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./DUE DATE
NSF 16-580 **12/15/16**

☐ Special Exception to Deadline Date Policy

FOR NSF USE ONLY
NSF PROPOSAL NUMBER
1723763

FOR CONSIDERATION BY NSF ORGANIZATION UNIT(S) (Indicate the most specific unit known, i.e. program, division, etc.)
CNS - Secure &Trustworthy Cyberspace

DATE RECEIVED	NUMBER OF COPIES	DIVISION ASSIGNED	FUND CODE	DUNS# (Data Universal Numbering System)	FILE LOCATION
12/15/2016	2	05050000 CNS	8060	002223642	12/16/2016 7:48am 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 MEMORIAL DR
ROCHESTER, NY. 146235603

NAME OF PRIMARY PLACE OF PERF
Rochester Institute of Technology

ADDRESS OF PRIMARY PLACE OF PERF, INCLUDING 9 DIGIT ZIP CODE
Rochester Institute of Technology
141 Lomb Memorial Avenue
Rochester ,NY ,146235603 ,US.

IS AWARDEE ORGANIZATION (Check All That Apply) (See GPG II.C For Definitions)
☐ SMALL BUSINESS ☐ MINORITY BUSINESS ☐ IF THIS IS A PRELIMINARY PROPOSAL
☐ FOR-PROFIT ORGANIZATION ☐ WOMAN-OWNED BUSINESS THEN CHECK HERE

TITLE OF PROPOSED PROJECT **SaTC: EDU: Collaborative: PLASMA: Practical LAbs in Security for Mobile Applications**

REQUESTED AMOUNT	PROPOSED DURATION (1-60 MONTHS)	REQUESTED STARTING DATE	SHOW RELATED PRELIMINARY PROPOSAL NO. IF APPLICABLE
$ 277,051	24 months	05/01/17	

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)
☐ VERTEBRATE ANIMALS (GPG II.D.6) IACUC App. Date _____
PHS Animal Welfare Assurance Number _____
☒ FUNDING MECHANISM **Research - other than RAPID or EAGER**
☐ HUMAN SUBJECTS (GPG II.D.7) Human Subjects Assurance Number _____
Exemption Subsection _____ or IRB App. Date _____
☐ INTERNATIONAL ACTIVITIES: COUNTRY/COUNTRIES INVOLVED (GPG II.C.2.j)
☒ COLLABORATIVE STATUS
A collaborative proposal from one organization (GPG II.D.4.a)

PI/PD DEPARTMENT
Software Engineering

PI/PD FAX NUMBER
585-475-7990

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 **Daniel Krutz**	**PhD**	**2013**	**585-475-2896**	**dxkvse@rit.edu**
CO-PI/PD **John Dean**	**PhD**	**2013**	**816-584-6422**	**john.dean@park.edu**
CO-PI/PD				
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).

Certification Regarding Conflict of Interest

The AOR is required to complete certifications stating that the organization has implemented and is enforcing a written policy on conflicts of interest (COI), consistent with the provisions of AAG Chapter IV.A.; that, to the best of his/her knowledge, all financial disclosures required by the conflict of interest policy were made; and that conflicts of interest, if any, were, or prior to the organization's expenditure of any funds under the award, will be, satisfactorily managed, reduced or eliminated in accordance with the organization's conflict of interest policy. Conflicts that cannot be satisfactorily managed, reduced or eliminated and research that proceeds without the imposition of conditions or restrictions when a conflict of interest exists, must be disclosed to NSF via use of the Notifications and Requests Module in FastLane.

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.

Certification Dual Use Research of Concern

By electronically signing the certification pages, the Authorized Organizational Representative is certifying that the organization will be or is in compliance with all aspects of the United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern.

AUTHORIZED ORGANIZATIONAL REPRESENTATIVE	SIGNATURE	DATE
NAME **Laura J Kleiman**	**Electronic Signature**	**Dec 15 2016 4:57PM**

TELEPHONE NUMBER	EMAIL ADDRESS	FAX NUMBER
585-475-2262	**ljksrs@rit.edu**	**585-475-7990**

PROJECT SUMMARY

Overview:

To meet the growing demand for secure mobile app developers, many institutions have created courses or even entire programs to teach app development or security. Unfortunately, many of these institutions lack the resources to include cybersecurity in their curriculum for both mobile and general software development. This is gravely problematic, especially since the United States already lacks qualified cybersecurity graduates and this shortfall is only expected to grow.

Building on PI Krutz's successful SIGCSE grant, we propose a novel laboratory environment named Practical LAbs in Security for Mobile Applications (PLASMA) to meet this educational gap. The forty proposed modules will each contain instructional material on a vulnerability, a sample app containing the vulnerability, steps to recreate the issue, instructions on how to remedy the problem, and a process to demonstrate that the vulnerability has been repaired. The modules and PLASMA environment will be deployed in a diverse set of educational settings including the lead institution (RIT) and participating institutes (Park University, NC A&T).

Intellectual Merit:

Many institutions lack the ability to add security-related activities to their curriculum due to resource constraints, resulting in a gap in mobile security education. The proposed modules are derived from real-world mobile security vulnerabilities and are systematically designed to cover principles that are fundamental in creating secure mobile applications. Cybersecurity activities are in significant demand in security education. Unfortunately, existing security-related exercises and labs are lacking since many have not been reviewed for quality by qualified security experts, are frequently difficult to adopt due to fragmented environments, or are expensive due to software costs. Our PLASMA modules will be designed and reviewed by cybersecurity experts, be simple to adopt since they will be available in easily deployable virtual machines, will use free and open source software, and will cover a wide range of mobile security topics for all experience levels. Keeping costs at a minimum is essential for ensuring wide-spread adoption, especially at more resource constrained institutions.

The modules will include instructional materials intended to make the adoption of these exercises as easy as possible, along with a variety of pre-installed open-source security tools that will be used in the modules. Using a web interface, instructors will be able to select a set of exercises tailored to their curriculum along with the appropriate experience level of their students. Summative and formative data will be collected throughout the deployment and usage of the modules and this information will be used to improve module design and measure their effectiveness.

Broader Impacts:

The results of this project can have a far-reaching impact on cybersecurity education, which is presently becoming more widespread in the United States (many institutions are creating courses and even entire degree programs in cybersecurity). Our PLASMA modules will have wide appeal, as they may also be used in non-security courses and other and computing-related curriculum. Due to the modular nature of the activities, injection into courses such as software engineering, mobile development, or other programming-oriented curricula is more easily achievable.

Because fewer resources are required for the implementation of our modules, institutions who have limited access to resources are given the opportunity to implement them as well. These modules can be used in a variety of outreach events, providing valuable feedback and helping to promote cybersecurity to underrepresented groups. Our initial activities have already been used in outreach activities for urban high school students, and RIT's Women in Computing organization. Plans are in place for our initial activities to be used at the New York Celebration of Women in Computing (NYCWIC), the SEED workshop at Syracuse University, and in other institutions including EPSCOR, HBCU, and HSI schools.

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.

PLASMA: Practical LAbs in Security for Mobile Applications
Project Summary

1 Introduction

The mobile revolution has grown to affect nearly all aspects of our lives, allowing for unprecedented capabilities. Unfortunately, these powerful devices frequently contain serious, and potentially harmful vulnerabilities. Currently, there are not enough highly trained cybersecurity experts in the United States [49]. To address these challenges, our nation needs mobile developers who not only understand how to create secure mobile software, but also grasp the importance of developing secure mobile software. Compared to conventional desktop software, mobile vulnerabilities may be much more impactful for a variety of reasons including the device's ability to know our precise location, amount of personal information stored on it, and even the ability of a mobile device to infect other nearby devices.

Although many institutions have created courses or even entire programs focused on mobile security education, they frequently suffer from challenges in creating high-quality, relevant course materials. Even worse, many institutions have the desire, but lack the necessary resources to create even a single computing security course, thus creating a gap between institutions with unequal amounts of resources. Even when institutions have the necessary resources to create effective mobile security activities, they often still face significant challenges. Creating robust sets of educational materials including lecture slides and activities is typically a very time intensive process, one which often keeps instructors from accomplishing more fulfilling roles such as student mentoring.

There is no existing template for instructors to use when integrating mobile security into their curriculum [44]. This is problematic since instructors are frequently re-inventing the wheel when it comes to cybersecurity education, which is a time consuming and often imperfect task. This fragmented education style is also problematic since it leads to unequal learning outcomes across institutions. Fragmented course materials also create difficulties in evaluating their effectiveness which leads to many questions: Are students learning the necessary security objectives? Is it fostering student interest in security? Are the activities conducive to student learning? We believe that our proposal will address several of the goals outlined by the NSF including helping to create a qualified STEM workforce and assisting STEM instructors in overcoming many of the challenges with adding quality mobile security components to their courses. Students using these activities will be better trained and more enthusiastic about security, thus helping to reduce the high failure rate in these courses.

Instructors are already frequently pressed for time, and existing security labs or activities typically run in different environments, which requires instructors to devote a significant amount of time setting up and configuring these environments. Due to time constraints, this is simply not an option for most instructors. Our proposed PLASMA modules will be encapsulated in an easy to adopt virtual machine environment which will promote its usage in a variety of educational settings.

