group meetings • Attend RIT Spring career fair	• Intern at a government agency • Attend a security conference • Initial assessment
2017-2018 **Cohort B** (6 grads)	• Monthly group meetings • Attend RIT fall career fair • Visit a local minority K-12 school	• Monthly group meetings • Capstone project • Attend RIT Spring career fair	• Start to work for a government agency • Attend a security conference • Exit assessment

Prior to project outset, Co-PI Raj will work with External Evaluator Howles to ensure that the final assessment and evaluation (A & E) plan is well-crafted to ensure that the project remains on track and its processes reflect continuous improvement.

7 Results from Prior NSF Support

PI Yuan has had no prior NSF support.

Co-PI Raj also currently serves as Co-PI on three other NSF projects. The latest of these is an NSF SFS Capacity Building project (DUE-1303269, $244,295, 2013-15). This multi-partner (RIT, Corning Community College, and Greater Southern Tier Board of Cooperative Educational Services) project focuses on Critical Infrastructure Protection (CIP) education by developing curricular materials and expertise at the high school and undergraduate levels. The project has begun developing several reusable CIP course modules for use in existing high school and courses without requiring major course or program modifications [23].

The second project, an NSF-NRI project (IIS-1208566, $266,855, 2012-14), has developed laboratory modules to permit students work with and alongside a team of co-robots as a concrete way to learn core computing concepts. Dr. Raj presented a paper [5] on this project at FIE 2013 and will be jointly presenting the project as part of the NSF Showcase at SIGCSE 2014.

Table 5: Elements of the Evaluation Plan of Goal 1 (Quantity)

Goal	Evaluation Questions	Data Source	Data Collection	Analysis
To increase the number of qualified graduates (Quantity Goal)	How effective were the processes used to identify and recruit BS students?	GPAs; co-op reports summaries; faculty recommendations	Collect data from the CS/SE/CSEC departments.	Expert review, critique of processes, etc. to suggest process improvements as needed
	How effective were the retention efforts used to ensure continued student success in coursework and the SFS program?	Attendance at various team-building events; mentoring meetings;	Collect the data from the SFS-program events; mentoring meeting reports.	Expert review to provide critique of process used to identify students and suggestions for process improvement

The third of these is an NSF TUES project (DUE-1141200, $113,594, 2012-15), which has developed three course modules to teach Service-Oriented Programming jointly at three institutions [11]: Howard University, SUNY College at Oswego, and RIT. Workshops to teach these modules have been presented at RIT and FIE 2013 citeraj-fie2013-sop-workshop. He will be presenting another SOP workshop at SIGCSE 2014 [12] and at the NSF Showcase at SIGCSE 2014. Current versions of the materials produced have been made available to workshop particpants.

Co-PI Raj previously served as Senior Personnel on an NSF REU project (CCF-0851743, $275,000, 2009-2012) on High Performance File Systems and Data Visualization at RIT [3]; during its three summers of operation, 30 undergraduate students were mentored, with over ten conference publications, panels, or presentations; several students also presented their work at international conferences.

Co-PI Meneely was a co-PI on *Applied Multi-Disciplinary Cryptography* (CCLI-0837656, 2011-2013, $149,598). He used the support to develop a new undergraduate course titled *Engineering Secure Software*.

The intellectual merit of this course is evident in recent publications on the course and curriculum [13, 10] along with the work on Vulnerability of the Day [14]. Topics covered include: security in requirements engineering, secure designs, risk analysis, threat modeling, deploying cryptographic algorithms, defensive coding, penetration testing, fuzzing, static analysis, and security assessment.

The broader impact of this activity was to develop this required course, thereby educating software engineering students in security. Currently, four sections of the course have been offered, totaling to over 100 undergraduates who have taken and passed the course over the past two years.

External Evaluator Howles served as PI on a Computing Undergraduate Scholarship Program (CUSP) project (DUE-0630913, $484,256, 2006-11) that supported two cohorts of 36 academically talented and financially needy computing students. Each cohort was funded for two years (Cohort 1 , 2007-2008; Cohort 2, 2009-2010). Students were advised and mentored during the two years of the scholarship and throughout their academic careers. When the grant ended in 2011, 30 of the 36 students in Cohort 1 had graduated or expected to graduate within two quarters; graduation rates for Cohort 2 students are not yet available because RIT runs 5 year program but most of these students are expected to graduate this year. Dr. Howles is also Senior Personnel (assessment coordinator) for two other NSF projects: (1) a TUE Multiplayer Board

Table 6: Elements of the Evaluation Plan of Goal 2 (Quality)

Goal	Evaluation Questions	Data Source	Data Collection	Analysis
To increase the quality of SFS graduates (Quality Goal)	How effective were the processes used to provide curricular support (coursework, research projects, theses) to the SFS students?	Examine actual courses taken and SFS scholar performance in these courses	Collect the data during every term.	Expert review to provide critique of process used to identify students and suggestions for process improvement
	How effective were the processes used to provide extra-curricular support (meetings with SFS faculty, colloquia attendance, participating in cyber security competitions, etc.)?	Examine attendance, quality of external and internal presenters, etc.	Collect the data at every event.	Expert review to provide critique of process used to identify students and suggestions for process improvement
	How effective were the processes used to provide support for student publications at conference and other venues?	Examine papers being published for quality of paper content and venue reputation.	Collect the data at every event.	Expert review to provide critique of process used to identify students and suggestions for process improvement

Game Strategies in the Introductory CS Curriculum" project (DUE-1044721, $198,678, 2011-2013), and (2) the SFS Capacity Building Project (DUE-1303269, $244,295, 2013-15) mentioned above.

8 Master of Science in Computing Security Program

A minimum of 30 credit hours are needed to graduate.

8.1 MS in Computing Security: Core Courses

- CSEC-601 Research Methods and Proposal Development (3 Sch)
- CSEC-603 Enterprise Security (3 Sch)
- CSEC-604 Cryptography and Authentication (3 Sch)
- Select of of the following three capstone options
  - GCCIS-CSEC-790 MS Thesis (6 sch)
  - GCCIS-CSEC-792 CSEC Project (3 sch)

- GCCIS-CSEC-793 Capstone for Computing Security (3 sch)

8.2 MS in Computing Security: Electives

Students need to take 5 or 6 courses from the following advanced electives depending on their choices of meeting capstone requirements. The following is a list of qualified advanced electives for the program. They are all three credit hour courses.