Rochester Institute of Technology and Park University plan to establish a two-year collaborative project to create educational mobile security modules. This project will also support the implementation of a cybersecurity program at Park University, which RIT will provide guidance over. Our proposal will also support several outreach activities focused on attracting underrepresented students to the field of cybersecurity.

2 NSF Merit Review Criteria

2.1 Intellectual Merit

The proposed modules, which will be created using real-world security vulnerabilities as guidelines, are systematically designed to cover a wide range of both fundamental security concerns as well as those which are far more advanced. These modules may also be used in a wide range of environments including computing outreach events and university level general programming, security and mobile courses. A primary goal of these modules is to allow them to be easily used at a far reaching number of institutions, especially those which currently might otherwise not possess the resources to offer similar activities. The proposed modules will be built upon a free laboratory environment, so adopters will only need to install free software to use our modules. This low cost, easy to use methodology is imperative for ensuring adoption on a large scale.

2.2 Broader Impacts

Although many institutions have added mobile or security courses to their curriculum, institutions frequently struggle in adding security to their curriculum [35, 5, 50]. Instructors frequently lack the time, resources, or knowledge to create robust, intriguing, real-world examples and instructional materials on how to most properly teach the creation of secure mobile apps. *We propose the creation of a unique set of educational mobile security modules to address these challenges.* These modules will contain instructional material, activities and evaluation tools which may be used in a variety of classrooms and outreach events. A primary objective is to not only make security education easier to include in the classroom, but importantly more fun and educational for students as well.

The outcome of this project has the potential to have an extensive impact on not only cybersecurity or mobile education, but on computing education as a whole. Due to their simplicity of adoption, the modules can easily be used in a variety of computing courses and outreach events. The inclusion of security related activities will become even more important as cybersecurity becomes more broadly included in existing computing programs and with the creation of cybersecurity programs. This project also cultivates a partnership between our two Universities, a byproduct of which will assist with Park University's creation of cybersecurity related curriculum and importantly create a a collaborative environment for improving computer security education.

To share our work with the community, the modules will be presented at a variety of venues including conference tutorials and outreach events. Our work will be submitted as papers to educational venues such as ICSE-SEET, SIGCSE, ITiCSE, CISSE, SIGITE, and ASEE. A tutorial based on our initial modules has already been accepted to appear at SAC 2017 [19]. We have been invited to share our modules at NY-CWIC [13], an annual conference for women in computing which is attended by approximately 250 students from across New York state. An objective of holding tutorials is to inform instructors about our modules so that they may use them in their own classes and outreach events. Outreach events will serve to educate students about the importance of creating secure software and get them interested in this important topic. Three partner schools (Curry College, Cal St. Chico, and NC A&T), including two which predominately serve underrepresented students, have agreed to use the modules in their curriculum.

3 Design Philosophy

3.1 Challenges With Current Educational Techniques:

Traditionally, there have been four main approaches to teaching students about software security. The first is for students to use security tools, such as intrusion detection systems and firewalls to analyze a system and

learn more about its possible vulnerabilities. In *attack-based* labs, students exploit systems to identify and exploit vulnerabilities. This approach is especially adept at teaching students the skills of penetration testing. *Administration-based* labs focus on teaching students to use security tools to enhance a system's security. The final popular approach is for students to design and create secure systems from scratch. Although these teaching styles can be very effective in a variety of situations, they do suffer from drawbacks which are addressed in our proposal. For example, while penetration testing and performing system exploitation activities can be a valuable skill for a software developer, they will often spend little time conducting these activities. Knowing defensive coding skills and how to properly protect the system is a more paramount skill for a software developer to posses [51]. Most existing labs cover a variety of security related activities ranging from firewalls to vulnerability analysis tools for C. Although this diversification is likely beneficial for many situations, it is not the most appropriate material for for courses which focus on mobile security.

There are many existing security exercises which may be found from a variety of sources ranging from online blogs, to funded NSF grants. Although there are a plethora of online resources for teaching various security principles [3, 22, 15, 10], these resources are deficient in a variety of ways, including: (I) They may not have been examined by security experts to ensure their quality (II) Are not available in a single environment, which can hinder adaptability (III) Not created in a uniform fashion, so each activity may be conducted in an inconsistent manner (IV) Do not contain a diverse set of security related activities (V) Do not contain supplementary educational materials.

Existing projects present security related educational activities [35, 38, 29, 50]. Although these works address a wide range of security topics using a hands on approach, none are focused on mobile security to the extent as our proposal, and do not provide instructional materials or an environment to aid in adoption. There have also been several recently funded NSF grants including ITSEED [27] and SEEDLabs[31] which create security related activities similar in format to ours. These grants address mobile security, but from the focal point of the system and not application perspective as we do. These labs have seen considerable success and adoption since their creation. We believe that we will realize similar success by using a similar concept of modules and a sharing mechanism using Virtual Machines. Yang et al. [6] focused on building security modules and in developing a course in mobile security. Our work differs in several significant ways including that we will be creating at least forty modules, compared to their six; Our modules will be provided in virtual machines, making their adoption much easier; While their modules are dedicated to app security, most deal with things such as malware or lost devices.

While the concept of mobile security has become an increasingly popular topic in both industrial and academic settings, it is unfortunately not adequately covered in many classrooms [45]. Although larger institutions often have the resources to devote entire courses or even programs to security, many small institutions and those who predominately serve underrepresented students often do not have adequate resources to meet this same objective. This lack of exposure to imperative mobile security concepts will leave these students at a clear disadvantage in relation to their counterparts who are more acclimated with these concepts. Educators frequently struggle with two primary challenges when integrating mobile security related settings into the classroom: (I) Inadequate resources to create the necessary course materials. (II) A lack of proper background knowledge to create the desired tasks [44].

The design of the proposed modules are guided by two objectives, which are based on our firm belief in two teaching philosophies.

Philosophy 1: *Mobile security education should provide real-world examples. Students should be provided opportunities to learn from real-world situations that provide an appropriate background, context and relevance for the examples.*

Software security is a very diverse area and may include topics ranging from social engineering to cryptography and can be covered in a variety of courses and situations from general programming to advanced security courses. Regardless of the course and topic, in order for students to learn to properly protect them-

selves from a vulnerability they must (I) Understand why the vulnerability is detrimental (II) Understand the cause of the vulnerability (III) Understand how to repair/protect against the vulnerability. In this proposal, we create modules which will fulfill these criteria. These principles shape the first objective of this proposed project: *to develop modules which cover a wide range of mobile security principles which as based off real-word examples.*

Philosophy 2: *Software security is important to everyone and software security education should be available to everyone.*

All computing students need to learn about security. Even minor vulnerabilities in the design or implementation of an application can have profound effects on all project stakeholders. Students should not be inhibited from learning about software security due to institution or instructor constraints. Since software security may be included in a diverse set of courses and situations, instructors should be able to pick and choose relevant materials and activities in an *a la carte* fashion. These adaptable modules will enable instructors to select the most relevant materials for their courses. Instructors will be able to select one module for their course, or even base their entire course around our provided materials. These principles shape the second objective of this proposed project: *to develop high quality modules which are ready to use in a variety of settings and contain all related instructional and activity materials.*

3.2 Expected Outcomes

We will create a robust set of modules to meet the desired primary project outcomes:

1. Create activities which will encourage the inclusion of security related concepts, practices and tools in computing courses.
2. Create uniform, multi-institutional activities and evaluation sets to reduce the industrial and educational gap in the mobile security domain.
3. Promote learning by example through using examples from real-world systems.
4. Foster student interest in computing/security through interesting and engaging activities and outreach events.
5. Educate students to create secure software by demonstrating proper security practices and the importance of creating secure software.

As shown in Table 1, our work will be driven by the following research questions:

Table 1: Research Questions

Research Question	Measurement
Are students more interested in security after using these modules?	Pre & post activity questionnaires
Are students who use these modules more likely to stay in computing/security fields?	Comparative measurement of student retention rates
Do the modules affect how students view the importance of security?	Pre & post activity questionnaires
Do the modules help students understand how to create secure apps?	Results from supplied quizzes
Do institutions which use these modules have a better retention rate?	Compare retention rates for institutions using these modules vs. those who do not.

These research questions will be addressed by using data collected by RIT, Park University, and other partner institutions in both classroom and outreach settings.

3.3 Provide Support for Underrepresented Groups

Several schools which serve underrepresented groups have committed to using our modules in their curriculum. These include California State University, Chico (HSI) and North Carolina A&T (HBCU). Women in Computing (WiC)[1] at RIT has also committed to using the modules at various outreach events.

A primary project goal is how the created artifacts may increase student interest and retention in cybersecurity programs, especially in institutions which historically serve underrepresented students. Many of these schools would not otherwise have the resources to include security activities such as ours in their courses. In this proposal, we will be closely working with WiC, the National Technical Institute for the Deaf (NTiD), and other groups at RIT and Park which serve underrepresented students. We will work with these groups to recruit students for both content creation and presentations at conferences and outreach activities in the community. We have been working with WiC to hold outreach workshops, and have already been invited to hold a workshop on our existing materials at NYC WIC [13].

One challenge of including cybersecurity related activities in the curriculum of many schools which serve underrepresented students is a lack of resources to create these activities. We hope that these created modules will allow for the easier inclusion of security related activities at these institutions.

Conducting community outreach activities will provide several benefits. Some of which include allowing us to receive initial feedback on our created artifacts and providing invaluable support to our local communities to reach many young people who would otherwise not be exposed to mobile/security related activities. All outreach events included in our proposed budget are directed towards assisting underrepresented student groups.

4 PLASMA Environment

4.1 Pedagogy:

Our project will use an active learning pedagogy. Research indicates that active learning promotes student retention and increases student performance while further motivating the students in comparison with conventional educational techniques [32, 28]. Research has also demonstrated active learning to be beneficial in security courses, especially when students are provided hands on, real-world examples of the covered topics [30, 48]. While active learning classrooms have demonstrated numerous benefits, especially in security education, they are frequently much more difficult to implement as opposed to conventional lecture driven classes. Instructors frequently struggle with creating active learning environments due to the lacking the necessary resources required to develop or purchase supporting materials for these classroom activities [48, 45].

4.2 Proposed Modules

Using prior funding, we've created ten mobile exercises, which we will continue to build upon. Each module will adhere to a single template to ensure continuity between the activities and make the adoption process of these modules as easy as possible. These modules will focus on important, relevant security concepts in mobile development and will contain the following:

1. Background on the vulnerability

[1] `http://wic.rit.edu/`

2. A YouTube video providing a short lecture on the activity
3. Instructor lecture slides about each vulnerability
4. A YouTube video clearly demonstrating how to conduct the activity
5. A sample app containing the vulnerability
6. Security assessment activity to identify the vulnerability
7. Steps to recreate the vulnerability
8. Steps to repair the vulnerability
9. A process to demonstrate that the vulnerability has been removed
10. Defensive coding practices to prevent vulnerability
11. Real-world examples of the vulnerability in the wild
12. Instructor quizzes to measure activity effectiveness and student comprehension (released only to approved instructors)

Instructors will be able to select each of the module's components as they desire. Our goal is to allow instructors to use as many or as few modules in their courses as they desire. The modules will be primarily intended for undergraduate college students, but should fit into a wide range of curriculum including upper level high school and graduate level courses. To accommodate a diverse set of classrooms and skill sets, the activities will range from simple exercises focused toward novice level developers and security students, to advanced topics intended to educate and motivate even the most experienced developers. Each module is intended to captivate student attention by clearly demonstrating the targeted vulnerability and how it could be exploited using real-world examples when possible.

Each module will contain a brief (5-10 minute) YouTube video providing appropriate background about the vulnerability and another video demonstrating how to conduct the activity. The primary motivations for the videos are to assist in flipped classroom settings, provide instructors with vital information about each vulnerability and to provide an educational mechanism for students who may be working through the modules without instructor support. The modules will be freely available on the project website [21], with each module containing all necessary material to conduct each activity. We will provide instructors materials on how to most appropriately use the modules in their classrooms and in outreach activities.

Modules will include a 10 question quiz on the activity and examined vulnerability. Quizzes and answer keys will only be made available to instructors upon their request and instructor verification through a brief email exchange. The primary objectives for creating these quizzes is to reduce the instructor effort in developing these evaluations, but also create a uniform evaluation mechanism between all institutions. Instructors will be asked, but not required to report aggregate exam scores to project personal. This data will be used to guide the creation of new course modules, adjust existing activities and quizzes, and assess the educational effectiveness of the modules.

Modules will be stand-alone so that instructors can choose only the most appropriate exercise(s) for their classroom. Although all project material will be available to download and use individually, when possible we will also provide all activities on a public Virtual Machine (VM) environment to make the set up and configuration process as easy as possible for the user. Unfortunately, due to platform constraints we will only be able to load Android modules on this VM. iOS activities will be available for individual download on our website.

To guide the creation of appropriate and robust vulnerability examples, we will use several inputs including: (I) Prevalent mobile vulnerabilities which will be found from a variety of sources including CVE databases, and other resources on the web (II) Recommendations from Consultant Richards and Senior Personnel Mirakhorli (III) Using coding style guidelines [14]. Whenever possible, real-world examples will be discussed to reinforce the relevance of the vulnerability. These real-world, hands on examples will help close an existing gap where far too many security related educational activities are only theoretical [45].

Senior Person Mirakhorli and Consultant Richards will provide guidance on selecting the appropriate vulnerabilities to include in our activities, and will review all created materials for accuracy. They will also assist in identifying real-world instances of the vulnerabilities to include in each activity. The following are a few of the vulnerability examples which we will be using in our modules:

- Secure HTTP transmission usage
- Secure use of Ad Libraries
- Secure Intent Usage
- Broadcast receivers: Prevent from receiving unwanted data
- Protection user data input
- Poor Authorization and Authentication
- Insecure activity access
- Context provider leakage prevention
- Protecting broadcast messages
- Javascript security: Protection against WebView attacks
- Denial of service protection
- Security Bundle information protection
- Buffer overflow
- Validating Input and Interprocess Communication
- Race conditions
- Access-control problems
- Weaknesses in authentication, authorization, or cryptographic practices
- Proper privilege escalation
- Designing Secure User Interfaces
- Avoiding Injection Attacks and XSS
- Designing Secure Helpers and Daemons
- DOS protection
- App memory load size
- Client Side Injection prevention

Due to space limitations, we will not include an example module in this proposal. However, you may view the existing *Secure Data Storage* activity on our project website: `http://www.TeachingMobileSecurity.com`.

4.2.1 Example Modules

Using previous funding, we have already created ten security activities. These do not include any supporting materials such as lecture slides, a virtual environment or instructional videos. Based on the amount of time required to construct these initial ten activities, we believe that over the course of the proposal we will be able to create forty modules. We will next describe a few of the selected activities which we will create.

Lab 1: Secure Data transmission (iOS & Android) Students will gain an understanding for properly ensuring that data is being transmitted securely from the app on the device to remote devices or servers. Far too frequently, information is securely stored on the device and the server, but not properly protected during the transmission phase. This module will contain an example of insecure data storage in an app, how it may be exploited, and how it may be repaired. The module will utilize a tool such as Wireshark [25] to examine network traffic.

Lab 2: Designing Secure User Interfaces (iOS & Android) Developers need to focus on creating user interfaces which not only exhibit high levels of usability and accessibility, but which are also secure. Some principles of creating secure interfaces include using secure defaults, securing all interfaces, properly storing all interface output and protecting against social engineering attacks [7]. Our module will contain several examples of user interface design issues, and proper protection measures. A tool suck as Peek [17] will be included in the activity.

Lab 3: Proper use of Ad libraries (iOS & Android) Students will learn the importance of securely using advertising libraries within their apps. Ad libraries are the primary source of revenue for a substantial number of apps. Unfortunately, 3rd party libraries such as these may pose dangers to the app. This module will demonstrate how these libraries gain access to the system's resources and how even seemingly innocent

libraries can perform malicious actions on the system. We will also discuss how static analysis tools, such as VectorAttackScanner [23] and PmDroid [33] can be used to identify possibly malicious ad libraries.
Lab 4: Intent Protection (Android) Students will learn how to securely use Intents in Android development. Intents are essentially messaging objects which may transmit information between components. Although using these may provide many benefits including allowing the OS to more appropriately react to events and allowing component level reuse within and across many apps. Unfortunately, there are security concerns when using Intents. For example, SMS messages are transmitted as Broadcast Intents, so they may be read or captured by other applications that have the READ_SMS permission. This module will discuss the concerns of using Intents and how they may be exploited. The module will also demonstrate how to securely use Intents. Tools such as VectorAttackScanner [23] will be used in the module to demonstrate finding Intent related vulnerabilities and possible exploits.
Lab 5: Secure data storage (iOS & Android) Students will learn how insecurely stored information on a device may be exploited, and how a developer may properly protect this information on a device. Mobile apps frequently store information in a variety of ways with data ranging from a user's high score in a game to their credit card number. It is important for developers to understand: A) What data they should and should not store on a local device B) How to properly protect data stored on the device C) Understand that although in a sandbox, information stored for an app can often be accessible to another app D) Identify potential vulnerabilities in existing systems. The module will provide an example app containing vulnerable data and steps to recreate an exploitation of this information. Students will then perform steps to repair the vulnerability and to then demonstrate that the vulnerability has been properly repaired. We will include a tool such as AppAudit [52] for students to use to check for insecure data storage.

Further modules will be proposed by security Consultant Richards and Senior Person Mirakhorli who will also review all created modules for quality assurance. When applicable, modules will also contain relevant security tools to detect vulnerabilities and show that they have been properly repaired [52, 11, 4, 26, 14, 23, 9, 12, 18, 33]. Including these tools in the virtual machine environment is important since it will reduce the burden of having to install these sometimes difficult tools. All included tools will be robust and popular tools, but will importantly be open source thus allowing for their free inclusion. To achieve widespread adoption and make the inclusion of these activities as easy as possible, instructors will also be provided material to prepare them for teaching the modules. Some of the provided material will include best practices for conducting and recruiting students for outreach events, how to best prepare student assistants for outreach events and best ways to include the modules in various classroom settings.