- GCCIS-CSEC-730 Advanced Computer Forensics
- GCCIS-CSEC-731 Web Server and Application Security Audits
- GCCIS-CSEC-732 Mobile Device Forensics
- GCCIS-CSEC-730 Advanced Computer Forensics
- GCCIS-CSEC-733 Information Security and Risk Management
- GCCIS-CSEC-741 Sensor and SCADA Security
- GCCIS-CSEC-742 Computer System Security
- GCCIS-CSEC-743 Computer Viruses and Malicious Software
- GCCIS-CSEC-744 Network Security
- GCCIS-CSEC-750 Covert Communications
- GCCIS-CSEC-751 Information Security Policy and Law
- GCCIS-ISTE-721 Information Assurance Fundamentals
- GCCIS-CSCI-622 Secure Data Management
- GCCIS-CSCI-642 Secure Coding
- GCCIS-CSCI-662 Foundations of Cryptography
- GCCIS-CSCI-734 Foundations of Security Measurement and Evaluation
- GCCIS-CSCI-735 Foundations of Intelligent Security Systems
- GCCIS-CSCI-762 Advanced Cryptography
- KGCOE-CMPE-661 Hardware and Software Design for Cryptographic Applications

8.3 MS in Computing Security: Suggested Areas of Focus

Furthermore, various subsets of the above electives provide a focus of study, or "clusters". The following clusters are available: **Systems and Network Security**, **Systems and Network Forensics**, **Secure Development**, **Science of Security**.

References

[1] S. Alshehri, S. Radziszowski, and R. K. Raj. Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption. In *ICDE Workshop on Data Management in the Cloud, DMC '12*. IEEE, 2012.

[2] S. Alshehri and R. K. Raj. Secure Access Control for Health Information Sharing Systems. In *IEEE International Conference on Healthcare Informatics, ICHI 2013*. IEEE, 2013.

[3] R. Bailey, H.-P. Bischof, M. Kwon, T. Miller, and R. Raj. On providing successful research experiences for undergraduates. In *Frontiers in Education Conference (FIE), 2011*, pages T2F–1–T2F–6, Oct 2011.

[4] E. Brown, B. Yuan, D. Johnson, and P. Lutz. Covert channels in the HTTP network protocol: Channel characterization and detecting man-in-the-middle attacks. *The Journal of Information Warfare*, 9(3):26–38.

[5] Z. Butler, R. K. Raj, and M. Kwon. Integrating highly-capable corobots into a computing curriculum. In *Frontiers in Education Conference, 2013 IEEE*, pages 1173–1175, Oct 2013.

[6] C. Forbes, B. Yuan, D. Johnson, , and P. Lutz. A covert channel in RTP protocol. In *The 9th International FLINS Conference*, pages 813–819. World Scientific.

[7] E. Golen, B. Yuan, and N. Shenoy. An evolutionary approach to underwater sensor deployment. *International Journal of Computational Intelligence Systems*, 2(3):182–201.

[8] W. Huba, B. Yuan, D. Johnson, and P. Lutz. A HTTP cookie covert channel. In *Proceedings of the 4th international conference on Security of information and networks*, SIN '11, page 133136. ACM.

[9] W. Huba, B. Yuan, Y. Pan, and S. Mishra. Towards a web tracking profiling algorithm. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 12–17, 2013.

[10] D. E. Krutz and A. Meneely. Wip: Teaching web engineering using a project component. page to appear, 2013.

[11] X. Liu, R. K. Raj, T. Reichlmayr, C. Liu, and A. Pantaleev. Incorporating service-oriented programming techniques into undergraduate cs and se curricula. In *Frontiers in Education Conference, 2013 IEEE*, pages 1369–1371, Oct 2013.

[12] X. Liu, R. K. Raj, T. Reichlmayr, C. Liu, and A. Pantaleev. Teaching service-oriented programming to cs and se undergraduate students. In *Proceeding of the 45th ACM Technical Symposium on Computer Science Education*, SIGCSE '14 workshop. To Appear, New York, NY, USA, 2014. ACM.

[13] M. Lukowiak, S. Radziszowskim, C. Wood, J. Vallino, and A. Meneely. Developing an applied, security-oriented computing curriculum. In *American Society for Engineering Education (ASEE)*, Houston, TX USA, 2012. ACM.

[14] A. Meneely and S. Lucidi. Vulnerability of the day: concrete demonstrations for software engineering undergraduates. In *Proceedings of the 2013 International Conference on Software Engineering*, ICSE 2013, pages 1154–1157, Piscataway, NJ, USA, 2013. IEEE Press.

[15] A. Meneely, P. Rotella, and L. Williams. Does adding manpower also affect quality?: an empirical, longitudinal analysis. In *Proceedings of the 19th ACM SIGSOFT symposium and the 13th European conference on Foundations of software engineering*, ESEC/FSE 2011, pages 81–90, 2011.

[16] A. Meneely, B. Smith, and L. Williams. Validating software metrics: A spectrum of philosophies. *TOSEM*, 21(4):24–48, Oct. 2012.

[17] A. Meneely and L. Williams. Secure open source collaboration: an empirical study of linus' law. In *Intl Conference on Computer and Communications Security (CCS)*, pages 453–462, Chicago, Illinois, USA, 2009. ACM.

[18] A. Meneely and L. Williams. On the use of issue tracking annotations for improving developer activity metrics. *Advances in Software Engineering*, 2010:1–9, 2010.

[19] A. Meneely and L. Williams. Strengthening the empirical analysis of the relationship between linus' law and software security. In *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, ESEM 2010, pages 9:1–9:10, 2010.

[20] A. Meneely and L. Williams. Socio-technical developer networks: Should we trust our measurements? In *International Conference on Software Engineering (ICSE)*, pages 281–290, Waikiki, Hawaii, USA, May 2011. ACM.

[21] A. Meneely, L. Williams, W. Snipes, and J. Osborne. Predicting failures with developer networks and social network analysis. In *Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of software engineering*, SIGSOFT '08/FSE-16, pages 13–23, 2008.

[22] A. Meneely and O. Williams. Interactive churn: Socio-technical variants on code churn metrics. In *Intl Workshop on Software Quality*, page to appear, Nov. 2012.

[23] S. Mishra, C. Romanowski, R. K. Raj, T. Howles, and J. Schneider. A curricular framework for critical infrastructure protection education for engineering, technology and computing majors. In *Frontiers in Education Conference, 2013 IEEE*, pages 1779–1781, Oct 2013.

[24] R. K. Raj. Experiences with the active collections framework. In R. Meersman, Z. Tari, and D. Schmidt, editors, *On The Move to Meaningful Internet Systems 2003: CoopIS, DOA, and ODBASE*, volume 2888 of *Lecture Notes in Computer Science*, pages 1504–1520. Springer Berlin Heidelberg, 2003.

[25] R. K. Raj and R. Savacool. Experiences with teaching secure data management. In *Frontiers in Education Conference (FIE), 2010 IEEE*, pages S3F–1–S3F–6, Oct 2010.

[26] M. Robertson, Y. Pan, and B. Yuan. A social approach to security: Using social networks to help detect malicious web content. In *Proceedings of the International Conference on Intelligent Systems and Knowledge Engineering*, pages 436–441.

[27] C. Romanowski, S. Mishra, R. K. Raj, T. Howles, and J. Schneider. Information management and decision support in critical infrastructure emergencies at the local level. In *Technologies for Homeland Security (HST), 2013 IEEE International Conference on*, pages 113–118, Nov 2013.