4.3 PLASMA Environment

A primary motivation of our project is to make it easily adoptable for a large number of institutions in a variety of situations. One of the limitations of existing security exercises and labs is the resource intensive setup and configuration of the required environments. This is a significant task which may inhibit an activity's adoption in a wide variety of situations. To address this limitation, all Android modules and materials will be pre-loaded on a Virtual Box [24] Virtual Machine (VM), which we chose since it is robust and free to download. Based on discussions from developers of the Syracuse SEED project [20], we know that using a single Linux VM for both the tools and Android emulator proved to be a very cumbersome, resource intensive endeavor. This would limit the potential for adoption by users with older, or less powerful machines. The SEED project found that creating two VMs with separate responsibilities alleviated many of the resource constraints and has worked very well in a similar educational environment. We will adopt a dual VM environment provided by the Syracuse SEED project to load our modules upon:

- **Tools VM:** Contains installed security tools and allows user to run commands against app.

- **Android Emulator:** Contains the Android emulator allowing the user to run example apps to see both the negative implications of a vulnerability, and to demonstrate that the vulnerability has been repaired.

We will also provide a instruction manual and support documentation for the PLASMA VM environment which will guide users through the usage process. An overview of our environment is shown in Figure 1.

Figure 1: PLASMA VM Environments

Several of the modules will utilize open source Android analysis tools such as Androidguard [1], Droid-FF [8], Androidhooker [2], PatDroid, [16] and PScout [18]. All of these tools will be pre-loaded on the provided VM. Individual Android modules will still be available for download on an individual basis if the user wishes to download a single activity and not the entire virtual machine environment. Unfortunately, due to platform limitations, we will be unable to include iOS modules on this VM, but they will be available for individual download. We do not feel this to be overly problematic since instructors teaching iOS will already have the proper development environment in place, thus limiting any negative impact of the modules not being on the virtual machine environment.

4.4 Module Development

Senior Person Mirakhorli and Consultant Richards will perform the initial step of identifying vulnerabilities that we would like to address in our modules. We will simultaneously select several students to begin working on the creation of the modules and will hire students from underrepresented groups whenever possible. Once the modules are created, they will be released in the following order and refined based on provided feedback from the following groups:

1. Small student focus groups: As part of the formative process, feedback regarding module quality and learning outcomes will be used to make necessary modifications to the modules prior to the general release to RIT and Park.
2. In class exercises at RIT and Park: Modules will be used as part of classroom exercises at both Park and RIT. These will provide feedback on the modules and lessons learned for using the modules in a classroom setting. We will evaluate preliminary learning outcomes through pre and post tests.
3. Partner schools: Feedback regarding the usefulness, instruction quality, and best practices emerging from the lessons learned at RIT and Park will be used to advise the partner schools as how they may best present the modules. The program goals of improving access of mobile security instruction to underrepresented groups, and improving instructor access to high quality mobile software security instruction will be evaluated through attendance and interview data obtained from the instructors.
4. Local outreach activities: The program's goals of improving access of mobile security instruction to underrepresented groups and improving student interest in software security for mobile devices will

be evaluated through surveys and website tracking data. Lessons learned from conducting outreach events will also be recorded.

5. Public deployment: Advertise modules for use at non-partner institutions and settings. Surveys will be used to evaluate the effectiveness of the modules for meeting their objectives.

4.5 Web Design and Hosting:

Necessary hardware support will be administered by the IT department that supports the PhD program at RIT [2]. Although managed by PI Krutz, the project website will be expanded upon by qualified RIT students. The primary web components to be developed and supported will include:

1. Information about each module.
2. Public forum which would allow students to comment and ask questions about each exercise in a open setting. Existing software will be used for this component, but will need to be integrated with the rest of the website.
3. Download and support links for VM and all other project artifacts.

We anticipate our modules will be used in a wide range of courses, by students with varying experience levels, so we want to make the module selection process as easy as possible for instructors. To assist instructors with this selection process, the website will allow them to select the desired platform and difficulty level of their modules. All modules meeting this criteria will then filtered and shown for available download. All selected modules with be added to a single, custom zip file which instructors may then download. An overview of the creation process is shown in Figure 2. Using this process, instructors will be assisted in getting the more relevant modules for their specific situation by choose the platform, difficulty level, and desired modules.

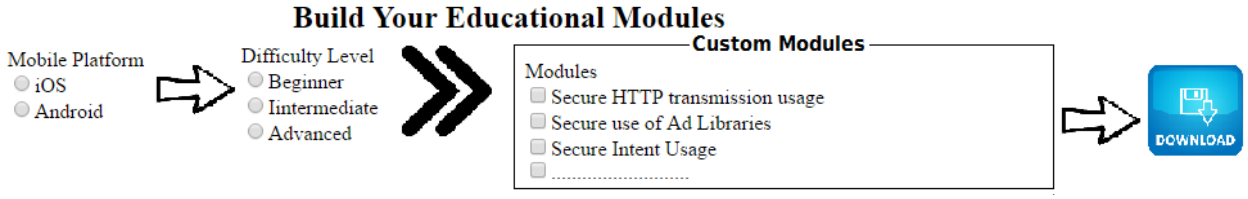


Figure 2: Custom Education Module Categorization

4.6 Initial Feedback

At several outreach events, our existing activities have already demonstrated their value and have provided invaluable lessons learned. To provide initial measurements on the effectiveness of the initial activities, we asked participants to complete a brief survey before and after completing a sample activity at each event. At an outreach event for approximately 15 Women in Computing students from RIT, survey results indicate that students felt that creating secure software was easier after participating in the activity than they felt prior to conducting the activity. This initial feedback indicates that increased familiarity with mobile security may make students feel like creating secure software is more achievable. However, the sample size for these results is very small and deserves further exploration. In an outreach event for local High School students with largely no computing background, their feedback demonstrates that they are much more interested in software security than they were prior to attending the outreach event. At both events, students expressed

[2] https://www.rit.edu/gccis/academics/phd-program

very positive feedback in terms of enjoying using the activities, feeling like the modules resembled relevant real-world situations and that they would recommend them to a friend.

We learned valuable lessons from these initial activities including ensuring that all participants properly have Android Studio installed on their devices, and the benefits of visual aides during the demo. Using PLASMA's VM environment, the issue of participants having an improper Android studio setup will be eliminated since this will be pre-installed on the provided VM.

5 Deployment Plan

Our modules will be deployed in several stages: proof-of-concept implementation, local deployment, workshop and tutorial advertising, and multiple-site deployment. During the proof-of-concept phase, all modules and related materials will be tested by a small group of students from both Park University and RIT. This initial proof-of-concept evaluation will provide information about adjustments which will need to be made to each module. This early feedback will help us to answer the following questions about our created modules:

1. What modules do students enjoy the most and why?
2. What further supporting materials could we provide to enhance student interest and recollection?
3. What structural or design issues exist in the modules?
4. Are the modules too complicated, or too simple?
5. What is the average amount of time required to complete the activities?
6. Are the learning and educational objectives being properly met?

The next phase will be to use the modules in local outreach activities. Some of which include outreach events at local libraries, and coordinated activities with student groups such as RIT's Women in Computing, or Park University's American Association of University women. This will allow us to not only share these modules with these groups, but importantly provide a way of observing students and instructors using our modules and provide feedback which can be used to make adjustments to the modules.

The modules will also be used in courses at several institutions who have already expressed interest in incorporating them into their curriculum. Some of these schools include California State University Chico: Intro To Computer Security (CINS 448) and Advanced Computer Security (CINS 548); RIT: Engineering of Secure Software (SWEN 331); Curry College: Information Technology Security (IT 2215) and Mobile Applications Security (MAPP 3800). Park University will use many of the modules in their cybersecurity courses which are currently under development, some of which include CS 330 Principles of Mobile Development and CS 314 User Interface Design (Secure interfaces). North Carolina A&T will use the modules in Application Development for Android Devices (ECEN 485/685).

After our modules have been refined, we will next "advertise" them to the public. This will be done at various conferences in tutorials and workshops. Based on our existing activities, we have already been invited to speak at Syracuse University's SEED security workshops [20, 31] and NYC WIC [13] in the Spring of 2017. We will also submit our findings in educational publications such as SIGCSE, ITiCSE, CISSE, and ASEE. Based on our existing activities, we have already had an ACM InRoads submission published [37].

Over the course of the proposal, we would like to hold at least public outreach activities in both the Rochester and Kansas City areas. We will hold outreach activities at free venues such as public libraries, so the only costs we anticipate in holding these events is paying the student workers. Our PIs have experience running similar outreach activities.

The modules will be licensed under the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; and permission is granted to copy, distribute and/or modify PLASMA modules under the terms of the license.

6 Evaluation Plan

PLASMA is designed to generate stronger interest in mobile security and provide modules to support institutions with limited resources. Our evaluation will be conducted to identify areas which can improve the overall quality of the project. The results of the evaluation will considered in terms of the specific program goals and intentions for which NSF grants are given. The purpose of the evaluation is to determine the degree to which PLASMA meets its program goals and funding intentions.

Analysis of the program goals will involve quantitative and qualitative processes including statistical significance measurement and theme development. Data collected through pre and post tests, focus groups, surveys, and interviews will be used as means for both formative and summative evaluation. The stakeholders for this project will include student participants, instructors, partner universities, and the National Science Foundation. Our goals are to determine if the activities properly support our educational and program objectives, and to determine what changes may be necessary to meet project goals.

The evaluation will be conducted by under the direction of PI Dean who has 15 years educating computing students in the undergraduate setting and PI Krutz who has over 6 years experience in this area. Senior Person Sparkman has over 5 years educating human resource development students at the master's and undergraduate levels. The project goals are presented in Table 2.

7 Management

PI Krutz and PI Dean will lead the team of academic faculty and a consultant from industry. A primary goal of forming this team was to combine experiences of a security researcher, computing educators, and industrial knowledge to create a robust set of modules. PI Krutz has worked on this project since its inception more than a year ago and has overseen its design and creation of initial activities. PI Dean will work with Senior Person Mirakhorli to form a partnership between Park University, and The Center for Cybersecurity at RIT. The partnership will involve sharing classroom activities, lessons learned, and general advice and guidance for Park's creation of security related curriculum. Consultant Richards will provide guidance on the modules to be created, as well as supervising the overall quality assurance of the activities.

PI Krutz and Senior Person Mirakhorli have previously collaborated on several research projects and grant proposals. Consultant Richards has been providing guidance to RIT's 'Engineering of Secure Software' course for several years, and has been an adviser providing guidance to PI Krutz on classroom materials and activities. PI Krutz and PI Dean have known each other for nearly ten years and frequently discuss classroom activities and pedagogical strategies.

Senior Person Sparkman will be responsible for the formative and summative evaluation of the research project. He will assess progress toward, and completion of program goals, and learning objectives. He will assess progress and goals through the collection and analysis of evaluation data. He will also monitor workshop quality, and the activities associated with the broader impact activities. An overview of the project roles is shown in Table 3.

7.1 Project Timeline of Activities:

To create robust modules which can be used as soon as possible, we will create our activities in groups of five. This will also allow us to not only share these activities as soon as possible, but to gather feedback on them as well. Our goal is to create ten modules in every 6 month block. An overview of our timeline is shown in Table 4.

Table 2: Program Goals

Program Goal	Data source	Indicators	Data analysis
1. Improve student retention in security (RIT, Park, Partner Universities)	• University program retention statistics • Post completion Interviews with participants	40% of the participants will enroll in security courses or pursue more security education after the program.	Quantitative and Qualitative Analysis
2. Improve student knowledge of mobile security practices	• Pre & post questionnaire, Quizzes and Focus group interview	75% of the instructors will acknowledge continued usage of the modules.	Quantitative and Qualitative Analysis
3. Improve instructor access to high quality mobile software security instruction	• Interviews with software engineering instructors	75% of the instructors will acknowledge continued usage of the modules.	Qualitative analysis
4. Improve access to mobile security instruction to underrepresented groups	• Attendance data • Instructor surveys	At least 25% of the partner schools will be EPSCOR, HBCUs, HSIs and public outreach venues	Qualitative analysis
5. Improve participant interest in software security for mobile devices	• Pre & post questionnaire • Track module usage through website	75% of the participants will rate their increase in interest from moderate to high.	Quantitative analysis

8 Course Development

Park University is currently adding several security related courses to their curriculum. This year, they plan to hire a new tenure track assistant professor with a focus on cybersecurity. Their Computer Science and Information Systems (CSIS) Department has proposed several new courses including: Principles of Mobile Development II and Mobile Computing Senior Project, CS 330 Principles of Mobile Development and CS 314 User Interface Design (Secure interfaces). Park is also creating a new cybersecurity specialty area for its Information and Computer Science (ICS) program.

In addition to assisting Park University's creation of these imperative security courses, their participation in the proposal will serve to provide feedback on the created modules and materials. Once they have added the modules to their curriculum, they will also share their experiences with other institutions through tutorials and workshops at conferences, and through publications.

Table 3: Project Roles

Investigator	Institution	Background	Project Role
Daniel E. Krutz	RIT, SE	Mobile Security, Computing Education	PI, Module creation and data collection. Project management.
John Dean	Park, CS	Computing Education	Co-PI. Curriculum development, data collection and project management.
Mehdi Mirakhorli	RIT, SE	Cybersecurity and Software Engineering Research	Sr. Personnel, Assess pilot study of educational material; Provide guidance on design and artifact distribution
Torrence E. Sparkman	RIT, CAST-DSS	Development, Evaluation & Instructional Design	Sr. Personnel, formative & summative evaluation
Thomas Richards	Cigital	Senior Security Consultant	Consultant, Provide guidance and evaluate created materials

9 Results from Prior NSF Support

PI Krutz has had no prior NSF support.

PI Dean has had no prior NSF support.

Senior Person Mirakhorli was recently awarded an NSF grant CCF-1543176, for $80,000 (2015-2016), for "Bringing Design Thinking into Developers' Coding Activities through an Architectural Tactic Recommender System". He has also served as senior personnel on a grant to develop tracing techniques related to software architecture (SHF.1218303, Small: Tactic-Centric Traceability Models for Preserving Architectural Quality).

Intellectual Merit: of the proposed project lies in its paradigm shift for integrating architecture design thinking into developers' daily coding activities, as well as the novel approach for recommending tactics and reusing tactics' implementation from open-source software systems. PI Mirakhorli pioneered development of automated architecture analysis techniques [39, 46] that can help developers better implement architectural tactics and prevent degradation of architectural qualities [41, 36, 53, 40, 43, 42, 39]. The ongoing project has produced several research papers, currently a journal paper is under major revision at Empirical Software Engineering (EMSE) journal and a second journal paper is under major revision at Journal of Systems and Software (JSS). Furthermore, this work has resulted several intermediate tools [47, 34, 43].

Broader Impacts: The work on Architecture Profilers has transitioned to industry and is now used by SonaType Co. The grant led to significant career development of PI Mirakhorli. He is currently a PI on a grant from US Department of Homeland Security that has augmented this funding ($98K) to apply early results to software security domain.

Senior Person Sparkman has had no prior NSF support.

Table 4: Project Timeline of Activities

Year	Semester	Activity
1	Fall	· Identify target modules · Recruit students to create modules · Create 10 modules · Begin web development & VM configuration · Prepare courses at Park which will use modules
	Spring	· Begin outreach activities (RIT) and collecting data · Refine generated modules based on feedback · Identify and create 10 more modules · Submit 1st publication on initial results · Conduct 1st security course at Park using created modules. Collect data from course.
	Summer	· Attend conferences to disseminate initial results · Conduct remote tutorials · Refine generated modules based on feedback · Analyze assessment data · Create initial publications
2	Fall	· Identify and create 10 more modules · Begin outreach programs at remote institutions and continue them at RIT · Continue security courses at Park · Refine generated modules based on feedback · Begin creating publications to share experiences · Analyze data collected from Park. Create data collection/improvement Plan.
	Spring	· Conduct outreach activities and collect data · Continue security courses at Park · Refine generated modules based on feedback · Identify and create final modules
	Summer	· Complete NSF Report · Attend conferences to disseminate results · Conduct remote tutorials · Concluding dissemination activities

References

[1] Androguard. https://github.com/androguard/androguard.

[2] Android hooker. https://github.com/AndroidHooker/hooker.

[3] Android secure coding standard. https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=111509

[4] Checkstyle. http://checkstyle.sourceforge.net/.

[5] Cloudpassage study finds u.s. universities failing in cybersecurity education. https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

[6] Collaborative project: Capacity building in mobile security through curriculum and faculty development award 1241670. https://www.nsf.gov/awardsearch/showAward?AWD_ID=1241670.

[7] Designing secure user interfaces. https://developer.apple.com/library/content/documentation/Security/Conceptual/Secu

[8] Droid-ff. https://github.com/antojoseph/droid-ff.

[9] Dyci dynamic code injection. https://github.com/DyCI/dyci-main.

[10] Exploitme mobile android labs. http://securitycompass.github.io/AndroidLabs/setup.html.

[11] Findbugs - find bugs in java programs. http://findbugs.sourceforge.net/.

[12] M-perm: Android permissions analysis tool. http://www.m-perm.com.

[13] Nycwic 2017. http://nycwic.hosting.acm.org/.

[14] Owasp mobile application security verification standard (masvs). https://github.com/OWASP/owasp-masvs.

[15] Owasp mobile security project. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

[16] Patdroid. https://github.com/mingyuan-xia/PATDroid.

[17] Peek. https://github.com/shaps80/Peek.

[18] Pscout. http://pscout.csl.toronto.edu/.

[19] Sac 2017 tutorials. http://www.sigapp.org/sac/sac2017/tutorials.html.

[20] Seed labs. http://www.cis.syr.edu/ wedu/seed/workshop.html.

[21] Teaching mobile security. http://teachingmobilesecurity.com/.

[22] Tutorial: Build an android application with secure user authentication. https://stormpath.com/blog/build-user-authentication-for-android-app.

[23] Vector attack scanner. https://github.com/JhetoX/VectorAttackScanner.

[24] Virtualbox. https://www.virtualbox.org/.

[25] Wireshark. https://www.wireshark.org.

[26] Xcode ide. https://developer.apple.com/xcode/features/.

[27] Y. Bai and X. Wang. Itseed: Hands-on labs for it security education (abstract only). In *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*, SIGCSE '14, pages 739–739, New York, NY, USA, 2014. ACM.

[28] C. C. Bonwell and J. A. Eison. *Active Learning: Creating Excitement in the Classroom. 1991 ASHE-ERIC Higher Education Reports.* ERIC, 1991.