[28] T. Schellenberg, B. Yuan, and R. Zanibbi. Layout-based substitution tree indexing and retrieval for mathematical expressions.

[29] Y. Shin, A. Meneely, L. Williams, and J. Osborne. Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. *IEEE Trans. Softw. Eng.*, PP(99):1, 2011.

[30] K. Stokes, B. Yuan, D. Johnson, and P. Lutz. ICMP covert channel resiliency. In K. Elleithy, T. Sobh, M. Iskander, V. Kapila, M. A. Karim, and A. Mahmood, editors, *Technological Developments in Networking, Education and Automation*, pages 503–506. Springer Netherlands.

BO YUAN

A. Professional Preparation

Shanghai Normal University, China	Mathematics	B.S.	1985
Shanghai Normal University, China	Applied Mathematics	M.S.	1988
Binghamton University (SUNY)	Systems Science	Ph.D.	1996
Postdoctoral Research Fellow NASA ACE Center New Mexico Highlands University	Intelligent Control	Postdoctoral	1996 to 1997

B. Appointments

- Associate Professor, Department of Computing Security, Rochester Institute of Technology, 2012–present.
- Associate Professor, Department of Networking, Security, and Systems Administration, Rochester Institute of Technology. 2009–2012.
- Assistant Professor, Department of Networking, Security, and Systems Administration, Rochester Institute of Technology. 2005–2009.
- Assistant Professor, Department of Information Technology, Rochester Institute of Technology. 2003–2005.
- Staff Scientist, Manning and Napier Information Services/Perspective Partners Rochester, New York. 1997–2003.
- Assistant Professor, Department of Mathematics, Shanghai Normal University, Shanghai, China. 1988–1991.

C. Products

C.1 Five Most Related

1. W. Huba, **B. Yuan**, Y. Pan, and S. Mishra, "Towards a web tracking profiling algorithm" IEEE International Conference on Technologies for Homeland Security (HST), pp. 12-17, 2013.
2. W. Huba, **B. Yuan**, D. Johnson, and P. Lutz, "A HTTP cookie covert channel," in Proceedings of the 4th international conference on Security of information and networks, ser. SIN 11. New York, NY, USA: ACM, 2011, pp. 133-136.
3. R. Zanibbi and **B. Yuan**, "Keyword and image-based retrieval for mathematical expressions," in Proc. Document Recognition and Retrieval XVIII, Proc. SPIE, vol. 7874, 2011.
4. E. Brown, **B. Yuan**, D. Johnson, and P. Lutz, "Covert channels in the HTTP network protocol: Channel characterization and detecting man-in-the-middle attacks," The Journal of Information Warfare, vol. 9, no. 3, pp. 26-38, 2010.
5. **B. Yuan**, "Secure communication with an asymptotic secrecy model." Knowledge-Based Systems, 20(3), pp. 478-484, 2007.

C.2 Five Other

1. T. Chellenberg, **B. Yuan**, and R. Zanibbi, "Layout-based substitution tree indexing and retrieval for mathematical expressions," Document Recognition and Retrieval XIX. Edited by Chien, Liang-Chy; Lee, Sin-Doo; Wu, Ming Hsien. Proceedings of the SPIE, Volume 8297, article id. 82970I, 8 pp. 2012.

2. E. Golen, **B. Yuan**, and N. Shenoy, An evolutionary approach to underwater sensor deployment, International Journal of Computational Intelligence Systems, vol. 2, no. 3, pp. 182201, 2009.
3. **B. Yuan** and George Klir, "chapter Data-driven identification of key variables," In: Intelligent Hybrid Systems: Fuzzy Logic, Neural Networks, and Genetic Algorithms, Kluwer, Boston, 1997.
4. Klir, G. and **B. Yuan** [1995] Fuzzy Sets and Fuzzy Logic: Theory and Applications. Prentice Hall, Upper Saddle River, NJ.
5. Calistri-Yeh, R. J., **B. Yuan**, G. B. Osborne, and D. L. Snyder, "Construction of trainable semantic vectors and clustering, classification, and searching using trainable semantic vectors," US Patent No. 6751621, 7299247, 7406456, 7912868, 8024331.

D. Synergistic Activities

1. Coached the RIT team that won CCDC National Champion
2. Coordinated cybersecurity effort at RIT as the director of The Center for the Advancement of Research and Education in Information Assurance (CARE-IA)
3. Instigated the re-design of computing security curriculum
4. Initiated covert communication research at RIT
5. Invented the TSV technology and implemented TSV based searching and clustering algorithms, while employed at Manning and Napier Information Service.

E. Collaborators and Other Affiliations

- Collaborators within the past 48 months
  - Daryl Johnson, RIT
  - Peter Lutz, RIT
  - Andrew Meneely, RIT
  - Sumita Mishra, RIT
  - Yin Pan, RIT
  - Richard Zanibbi, RIT
  - Rajendra K. Raj, RIT
  - N. Shenoy, RIT
- Graduate advisors and postdoctoral sponsors
  - George J. Klir, Binghamton University (Ph.D. advisor)
  - Djuro George Zrilic, NASA ACE Center/New Mexico Highlands University (Postdoctoral advisor)
- M.S. thesis/capstone advisor, with 19 M.S. students graduated:
  - *Current affiliations included where known.*
    T. Watt (Parsan), W. Huba (Hiveary) , T. Tufts (BAE), R. Savacool (Nixon Peabody), P. Lloyd, D. Pisano (MITRE), J. Salcedo, M. N. Guillermo, C. Forbes, M. Gottlieb, J. Koppe (Lead), L. Kailburn, R. Asencio, T. J. Lantier, C. Janiak, Y. Xu, N. Dave, M. N. Ko & A. Tani

ANDREW MENEELY

A. Professional Preparation

Calvin College	Computer Science	BA	2006
	Additional Major: Mathematics		
North Carolina State University	Computer Science	MS.	2008
	Computer Science	Ph.D.	2011

B. Appointments

- Assistant Professor, Department of Software Engineering, Rochester Institute of Technology, 2011–present.
  Secondary member, Department of Computing Security.

C. Products

C.1 Five Most Related

1. **Andrew Meneely**, Harshavardan Srinivasan, Ayemi Musa, Alberto Rodriguez, Matthew Mokary, and Brian. Spates, "When a patch goes bad: Exploring the properties of vulnerability-contributing commits". Proceedings of the 2013 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, 2013
2. **Andrew Meneely**, Ben Smith, Laurie Williams. "Validating Software Metrics: A Spectrum of Philosophies", Transactions on Software Engineering Methodologies (TOSEM), vol 21. no. 4.
3. **Andrew Meneely**, Laurie Williams, "Socio-Technical Developer Networks: Should We Trust Our Measurements?" Int'l Conference on Software Engineering (ICSE) 2011, p281-290.
4. Yonghee Shin, **Andrew Meneely**, Laurie Williams, Jason Osborne. "Evaluating Complexity, Code Churn, and Developer Activity Metrics as Indicators of Software Vulnerabilities." IEEE Transactions on Software Engineering (TSE) 2011, vol 37, issue 6, p772-787.
5. **Andrew Meneely**, Laurie Williams. "Secure Open Source Collaboration: An Empirical Study of Linus' Law". Computer and Communication Security (CCS), Chicago, IL, pp453-462, 2009.