[29] H. Chi and D. A. Rubio. Design insider threat hands-on labs. In *Proceedings of the 2014 Information Security Curriculum Development Conference*, InfoSec '14, pages 17:1–17:1, New York, NY, USA, 2014. ACM.

[30] A. Conklin. Cyber defense competitions and information security education: An active learning solution for a capstone course. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, volume 9, pages 220b–220b. IEEE, 2006.

[31] W. Du and R. Wang. Seed: A suite of instructional laboratories for computer security education. *Journal on Educational Resources in Computing (JERIC)*, 8(1):3, 2008.

[32] S. Freeman, S. Eddy, M. McDonough, M. Smith, N. Okoroafor, H. Jordt, and M. Wenderoth. Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences of the United States of America*, 111(5):8410–5, 2014-06-10 00:00:00.0.

[33] X. Gao, D. Liu, H. Wang, and K. Sun. Pmdroid: Permission supervision for android advertising. In *Reliable Distributed Systems (SRDS), 2015 IEEE 34th Symposium on*, pages 120–129, Sept 2015.

[34] D. Gonzalez, A. Popovich, and M. Mirakhorli. *TestEX: A Search Tool for Finding and Retrieving Example Unit Tests from Open Source Projects*. `http://design.se.rit.edu/papers/TestEX.pdf`, 2016.

[35] M. Guo, P. Bhattacharya, M. Yang, K. Qian, and L. Yang. Learning mobile security with android security labware. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education*, SIGCSE '13, pages 675–680, New York, NY, USA, 2013. ACM.

[36] E. Kouroshfar, M. Mirakhorli, H. Bagheri, L. Xiao, S. Malek, and Y. Cai. A study on the role of software architecture in the evolution and quality of software. In *2015 IEEE/ACM 12th Working Conference on Mining Software Repositories*, pages 246–257, May 2015.

[37] D. E. Krutz and S. A. Malachowsky. Teaching android security through examples: A publicly available database of vulnerable apps. *ACM Inroads*, 7(4):96–98, Nov. 2016.

[38] L. Li, K. Qian, Q. Chen, R. Hasan, and G. Shao. Developing hands-on labware for emerging database security. In *Proceedings of the 17th Annual Conference on Information Technology Education*, SIGITE '16, pages 60–64, New York, NY, USA, 2016. ACM.

[39] J. C.-H. Mehdi Mirakhorli. Detecting, tracing, and monitoring architectural tactics in code. *IEEE Trans. Software Eng.*, 2015.

[40] M. Mirakhorli and J. Cleland-Huang. Modifications, tweaks, and bug fixes in architectural tactics. In *Proceedings of the 12th Working Conference on Mining Software Repositories*, MSR '15, pages 377–380, Piscataway, NJ, USA, 2015. IEEE Press.

[41] M. Mirakhorli, P. Mäder, and J. Cleland-Huang. Variability points and design pattern usage in architectural tactics. In *Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering*, FSE '12, pages 52:1–52:11, New York, NY, USA, 2012. ACM.

[42] M. Mirakhorli, Y. Shin, J. Cleland-Huang, and M. Cinar. A tactic centric approach for automating traceability of quality concerns. In *International Conference on Software Engineering, ICSE (1)*, 2012.

[43] I. Mujhid, J. C. S. Santos, R. Gopalakrishnan, and M. Mirakhorli. *A Search Engine for Finding and Reusing Architecturally Significant Code.* Under Major Revison for Journal Publication and a Technical Report at Rochester Institute of Technology, `http://design.se.rit.edu/papers/JSS2016.pdf`, 2016.

[44] J. Patt. No clear path for prospective cybersecurity specialists. http://theinstitute.ieee.org/career-and-education/career-guidance/no-clear-path-for-prospective-cybersecurity-specialists.

[45] M. Rozenfeld. Most top computer science programs skip cybersecurity. http://theinstitute.ieee.org/career-and-education/education/most-top-computer-science-programs-skip-cybersecurity.

[46] J. Santos, I. Mujhid, and M. Mirakhorli. *Facilitating Architecture-Centric Threat Modeling*. Under Major Revison for Journal Publication and Technical Report at Rochester Institute of Technology, `http://design.se.rit.edu/papers/IEEESec.pdf`, 2016.

[47] J. C. S. Santos, M. Mirakhorli, I. Mujhid, and W. Zogaan. *BUDGET: a Tool for Supporting Software Architecture Traceability Research*. 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), Tool Demonstration, 2016.

[48] D. Schweitzer, D. Gibson, and M. Collins. Active learning in the security classroom. In *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*, pages 1–8, Jan 2009.

[49] A. Setalvad. Demand to fill cybersecurity jobs booming. http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.

[50] X. Wang, Y. Bai, and G. C. Hembroff. Hands-on exercises for it security education. In *Proceedings of the 16th Annual Conference on Information Technology Education*, SIGITE '15, pages 161–166, New York, NY, USA, 2015. ACM.

[51] K. A. Williams, X. Yuan, H. Yu, and K. Bryant. Teaching secure coding for beginning programmers. *J. Comput. Sci. Coll.*, 29(5):91–99, May 2014.

[52] M. Xia, L. Gong, Y. Lyu, Z. Qi, and X. Liu. Effective real-time android application auditing. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, SP '15. IEEE Computer Society, 2015.

[53] W. Zogaan, J. Santos, I. Mujhid, D. Gonzalez, and M. Mirakhorli. *Automated Training-Set Creation for Software Architecture Traceability Problem.* Under Major Revison for Journal Publication and Technical Report at Rochester Institute of Technology, `http://design.se.rit.edu/papers/EMSE2016.pdf`, 2016.

Daniel E. Krutz
Software Engineering Department
Phone: (585) 475 2896
dxkvse@rit.edu
http://www.se.rit.edu/~dkrutz/

(a) Professional Preparation

St. John Fisher College Rochester, NY	Computer Science, History	BS, 2004
RIT Rochester, NY	Software Design and Management	MS, 2007
Nova Southeastern University Ft. Lauderdale, FL	Computer Science	PhD, 2013

(b) Appointments

9/10-present	**Lecturer,** Software Engineering Department, RIT
8/09-8/10	**Technology Consultant,** Mindex Technologies
2/09-8/09	**Sr. Software Engineer,** 5Linx Enterprises
5/04-1/09	**R&D Software Developer,** Xerox Corporation

(c) Products

Related to project

1. **Krutz, Daniel** & Malachowsky, Samuel 2016 "Teaching Android Security Through Examples: A Publicly Available Database of Vulnerable Apps" - ACM InRoads
2. Munaiah, Nuthan; Klimkowsky, Casey; Trudeau, Shannon; Blaine, Adam; Malachowsky, Samuel; Perez, Cesar and **Krutz, Daniel**. 2016 "Darwin: A Static Analysis Dataset of Malicious and Benign Android Apps" - International Workshop on App Market Analytics (WAMA 2016)
3. **Daniel Krutz**, Nuthan Munaiah, Andrew Meneely and Samuel Malachowsky 2016. "Examining the Relationship between Security Metrics and User Ratings of Mobile Apps: A Case Study" - International Workshop on App Market Analytics (WAMA 2016)
4. **Krutz, Daniel**; Mirakhorli, Mehdi; Malachowsky, Samuel; Ruiz, Andres; Peterson, Jacob & Filipski, Andrew. 2015 "A Dataset of Open-Source Android Applications" (MSR)
5. **Krutz, Daniel**; Meneely, Andrew & Malachowsky, Sam 2015 "An Insider Threat Activity in a Software Security Course"', Frontiers in Education Conference (FIE)

Others of significance

6. **Krutz, Daniel** & Mirakhorli, Mehdi. 2016 "Architectural Clones: Toward Tactical Code Reuse" ACM Symposium on Applied Computing (SAC)
7. **Krutz, Daniel**; Kaplan, Jayme; Jones, Scott & Malachowsky, Sam. 2015 "Enhancing the Educational Experience for Deaf and Hard of Hearing Students in Software Engineering", Frontiers in Education Conference (FIE)

8. **Krutz, Daniel**; Malachowsky, Samuel & Shihab, Emad. 2015 "Examining the Effectiveness of Using Concolic Analysis to Detect Code Clones" ACM Symposium on Applied Computing (SAC)
9. **Krutz, Daniel** & Le, Wei. 2014 "A Code Clone Oracle" Mining Software Repositories (MSR)
10. **Krutz, Daniel** & Shihab, Emad. 2013 "CCCD: Concolic Code Clone Detection", Working Conference on Reverse Engineering (WCRE)

(d) Synergistic Activities

1. Conducted multiple outreach events for underrepresented college and High School students.
2. Created initial set of educational Android modules, which have been used at several outreach events.
3. Recent development efforts include teaching undergraduate courses in defensive coding practices
4. Member of the Software Engineering department's undergraduate curriculum committee (2011-2015) and graduate curriculum committee (2015-Present).