C.2 Five Other

1. **Andrew Meneely**, Laurie Williams. "Strengthening the Empirical Analysis of the Relationship between Linus' Law and Software Security." Empirical Software Engineering & Measurement (ESEM), Bolzano-Bozen, Italy, pp. 1-10, 2010.
2. **Andrew Meneely**, Pete Rotella, Laurie Williams. "Does Adding Manpower Also Affect Quality? An Empirical, Longitudinal Analysis", Foundations in Software Enginering (FSE), Szeged, Hungary, 2011.
3. Laurie Williams, **Andrew Meneely**, Grant Shipley. "Protection Poker: The New Software Security 'Game' " in IEEE Privacy & Security 2010, vol. 8, no. 3, pp. 14-20.
4. **Andrew Meneely**, Oluyinka Williams. "Interactive Churn Metrics: Socio-technical Variants of Code Churn" at the Int'l Workshop on Software Quality (WoSQ). Raleigh, NC, USA. 2012.
5. **Andrew Meneely**, Laurie Williams, Jason Osborne, Will Snipes, "Predicting Failures with Developer Networks and Social Network Analysis" in Foundations in Software Engineering (FSE), Atlanta, GA, pp. 13-23, 2008.

D. Synergistic Activities

1. Performed empirical case studies on the security of three large open source products (Linux Kernel, PHP programming language, Wireshark). The case studies research comprised the large part of Andrews doctoral dissertation, and was the source of several top-tier publications. This work resulted the following contributions:
   - The discovery that social network analysis of software development teams can be used to generate metrics that (a) give us actionable insight into team structure, and (b) are correlated with post-release vulnerabilities at the file level.
   - A predictive model that can predict post-release vulnerabilities at the source code file level. This model is one of the most robust and informative vulnerability prediction models found in the academic literature.
2. Liaised and consulted for industry partners on several empirical and quantitative case studies, focusing on process metrics in the realm of software reliability. These case studies have resulted in several top-tier publications in addition to providing analytics and insight for the industrial partners.
3. Developed and taught four terms of an undergraduate course titled "Engineering Secure Software." This course is required for all Software Engineering undergraduates.

E. Collaborators and Other Affiliations

- Collaborators within the past 48 months
  - Christian Bird, Microsoft
  - Premkumar Devanbu, UC Davis
  - Marcin Lukowiak, RIT
  - Joan Myers, ARA
  - Jason Osborne, NCSU
  - Stanisław Radziszowski, RIT
  - Rajendra K. Raj, RIT
  - Pete Rotella, Cisco
  - Emad Shihab, RIT
  - Yonghee Shin, NCSU
  - John Slankas, NCSU
  - Ben Smith, NCSU
  - Brian Spates, RIT
  - Harshavardhan Srinivasan, RIT
  - James Vallino, RIT
  - Oluyinka Williams, RIT
  - Bo Yuan, RIT
- Graduate advisors and postdoctoral sponsors
  - Laurie Williams, North Carolina State University Graduate advisor)
- Current students at RIT:
  - Matthew Mokary (undergrad), Ayemi Musa (MSc), Brian Spates (Undergrad), Oluyinka Williams (undergrad), Alberto Rodriguez (MSc)

RAJENDRA K. RAJ

A. Professional Preparation

Indian Institute of Technology, Madras, India	Electrical Engineering	B.Tech.	1980
The University of Tennessee, Knoxville	Computer Science	M.S.	1983
University of Washington, Seattle	Computer Science	M.S.	1985
University of Washington, Seattle	Computer Science	Ph.D.	1991

B. Appointments

- Professor, Department of Computer Science, Rochester Institute of Technology, 2008–present. Secondary member, Department of Computing Security.
- Associate Professor, Department of Computer Science, Rochester Institute of Technology, 2001–08.
- Vice President (from 1996), Information Technology Division, Morgan Stanley & Co., New York, 1992–2001.
- Assistant Professor, Department of Computer Science, SUNY, Oswego, 1985–86, 1990–92.

C. Products

C.1 Five Most Related

1. C. J. Romanowski, S. Mishra, **R. K. Raj**, T. Howles & J. Schneider, "Information Management and Decision Support in Critical Infrastructure Emergencies at the Local Level," *IEEE Conference on Technologies for Homeland Security (HST '13)*, Boston, Nov 2013.
2. S. Mishra, C. J. Carol Romanowski, **R. K. Raj**, T. Howles & J. Schneider, "A Curricular Framework for Critical Infrastructure Protection Education for Engineering, Technology and Computing Majors," *2013 IEEE Frontiers in Education Conference*, Oklahoma City, Oct 2013.
3. S. Alshehri and **R. K. Raj**, "Secure Access Control for Health Information Sharing Systems," *IEEE International Conference on Healthcare Informatics*, Philadelphia, Sep 2013.
4. S. Alshehri, S. P. Radziszowski & **R. K. Raj**, "Secure Healthcare Data Management in the Cloud Using Ciphertext-Policy Attribute-Based Encryption," *ICDE Workshop on Data Management in the Cloud (DMC)*, Washington, DC. April 2012.
5. **R. K. Raj** and R. Savacool, "Teaching Secure Data Management," *2010 IEEE Frontiers in Education Conference*, Washington, DC, October 2010.

C.2 Five Other

1. C. J. Romanowski and **R. K. Raj**, "Catching the Wave: Big Data in the Classroom," mini-workshop, *2013 IEEE Frontiers in Education Conference*, Oct 2013.
2. X. Liu,**R. K. Raj**, T. Reichlmayr, C. Liu, and A. Pantaleev, "Teaching Service-Oriented Programming to CS & SE Undergraduate Students," workshop, *2013 IEEE Frontiers in Education Conference*, Oct 2013.
3. R. J. Bailey, H-P. Bischof, M. Kwon, T. Miller and **R. K. Raj**, "On Providing Successful Research Experiences for Undergraduates," *2011 IEEE Frontiers in Education Conference*, Rapid City, Oct 2011.
4. **R. K. Raj**, S. Mishra, C. J. Romanowski and T. M. Howles,"CyberSecurity as General Education," *Colloquium for Information Systems Security Education*, Fairborn, OH, June 2011.
5. C. A. Wood and **R. K. Raj**,"Keyloggers in Cybersecurity Education," *2010 International Conference on Security and Management*, Las Vegas, July 2010.

D. Synergistic Activities

1. Current research includes security and distribution sy large-scale and cloud data management, as applied to scientific, financial, healthcare domains, and critical infrastructure protection.
2. Current pedagogical projects include improving computing education, and developing course modules for educating underraduates and high school seniors about critical infrastructure protection.
3. As a member of RIT steering committees, helped to create three innovative graduate programs: (i) a Ph.D. in use-inspired computing, (ii) an M.S. in computing security & information assurance, and (iii) a certificate program in Big Data Analytics.
4. Recent curricular development include creating and teaching graduate courses in secure coding; mobile computing; big data analytics; and in cloud and large-scale data management.
5. Focus on program assessment and improvement, and have consulted with several universities internationally. Also serve as an ABET/CAC Program Evaluator (and Commissioner, 2013-15).

E. Collaborators and Other Affiliations

- Collaborators within the past 48 months
  - Suhair Alshehri (RIT), Reynold Bailey (RIT), Bharat Bhole (RIT), Hans-Peter Bischof (RIT), Tara Bolt (GST BOCES), Zack Butler (RIT), Michael Bilynsky (CCC), Daryl Dates (CCC), Trudy Howles (RIT), Minseok Kwon (RIT), Chunmei Liu (Howard University), Xumin Liu (RIT), Alicia McNett (CCC), Andrew Meneely (RIT), Tracy Miller (RIT), Sumita Mishra (RIT), John Owens (GST BOCES), Alex Pantaleev (SUNY Oswego), Stanisław Radziszowski (RIT), Manian Ramkumar (RIT), Thomas Reichlmayr (RIT), Carol Romanowski (RIT), Richard Savacool (RIT), Jennifer Schneider (RIT), Priyanka Sinha (Microsoft), Christopher Wood (RIT) and Bo Yuan (RIT).
- Graduate advisors and postdoctoral sponsors
  - Henry M. Levy, University of Washington, Seattle (Ph.D. advisor)
- M.S. thesis/capstone advisor, with 64 M.S. students graduated:
  - *Current affiliations included where known.*
    Anup Ahire, Susan Athalye, Adarsh Atluri (Expedia), Christopher Ball, Kalexin Baoerjiin (IBM), Manjunath Beeraladinni (Barclays), Harita Chilukuri, Alan Cohen, Christopher Corcimiglia, Muhannad Darnasser, Nikhil Deshpande, Bhavik Desai, Pooja Desai, Bhavik Doshi, Rinkesh Dubey, Prabin Dutta, Pardeep Farwaha, Bhaskar Gopalan, Mustafa Furniturewala, Mayank Goel (Ernst & Young), Sreeprasad Govindankutty, Ashish Gupta, Nitasha Gupta, Rahul Gupta, Yan Hu, Rasika Joshi, Ravi Ram Kallepalli (NVIDIA), Abhishek Kamble, Omkar Kolangade, Megan Kukielka (TCGplayer.com), Shalabh Kumar, Xuxuan Liang, Gourav Mitra, Sushil Magdum, Munira Manasawala, Rutul Mashruwala, Vikas Mathur, Catherine McCorkindale (Xerox), Mayank Mehta, Jogesh Menon, Ashfaq Mohammed, Asha Patel, Nikhil Patil, Vinod Pesara, Viswanath Prasad, Subodh Raikar, Ashish Rathod (Ford), Keith Russell, Supreet Sachadeva, Mohanish Sawant, Navalkishore Sarda, Arpit Shah, Chitrang Shah, Yesha Shah, Chandni Sharma, Vishal Sharma, Deepak Shenoy, Priyanka Sinha (Microsoft), Vanshika Sinha, Soujanya Soni (IBM Research, India), Victoria Steck, Karthikeyan S. N. Sridhar (Microsoft), Joseph Tholath & Haojuan Xu.

SUMMARY PROPOSAL BUDGET

YEAR 1

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
Rochester Institute of Tech

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Bo Yuan

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Bo Yuan - PI**	0.00	0.00	0.75	**8,750**	
2. **Andrew P Meneely - Co-PI**	0.00	0.00	0.50	**4,662**	
3. **Rajendra K Raj - Co-PI**	0.00	0.00	0.50	**6,694**	
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**3**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	1.75	**20,106**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**1**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**2,400**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**22,506**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,213**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**24,719**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**2,408**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **120,000**					
2. TRAVEL **18,000**					
3. SUBSISTENCE **0**					
4. OTHER **6,000**					
TOTAL NUMBER OF PARTICIPANTS (**6**) TOTAL PARTICIPANT COSTS				**144,000**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**600**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**3,911**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**206,544**	
TOTAL OTHER DIRECT COSTS				**211,055**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**382,182**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Modified Total Direct Costs (Rate: 44.5000, Base: 31638)**					
TOTAL INDIRECT COSTS (F&A)				**14,079**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**396,261**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**396,261**	

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Bo Yuan

ORG. REP. NAME*
David Bond

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET

YEAR 2

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
Rochester Institute of Tech

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Bo Yuan

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Bo Yuan - PI**	0.00	0.00	0.75	**9,013**	
2. **Andrew P Meneely - Co-PI**	0.00	0.00	0.50	**4,802**	
3. **Rajendra K Raj - Co-PI**	0.00	0.00	0.50	**6,895**	
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**3**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	1.75	**20,710**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**1**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**2,400**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**23,110**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,259**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**25,369**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**5,228**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **270,000**					
2. TRAVEL **36,000**					
3. SUBSISTENCE **0**					
4. OTHER **12,000**					
TOTAL NUMBER OF PARTICIPANTS (**12**) TOTAL PARTICIPANT COSTS				**318,000**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**1,200**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**4,028**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**462,629**	
TOTAL OTHER DIRECT COSTS				**467,857**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**816,454**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Modified Total Direct Costs (Rate: 44.5000, Base: 35825)**					
TOTAL INDIRECT COSTS (F&A)				**15,942**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**832,396**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**832,396**	

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Bo Yuan

ORG. REP. NAME*
David Bond

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET

YEAR 3

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
Rochester Institute of Tech

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Bo Yuan

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Bo Yuan - PI**	0.00	0.00	0.75	**9,283**	
2. **Andrew P Meneely - Co-PI**	0.00	0.00	0.50	**4,946**	
3. **Rajendra K Raj - Co-PI**	0.00	0.00	0.50	**7,102**	
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**3**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	1.75	**21,331**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**1**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**2,400**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**23,731**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,307**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**26,038**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**5,228**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **150,000**					
2. TRAVEL **18,000**					
3. SUBSISTENCE **0**					
4. OTHER **6,000**					
TOTAL NUMBER OF PARTICIPANTS (**6**) TOTAL PARTICIPANT COSTS				**174,000**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**600**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**4,149**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**256,928**	
TOTAL OTHER DIRECT COSTS				**261,677**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**466,943**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Modified Total Direct Costs (Rate: 44.5000, Base: 36014)**					
TOTAL INDIRECT COSTS (F&A)				**16,026**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**482,969**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**482,969**	

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Bo Yuan

ORG. REP. NAME*
David Bond

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET

Cumulative

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **Rochester Institute of Tech**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Bo Yuan**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Bo Yuan - PI**	0.00	0.00	2.25	**27,046**	
2. **Andrew P Meneely - Co-PI**	0.00	0.00	1.50	**14,410**	
3. **Rajendra K Raj - Co-PI**	0.00	0.00	1.50	**20,691**	
4.					
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**3**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	5.25	**62,147**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**3**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**7,200**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**69,347**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**6,779**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**76,126**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**12,864**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **540,000**					
2. TRAVEL **72,000**					
3. SUBSISTENCE **0**					
4. OTHER **24,000**					
TOTAL NUMBER OF PARTICIPANTS (**24**) TOTAL PARTICIPANT COSTS				**636,000**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**2,400**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**12,088**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**926,101**	
TOTAL OTHER DIRECT COSTS				**940,589**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**1,665,579**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**46,047**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**1,711,626**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**1,711,626**	

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME: **Bo Yuan**

ORG. REP. NAME*: **David Bond**

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

C ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

RIT Budget Justification

Bo Yuan, Ph.D.