John Dean
Chair, Department of Computer Science and Information Systems
Park University
Phone: 816-584-6422
john.dean@park.edu

(a) Professional Preparation

University of Kansas Lawrence, KS	Electrical Engineering	B.S., 1985
University of Kansas Lawrence, KS	Computer Science	M.S. 1988
Nova Southeastern University Davie, FL	Computer Science	Ph.D. 2013

(b) Appointments

7/01-present **Department Chair, Computer Science and Information Systems Department,** Park University

(c) Products

Others of signficance

1. Dean, J. & Dean, R. 2014. Introduction to Programming with Java – A Problem Solving Approach, 2nd ed. New York: McGraw-Hill. http://www.mhhe.com/dean2e.
2. Dean, J. & Dean, R. 2008. Introduction to Programming with Java – A Problem Solving Approach. New York: McGraw-Hill. http://www.mhhe.com/dean.
3. Dean, J., Mitropoulos, F. 2014. An Aspect Pointcut for Parallelizable Loops. Proceedings of the 29th ACM Symposium on Applied Computing. Pages 1619-1624, http://dl.acm.org/citation.cfm?id=2554850.2554917.
4. Dean, J. 2012. Electronic Voting with Scantegrity: Analysis & Exposing a Vulnerability. Electronic Government, an International Journal. Pages 27-45, http://www.inderscienceonline.com/doi/abs/10.1504/EG.2012.044777?journalCode=eg.
5. Dean, J. 2008. Staff Scheduling by a Genetic Algorithm with a Two-Dimensional Chromosome Structure. Proceedings of the 7th International Conference on the Practice and Theory of Automated Timetabling. Pages 18-22, http://patatconference.org/patat2008/proceedings/Dean-WA3c.pdf.

(d) Synergetic Activities

1. Grant for an Aspirations in Computing awards ceremony for achievements in computing by high school girls in Missouri and Kansas. National Center for Women and Information Technology. $2,000. 2012-2013 academic year.
2. Grant for "Advanced Combat Simulation for More Effective Anti-Terrorist Operations." United States Department of Defense. $30,000. 2007-2008 academic year.

BIOGRAPHICAL SKETCH

Mehdi Mirakhorli

(a) Professional Preparation

Teacher Training University (TMU)	Computer Science	BS	2002-2005
National University of Iran (SBU)	Computer Science	MS	2006-2008
DePaul University	Computer Science	PhD	2009-2014

(b) Appointments

Assistant Professor	Rochester Institute of Technology	2014-Present
Researcher	U.S. Department of Homeland Security (DHS)	2013-2014
Research Assistant	DePaul University	2009-2014
Software Architect	Multiple Software Companies	2005-2009

(c) Publications

Related

1. **Mehdi Mirakhorli**, Jane Cleleand Huang, Detecting, Tracing and Monitoring Architectural Tactics in Code, *IEEE Transactions on Software Engineering*, 2016.
2. Ehsan Kouroshfar, **Mehdi Mirakhorli**, Hamid Bagheri, Lu Xiao, Sam Malek, and Yuanfang Cai, "A Study on the Role of Software Architecture in the Evolution and Quality of Software", *The 12th Working* Conference on Mining Software Repositories (MSR), 2015.
3. Mehdi Mirakhorli, Hongmei Chen and Rick Kazman. "Mining Big Data for Detecting, Extracting and Recommending Architectural Design Concepts", 1st International Workshop on BIG Data Software Engineering, 2015.
4. *Mehdi Mirakhorli*, "Software Architecture Reconstruction: Why? What? How?", *IEEE 22nd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, 2015
5. **Mehdi Mirakhorli**, Yonghee Shin, Jane Cleland-Huang and Murat Cinar, "A Tactic-Centric Approach for Automating Traceability of Quality Concerns", *34th International Conference on Software Engineering (ICSE)*, 2012 , pp.639-649, **ACM SIGSOFT Distinguished Paper Award**.

Other

6. Negar Hariri, Carlos Castro-Herrera, **Mehdi Mirakhorli**, Jane Cleland-Huang, Bamshad Mobasher, "Supporting Domain Analysis through Mining and Recommending Features from Online Product Listings", *IEEE Transaction on Software Engineering (TSE)*, 2013, vol. 99, no. DOI: http://doi.ieeecomputersociety.org/10.1109/TSE.2013.39.
7. Mehran Mozafari Kermani, Reza Azarderakhsh, **Mehdi Mirakhorli**, "Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education", *ASEE Conferences: American Society for Engineering Education (ASEE)*, 2016.
8. Joanna C. S. Santos, **Mehdi Mirakhorli**, Ibrahim Mujhid, and Waleed Zogaan, "BUDGET: a Tool for Supporting Software Architecture Traceability Research", *13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, 2016.
9. Horatiu Dumitru, Marek Gibiec, Negar Hariri, Jane Cleland-Huang, Bamshad Mobasher, Carlos Castro-Herrera, **Mehdi Mirakhorli**, "On-demand feature recommendations derived from mining public product descriptions", *International Conference on Software Engineering (ICSE)* 2011, pp.181-190, (14% acceptance). **ACM SIGSOFT Distinguished Paper Award**
10. Tactic Profiler Tool released on US Department of Homeland Security, Software Assurance Marketplace (SWAMP) project. https://continuousassurance.org/

(d) Synergistic Activities

1. **Organizing Committee:** DataTrack Chair at RE'2017, Tool Demo Chair at FSE'2017, Workshops Chair at FSE'2016, Co- chair for the First International Workshop on Bringing Architecture Design Thinking into Developers' Daily Activities (Bridge'16), Technical Briefing on Bigger Data for Software Engineering, ICSE 2015; Focused Group on Mining New Patterns, Pattern Languages of Programs (PLoP), 2014; Program Chair, 4th International Workshop on Twin Peaks of Requirements and Architecture, IEEE International Conference on Software Engineering (ICSE), 2014., Organizer of TwinPeaks@RE13 and TwinPeaks@ICSE13, Program Chair at TwinPeaks@RE12, Student Volunteer Chair, 20th IEEE International Requirements Engineering Conference, September 24th-28th, 2012.

2. **Program Committee Services:** IEEE International Conference on Software Architectures (ICSA 2017), 23rd International Working Conference on Requirements Engineering: Foundation for Software Quality (REFSQ'2017), Software Engineering Education Track at the International Conference on Software Engineering (ICSE 2016), Tool Demo at ICSE 2016; Tool Demo at ASE'2016, Tool Demo at RE'2015, 22nd International Conference on Software Analysis, Evolution and Reengineering (SANER'2014), The 8th International Symposium on Software and Systems Traceability (SST 2015), Early Research Achievements (ERA) track of the 30th International Conference on Software Maintenance and Evolution (ICSME 2014), 7th International Workshop on Traceability in Emerging Forms of Software Engineering, Requirements Engineering for Systems, Services, and Systems of Systems (RES^4) at 19th IEEE International Requirements Engineering Conference (RE'10), 2010. Pattern Shepherd, Pattern Languages of Programs Conference (PLoP'13), 2013.

3. **Reviewing Services:** IEEE Transactions on Software Engineering (TSE), Information and Software Technology, Brazilian Journal of Universal Computer Science (J.UCS) Special Issue: Software Components, Architectures and Reuse, 2013.

4. **Associte Editor**: IEEE Software Blog on Software Architecture. **Guest Editor**, IEEE Special Issue on TwinPeaks of Requirements and Architecture.

5. **Industrial/Government Outreach:** ***ALTA Distinguished Speaker***, Alcatel-Lucent (2013), Software Engineering Institute (SEI) Architecture Technology User Network (SATURN), 2014.

Biographical Sketch

Torrence E. Sparkman Ph.D.

(a) Professional Preparation

University of Illinois	Chicago, IL.	Business Management	Bachelor of Science, 1993
Trinity Evangelical Divinity School	Deerfield, IL.	Urban Ministry	Master of Divinity, 2002
University of Illinois	Urbana-Champaign, IL.	Human Resource Education	Ph.D. 2012

(b) Appointments

8/2014-Present	Assistant Professor, Rochester Institute of Technology
8/2012-8/2014	Visiting Associate Professor & Program Outreach Coordinator, University of Houston
8/2011-8/2012	Visiting Assistant Professor & Program Outreach Coordinator
8/2010-1/2011	Adjunct Professor-Urbana Theological Seminary, Champaign, IL.
8/2004-1/2005	Adjunct Professor- School of Urban Missions, New Orleans, LA.

(c) Products

Sparkman, T.E., (2015). "The factors and conditions for National Human Resource Development in Brazil. European Journal of Training and Development, 39(8), 666-680.

(d) Synergistic Activities

- Currently working on (RIT) internally funded: "Identifying laboratory skills and social supports for 1st and 2nd year underrepresented science students." (2016-2017).
- Currently working on (RIT) internally funded: Using virtual technology to enhance learning in the Electrical Machines and Transformers course. (2016-2017).
- "Understanding and addressing executive leadership development needs" Guest Lecturer, Mandela –Washington Fellowship- For Young African Leaders, University of Illinois. 2016.
- Lead the development of the first University of Houston- HRD Career Symposium and Social, 2012.