NSF SFS: Scholar Track: Preparing Crosscutting Cybersecurity Scholars

Salary amounts are based on actual salaries and include a 3% annual cost of living increase for faculty and staff. RIT utilizes a 9.5 month contract for the Academic Year.

Senior Personnel:

Bo Yuan, PhD, Associate Professor, PI: salary support is requested for three weeks summer (7.89% effort) salary for each of the three years. PI Yuan will be responsible for promoting the RIT SFS program and the supervision of graduate and undergraduate students who are enrolled in the program. PI Yuan also serves as the main point of contact at RIT with NSF on all issues related to this project.

Andy Meneely, PhD, Assistant Professor, Co-PI: salary support is requested for two weeks summer (5.26% effort) salary for each of the three years. Co-PI Meneely will be responsible for promoting the RIT SFS program and the supervision of graduate and undergraduate students who are enrolled in the program.

Rajendra Raj, PhD, Professor, Co-PI: salary support is requested for two weeks summer (5.26% effort) salary for each of the three years. Co-PI Raj will be responsible for promoting the RIT SFS program and the supervision of graduate and undergraduate students who are enrolled in the program. Dr. Raj will also assume the responsibility for the internal assessment and evaluation of the project.

Other Personnel:

Consultant/Evaluator Support

Trudy Howles, PhD, will be hired as the external evaluator for this project. Dr. Howles will be responsible for finalizing a detailed Assessment and Evaluation plan and evaluating the RIT SFS program at the end of each year to ensure the project remains on track. $12,088 for three years in total is requested to support this effort. By the time this project takes effect, Dr. Howles will be retired from RIT but will continue to provide the required assessment and evaluation.

Administrative Staff Support: Salary support is requested for a total of 160 hours per year of the three years at the rate $15 per hour. The person will be responsible for managing application materials, handling any paperwork including seminar announcements, travel arrangements, appointments with students, etc.

Benefits:

Benefits for summer effort for the PI and Co-PIs are calculated at provisional FY 2013 rate of 8.1%. Benefits are not assessed on student stipends or wages. Actual rates will be used once known.

Capital Equipment:

None

Travel:

Support is requested for one PI or Co-PIs to travel along with students to a security conference in the first and the third year, two PI or Co-PIs travel along with students in the second year. Support is also requested for PI to travel to NSF in each of the three years.

Faculty Trip Summary –

Destination	**Number of Travelers**	**Budget year**
PI travel to NSF	1	1, 2, 3
Shmoocon	2	1, 2, 3
RSA Conference	2	2, 3

Students enrolled in this program will be required to attend OPM job fair every year. They are also encouraged to attend one additional technical conference as a presenter or an audience at least once during the two years in the program.

Student Trip Summary –

Destination	**Number of Travelers**	**Budget year**
OPM job fair	12	1, 2, 3
Shmoocon	6	1, 2, 3
RSA Conference	6	2, 3

Travel Estimate Cost Detail

All estimates based on representative costs found on internet travel sites such as Orbitz and/or Travelocity, hotel websites, cab company websites, university websites, conference sites and/or historical averages. The RIT per diem for meals is $44/day.

Destination	**Category**	**Total**
PI Meeting at NSF, Washington, DC	RT Airfare –	$ 400
	Hotel Accommodations	$ 400
	Ground Transportation	$ 100
	Meals ($44/day)	$ 132
		$ **1032/trip/person**
Shmoocon, Washington, DC	RT Airfare –	$ 400
	Registration	$ 200
	Hotel Accommodations	$ 500
	Ground Transportation	$ 100
	Meals ($44/day)	$ 176

		$ **1376/trip/person**
RSA Confrence, San Francisco, CA, USA Estimation for domestic travel	RT Airfare –	$ 800
	Hotel Accommodations	$ 1000
	Academic Registration Fee	$ 700
	Ground Transportation	$ 100
	Meals ($44/day)	$ 220
		$ 2820/trip/person

Participant Support:

RIT Golisano College of Computing and Information Sciences has tuition rates at $34,424 a year for undergraduate students, $37236 for graduate students currently. Stipend, SFS job fair and other travel, and textbook allowance are specified as the same as in the program solicitation document. Here is a summary of student support costs.

Category	Year 1 6 undergraduate	Year 2 6 undergraduates a 6 graduates	Year 3 6 graduates	Total
Stipend	$120,000	$270,00	$150,000	$540,000
Tuition	$206,544	$462,629	$256,928	$926,101
SFS Job Fair and o Travel	$18,000	$36,000	$18,000	$72,000
Textbook Allowan	$6,000	$12,000	$6,000	$24,000

Other Direct Costs:

We are requesting $2,400 in total for Materials and Supplies, $100 for each student each year for incidentals that may incur during monthly meetings such as presentation material cost, USB drivers, etc.

F&A/Indirect Costs:

Rochester Institute of Technology has a 44.5% F&A rate applied to all modified direct costs. Modified costs are direct costs less capital equipment (value of >$1,500 and a useful life >1 year life), participant costs, tuition and the amount in excess of $25,000 of each subcontract.

RIT's cognizant federal agency is the Department of Health and Human Services, representative Council Moore (212-264-2069). A copy of the most recent agreement can be found at: http://www.rit.edu/research/srs/proposalprep/other_costs_to_include.html

Current and Pending Support

Bo Yuan

Support: Pending
Title: SFS Cybersecurity as a Diverse Discipline
Source of Support: NSF
Program: 14-510 Scholarships for Service
Amount Requested: $1,711,625
Project Period: 09/01/2014 - 08/30/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.75 mo

---

Support: Pending
Title: Information Security Talent Search Competition
Source of Support: DOD.National Security Agency (NSA)
Program: BAA 005-13 - Cyber Competition Awards
Amount Requested: $5,980
Project Period: 06/01/2014 - 05/31/2015
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** .05 mo

---

Support: Pending
Title: Gamified Digital Forensics Course Modules for Undergraduates
Source of Support: NSF-National Science Foundation
Program: 11-692 - Advanced Technological Education
Amount Requested: $470,489
Project Period: 06/01/2014 - 05/31/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** .5 mo

---

Current and Pending Support

Andy Meneely

Support: Pending
Title: SFS Cybersecurity as a Diverse Discipline
Source of Support: NSF
Program: 14-510 Scholarships for Service
Amount Requested: $1,711,625
Project Period: 09/01/2014 - 08/30/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.5 mo

---

Support: Pending
Title: Leveraging Developer Knowledge Transfer via Empirical Study of Code Reviews
Source of Support: Rochester Institute of Technology
Program: Grant Writers' Boot Camp
Amount Requested: -
Project Period: 03/01/2013 - 05/31/2014
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:**____

Support: Currnt
Title: Growing the Science of Security Through Analytics
Source of Support: DOD.National Security Agency (NSA) / North Carolina State University - HE (NCSU)
Program: BAA - Science of Security Lablet
Amount Requested: $244,801
Project Period: 03/01/2014 - 03/01/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 1.0

Support: Pending
Title: TWC: Small: Evidence-Based Engineering of Secure Software
Source of Support: NSF-National Science Foundation
Program: NSF 12-596 - Secure and Trustworthy Cyberspace
Amount Requested: $110,947
Project Period: 07/01/2014 - 06/30/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:**____

Support: Pending
Title: SHF: Small: Understanding High-Impact Software Defects: Empirical Analyses of Products and Projects
Source of Support: NSF-National Science Foundation
Program: NSF 12-581 - Computing and Communication Foundations
Amount Requested: $499,910
Project Period: 09/01/2014 - 08/31/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:____** **Acad:____** **Sumr:____**

Support: Pending
Title: CAREER: Engineering Secure Software with Empirical Methods
Source of Support: NSF-National Science Foundation
Program: 11-690 - CISE SHF
Amount Requested: $459,959
Project Period: 05/01/2014 - 05/01/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:____** **Acad:____** **Sumr:____**

Current and Pending Support

Rajendra Raj

Support: Pending
Title: SFS Scholarships
Source of Support: NSF
Program: 14-510 Scholarships for Service
Amount Requested: $1,711,625
Project Period: 09/01/2014 - 08/30/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.5 mo

---

Support: Current
Title: Collaborative Research: Developing Course Modules to Teach Service-Oriented Programming Through Exemplification and Visualization
Source of Support: NSF-National Science Foundation
Program: 10-544 - TUES
Contract Number: DUE-1141200
Amount Awarded: $113,594
Project Period: 08/15/2012 - 07/31/2015
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.25 mo

---

Support: Current
Title: NRI-Small: Human-Robot Collectives as a Curriculum-Wide CS
Source of Support: NSF-National Science Foundation
Program: 11-553 - National Robotics Initiative
Contract Number: IIS-1208566
Amount Awarded: $266,855
Project Period: 10/01/2012 - 09/30/2014
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.5 mo

---

Support: Current
Title: Modular Steps Towards Broadening Expertise in Critical Infrastructure Protection
Source of Support: NSF-National Science Foundation
Program: 12-585 - CyberCorps: Scholarship for Service (SFS)
Contract Number: DUE 1303269
Amount Awarded: $244,295
Project Period: 08/01/2013 - 07/31/2015

Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.5 mo

---

Support: Current
Title: Leveraging historical emergency data to support emergency management
Source of Support: LMI
Program:
Contract Number:
Amount Awarded: $43,789
Project Period: 11/01/2013 - 09/30/2014
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.25 mo

---

RIT Facilities for Security Education

RIT has invested a great deal of time and energy to building state-of-the-art facilities for our students. Students in many lab based courses are assigned laboratory exercises that complement the theories and concepts delivered during classroom lectures.

Five physical labs are used by the Department of Computing Security: The Basic Networking Lab, The Systems Administration Lab, The Projects Lab, The Forensics Lab and The Security Lab (an air-gapped facility). More than 45 routers and 55 switches, various firewall products, Virtual Private Network (VPN) routers, network monitoring hardware, wireless access points, honeynets reside in the labs, as well as a virtualization cluster for student use.

Three terabytes of 14 disk storage are used to provide standard operating system "images" and student workspace. Fiber connections between servers and switches maximize throughput. Servers running Windows and Linux provide various services, authentication and web pages. A supply room "cage" of network supplies (laptops, wireless access equipment, routers, cable testers, etc.) totaling approximately $250,000 is available for students to sign out and use for course-related work. All of the equipment in these labs is used entirely to support the curriculum and is available to students at all times for research, experimentation, testing and learning.

The Security Lab includes 14 benches with multiple workstations on each, as well as equipment racks filled with network and systems security equipment dedicated entirely to student lab work and experimentation. Four of the racks are specified for systems and network security and each includes multiple server-class rack-mount computers, hubs, switches, routers, and firewalls.

The Security Lab is designed with the concept of an "air-gap" to ensure that attack traffic used for classroom experimentation, diagnosis and study remains isolated from the department, and campus infrastructure. Student equipment carried into the lab is prohibited from being connected to the lab infrastructure. This is to prevent attack traffic and malware that may be present in the lab from affecting student owned equipment and RIT campus network.

While the physical labs are still a primary mode of curriculum delivery, many courses and research projects are also running on virtual platforms within the department. GCCIS has built a private-cloud within which students build complex networks and server configurations over a remote connection. This platform provides access to environments that can be network-attached as well as "sandboxed" environments within which malicious code can be released in order to evaluate its function without concern of infecting hosts on other networks. The "sandbox" feature is currently used to support courses in malware and virus deconstruction. The faculty designed and developed cloud-based approach provides students with 24x7 access to the lab environment, with the ability to build complex network and server configurations without the need for physical hardware, and capacity for both guided learning and self-discovery.

Rochester Institute of Technology
SFS Scholarships Project

Preparing Crosscutting Cybersecurity Scholars

Data Management Plan

This plan presents the following:

1. An explanation of the data and artifacts generated through this project including assessment data, software, publications and other materials.
2. The plan for managing and disseminating the project-generated data and artifacts.

1. Data Generated by the Project

Student admission data will be collected via submitted application materials such as resumes, transcripts, and recommendation letters for admission purpose. Once admission decisions are made, and lessons summarized for the following year (only in the first year), student application materials will be sealed and/or destroyed.

As outlined in our assessment and evaluation plan, we will also collect data to assess the effectiveness of our processes such as those used to admit students, mentor students, develop cohort experiences, measure student presentation effectiveness, and student progress over the existence of this SFS Scholarships' program. Some of this data will be collected as pre/post assessments, survey responses, or other feedback. We will develop the evaluation instruments, and retain a repository of the collected data in anonymized form.

We have initiated conversations with RIT's Institutional Review Board (IRB) regarding research using human subjects. We will adhere to all IRB guidelines regarding participant notification and consent, and the confidential collecting and handling of all data.

2. Plan for Managing the Data

The plan for data management has two parts: the management and the dissemination.

Management:
Student records are strictly confidential, protected under the federal Family Educational Rights and Privacy Act of 1974 (FERPA). To protect all students' privacy, we will share the student learning data in summary form only so that we can monitor the level of dissemination for any required reporting. Similarly, we will protect the feedback from instructors and use the anonymized responses only for continuous improvement efforts. We will share the results of the surveys, and will also share the assessment instruments we develop. Survey instruments may be made available through our website.

Confidential data, including individual survey responses and grade data, will not be released to outside parties. This data will be retained throughout the life of the project in anonymized form and used to generate annual reports and the final report to NSF. Once the project has ended, this data will be retained for one year, then purged.

Dissemination:
Summarized student and faculty feedback for evaluating the program that is not considered confidential or protected in nature may be used for reporting purposes.

Related papers and/or conference presentations submitted by the SFS Scholars and the PIs will be made publicly available if allowed by the accepting institution or organization. If the institution or organization accepting the paper or presentation assumes the copyright, we will post a full citation so interested parties can locate the published document.

Standard reports for the NSF will be generated and electronically submitted through normal channels. In addition, we may use summary reports for pedagogical purposes so that other SFS and approved institutions may see our results and lessons learned in supporting these SFS Scholars. Annual and final reports will evaluate our adherence to this Data Management Plan.

TRUDY HOWLES

A. Professional Preparation

Rochester Institute of Technology, Rochester	Computer Science	BS, 1985
Rochester Institute of Technology, Rochester	Computer Science	MS, 1990
Nova Southeastern University, Ft. Lauderdale	Educational Specialist	2006
Nova Southeastern University, Ft. Lauderdale	Computing Technology in Education	PhD, 2007

B. Appointments

- Professor, Department of Computer Science, Rochester Institute of Technology, 2012-Present.
- Associate Professor, Department of Computer Science, Rochester Institute of Technology, 2005-2012.
- Assistant Professor, Department of Computer Science, Rochester Institute of Technology, 1997-2005.
- Senior Software Development Engineer, Eastman Kodak Company, Rochester NY, 1994-1997.
- Adjunct Professor, Joint Appointment with the Department of Computer Science and the National Technical Institute for the Deaf, Rochester Institute of Technology, 1989-1995.

C. Products

C.1 Five Most Related

1. C. J. Romanowski, S. Mishra, R. K. Raj, **T. Howles** & J. Schneider, "Information Management and Decision Support in Critical Infrastructure Emergencies at the Local Level," *IEEE Conference on Technologies for Homeland Security (HST '13)*, Boston, Nov 2013.
2. S. Mishra, C. J. Carol Romanowski, R. K. Raj, **T. Howles** & J. Schneider, "A Curricular Framework for Critical Infrastructure Protection Education for Engineering, Technology and Computing Majors," *2013 IEEE Frontiers in Education Conference*, Oklahoma City, Oct 2013.
3. **T. Howles** & P. McQuaid. "Challenges in Building Secure Software." Software Quality Professional, 14(3), June 2012, pp. 4-13.
4. **T. Howles** and P. McQuaid. "Building Secure Software." In Proceedings of the American Society for Quality 2011 International Conference on Software Quality, San Diego, CA, February 8-11, 2011.
5. **T. Howles.** "Emphasizing Privacy Preservation in an Undergraduate Data Mining Course." The Journal of Computing Sciences in Colleges, 27(6), June 2012, pp. 121-127.

C.2 Five Other

1. R. K. Raj, S. Mishra, C. J. Romanowski and **T. M. Howles,"**CyberSecurity as General Education,"*Colloquium for Information Systems Security Education*, Fairborn, OH, June 2011.
2. **T. Howles**, C. Romanowski, S. Mishra, & R. Raj. "A Holistic, Modular Approach to Infuse CyberSecurity into Undergraduate Computing Degree Programs." In Proceedings of the 5th Annual Symposium on Information Assurance (ASIA '11), Albany, NY, 2011.
3. **T. Howles**. "A Study of Attrition and the Use of Student Learning Communities in the Computer Science Introductory Programming Sequence." Computer Science Education, Vol. 19, No. 1, March, 2009.
4. **T. Howles**. "The Declining Interest and Persistence in University Computing Programs." In Proceedings of the World Congress for Software Quality, A joint effort of the American Society for Quality, the Software Group of the European Organization for Quality and the Union of Japanese Scientists and Engineers, Bethesda, MD. Invited speaker, 2008.

5. F. Kazemian & **T. Howles**. "Teaching Challenges: Testing and Debugging Skills for Novice Programmers." Software Quality Professional, 11(1), 5-12, 2008.

D. Synergistic Activities

- Recent curricular development efforts include teaching graduate courses in secure coding, big data analytics, and advanced data mining.
- Delivered six non-credit undergraduate seminars to expose students to cybersecurity vulnerabilities and challenges.
- Completed a 10-week academic leave in 2011 to work with local companies to better understand current security problems and challenges.
- PI on a grant awarded through the RIT Provost's Office to pilot a new approach to delivering the introductory programming sequence. This sequence was carefully structured to support a variety of learning styles based on student backgrounds and characteristics. This effort became the basis for the active learning components of the Institute sponsored Student Learning Communities. Served as a mentor/teacher for the Women in Computing Student Learning Communities for five years; this created a cohort of female students enrolled in computer science, software engineering and computer engineering their entire first year of study
- Co-facilitator of the Institute-wide Faculty Learning Communities for four years, and a current member of RIT's Learning Community Advisory Board

E. Collaborators & Other Affiliations

- ***Collaborators and Co-Editors within the past 48 months***
  - Carol Romanowski, Center for Multidisciplinary Studies, Rochester Institute of Technology
  - Sumita Mishra, Department of Networking, Security & Systems Administration Rochester Institute of Technology
  - Rajendra Raj, Department of Computer Science, Rochester Institute of Technology
  - Steven Terrell, Graduate School of Computer and Information Sciences, Nova Southeastern University
  - Paul Tymann, Department of Computer Science, Rochester Institute of Technology
  - Sage Miller, Math and Computer Science Department, Webster Central Schools
  - Taz Daughtrey, Department of Computer Science, James Madison University
  - Patricia McQuaid, Department of Management Information Systems, California Polytechnic State University

- ***Graduate Advisors and Postdoctoral Sponsors.***
  PhD Graduate Advisor
  - Steven Terrell, Ph.D., Graduate School of Computer and Information Sciences, Nova Southeastern University

- ***MS Thesis/Project Supervisor, Co-chair, or Committee member***
  - Vishal Goradia, Jagadeesh Patchala, Mayank Goel, Ravi Ram Kallepalli, Jason Christopher, Christian Castello, Randall Vorhour, Adarsh Atluri, Michael Sussman, Gregory Fotiades, Anvi Malia, Dawn DiPietra, Joseph Dowling, Eitan Romanoff, Deepak Taunk, Camaria Bevavy, Rahul Jadon, Samhita Phukan, Ramnath Anantharaman, Yamini Santhanam.

  Number of graduate students advised: 20