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
Daniel Krutz

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. **Daniel Krutz - none**	0.00	0.00	2.00	**17,707**	
2. **John Dean - none**	0.00	0.00	0.00	**0**	
3. **Mehdi Mirakhorli**	0.00	0.00	0.75	**7,297**	
4. **Torrence Sparkman**	0.00	0.00	0.25	**2,376**	
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**4**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	3.00	**27,380**	
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. (**2**) GRADUATE STUDENTS				**5,280**	
4. (**6**) UNDERGRADUATE STUDENTS				**2,520**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**35,180**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,163**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**37,343**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**6,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**3,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**58,032**	
TOTAL OTHER DIRECT COSTS				**61,332**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**104,675**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Facilities and administrative (Rate: 46.5000, Base: 76513)**					
TOTAL INDIRECT COSTS (F&A)				**35,579**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**140,254**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**140,254**	

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

PI/PD NAME
Daniel Krutz

ORG. REP. NAME*
Laura Kleiman

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
Daniel Krutz

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. **Daniel Krutz - none**	0.00	0.00	2.00	**18,238**	
2. **John Dean - none**	0.00	0.00	0.00	**0**	
3. **Mehdi Mirakhorli**	0.00	0.00	0.25	**2,447**	
4. **Torrence Sparkman**	0.00	0.00	0.00	**7,516**	
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**4**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	2.25	**28,201**	
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. (**2**) GRADUATE STUDENTS				**5,280**	
4. (**6**) UNDERGRADUATE STUDENTS				**2,520**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**36,001**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,228**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**38,229**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**12,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**3,300**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**57,624**	
TOTAL OTHER DIRECT COSTS				**60,924**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**111,153**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Facilities and administrative (Rate: 46.5000, Base: 55149)**					
TOTAL INDIRECT COSTS (F&A)				**25,644**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**136,797**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**136,797**	

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

PI/PD NAME
Daniel Krutz

ORG. REP. NAME*
Laura Kleiman

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: **Daniel Krutz**

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. **Daniel Krutz - none**	0.00	0.00	4.00	**35,945**	
2. **John Dean - none**	0.00	0.00	0.00	**0**	
3. **Mehdi Mirakhorli**	0.00	0.00	1.00	**9,744**	
4. **Torrence Sparkman**	0.00	0.00	0.25	**9,892**	
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**4**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	5.25	**55,581**	
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. (**4**) GRADUATE STUDENTS				**10,560**	
4. (**12**) UNDERGRADUATE STUDENTS				**5,040**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**71,181**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**4,391**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**75,572**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**18,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**6,600**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**115,656**	
TOTAL OTHER DIRECT COSTS				**122,256**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**215,828**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**61,223**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**277,051**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**277,051**	

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

PI/PD NAME: **Daniel Krutz**

ORG. REP. NAME*: **Laura Kleiman**

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

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

Rochester Institute of Technology (RIT)
Budget Justification
Daniel E. Krutz
SaTC: EDU: PLASMA: Practical LAbs in Security for Mobile Applications

Salary amounts are based on actual salaries and include 3% anticipated annual merit increases for faculty and staff. RIT utilizes a 9.5-month contract for the Academic Year. The RIT Fiscal Year (FY) starts on July 1 and ends June 30 of the subsequent year.

Note: Educational institutions which receive federal funding are required by the United States Office of Management and Budget (OMB) "Uniform Administrative Requirements, Cost Principles and Audit Requirements for Federal Awards" (Uniform Guidance) to maintain an effort reporting system, the purpose of which is to assure that the distribution of pay is in accordance with actual effort expended (by funding source and activity). RIT's Monitored Workload System was established to meet this requirement by accumulating data that accounts for 100% of effort for Faculty/Staff. As a result, the effort reporting system does not allow RIT to estimate, monitor, or report labor by hours.

Senior Personnel:

Daniel E, Krutz, Lecturer, PI: salary support is requested for 2 month(s) summer salary for each of the 2 years. PI Krutz will be directly responsible for managing the creation of the modules and initial outreach activities, and the interactions between associated universities. PI Krutz will also be responsible for disseminating project findings and created modules.
Budget Request: Yr 1--$17,707, Yr 2--$18,238

Mehdi Mirakhorli, Assistant Professor, Senior Personnel: salary support is requested for 1 week summer salary for each of the 2 years. Senior Personnel Mirakhorli will act as a liaison between RIT's Center of Cybersecurity and Park's developing cybersecurity programs. He will also assist in proposing new modules and provide feedback on created modules. As someone with extensive sponsored research experience, he will also provide guidance on conducting our activities and disseminating our results.
Budget Request: Yr 1 --$2,376, Yr 2--$2,447

Torrence Sparkman, Assistant Professor, Senior Personnel: salary support is requested for 3 weeks summer salary for each of the 2 years. Senior Personnel Sparkman will be responsible for the formative and summative evaluation of the research project. He will assess progress toward, and completion of, program goals and learning objectives. He will assess progress and goals through the collection and analysis of evaluation data. He will also monitor workshop quality and the activities associated with the broader impact activities, such as the working relationships with supporting universities and other venues for research dissemination.
Budget Request: Yr 1 --$7,297, Yr 2--$7,516

Other Personnel:

Graduate Students: support is requested for two (2) Graduate students to assist with the development of the modules, and other project related materials. All efforts will be made to hire students from underrepresent groups. These students may also be asked to support other institutions who are adopting our modules.

Budget Request: Yr 1--$5,280, Yr 2--$5,280

Undergraduate Students:
Support is requested for a total of six (6) undergraduate students:

- Three (3) students to assist with setting up and running outreach activities. The budget includes funding for training and conducting the activities. At the conclusion of each event, students will also record lessons learned and other information which may be used to improve usage of the created modules at outreach events.
- Three (3) Women in Computing (WIC) students to assist with setting up and running outreach activities. They will conduct 5 outreach events a year, with 3 students working at each event. At the conclusion of each event, students will also record lessons learned and other information which may be used to improve usage of the created modules at outreach events.

Budget Request: Yr 1--$5,040, Yr 2--$5,040

Benefits:
Benefit rates for faculty and staff during the academic or calendar year are calculated at the approved federal rate at the provisional federal rate of 28.7% (FY 2017 and beyond). Benefits for faculty summer effort are calculated at the provisional federal rate of 7.9% (FY 2017 and beyond). Benefits are not assessed on student stipends or wages. Actual rates will be used once known.
Budget Request: Yr 1--$2,163, Yr 2--$2,228

Travel:
Support is requested for project personnel and students to travel to national conferences to both present our findings, and promote our modules in tutorials. Each conference trip is estimated at $2,000 per person. Some possible conferences include SIGCSE, FIE, ICSE-SEET, CISSE, SIGITE and ASEE. When conducting tutorials, two members will attend the conference while one person. We may also use some of the allocated travel allotment to fund a graduate student to assist with a tutorial or present our findings. We plan on presenting our findings at 3 venues, and conducting 6 tutorials. Conducting tutorials at conferences is imperative for helping to advertise our modules and providing guidance on how they should be used in classrooms and outreach events. Similar proposals (such as the Syracuse SEED Project) have brought instructors to their University to teach them how to use their labs. Traveling to venues to help other instructors will keep costs down.
Budget Request: Yr 1--$6,000, Yr 2--$12,000

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.

Other Direct Costs:

- Subaward: The proposed project will assist Park University in its development of Cybersecurity and mobile curriculum, something which is desperately needed by this EPSCoR institution. Park University has committed to heavily using our modules in their curriculum, thus providing important early feedback on their use in Cybersecurity and

mobile courses. This feedback will be useful in providing guidance on necessary adjustments to the modules and to evaluate their educational effectiveness.
Budget Request: Yr 1--$53,162, Yr 2--$56,004

- Purchased service: A primary objective of our proposed modules are to help institutions and groups in mobile security education, especially those which typically serve underrepresented students. Our proposal includes support for outreach events for both Women in Computing (WiC) at RIT and North Carolina A&T, an HBCU institution. In addition to supporting these two groups, these outreach events will provide valuable feedback on both the modules, and in their impact on defined educational objectives.
Budget Request: Yr 1--$1,620, Yr 2--$1,620

- Although our base Virtual Machine will be provided by the Syracuse SEED project, it will need to be slightly modified to accommodate our modules. Our website will need to be enhanced and maintained to accommodate new modules and materials. The website will also contain a public forum which will allow students to discuss modules, and a mechanism to allow instructors to build custom module sets. All development work will be conducted by students at RIT. Based on the advice of our IT department, in order to keep costs low the project website will hosted using an external provider. The anticipated costs of a domain name and hosting for seven years is $250. The rest of the requested money will be used to pay Graduate students for VM and website development work.
Budget Request: Yr 1--$3,250, Yr 2—N/A

- Consultant: Thomas Richards, Senior Security Consultant Cigital. As someone who is active in cybersecurity in industry, Richards will be responsible for providing guidance on module creation, and will review all created modules for accuracy.
Budget Request: Yr 1--$3,300, Yr 2--$3,300

F&A/Indirect Costs:

RIT has a federally negotiated F&A rate of 46.5% applied to all modified total direct costs. Modified total direct costs are total direct costs less capital equipment (value of >$1,500 and a useful life of >1 year), participant support costs, tuition remission and the amount in excess of the first $25,000 of each subaward.

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
Budget Request: Yr 1--$76,513, Yr 2--$55,149

SUMMARY PROPOSAL BUDGET

YEAR 1

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

ORGANIZATION
Park University

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
John Dean

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. **John Dean**	0.75	0.00	0.00	**4,800**	
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	0.75	0.00	0.00	**4,800**	
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. (**1**) GRADUATE STUDENTS				**1,500**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**2**) OTHER				**20,320**	
TOTAL SALARIES AND WAGES (A + B)				**26,620**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**8,792**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**35,412**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**2,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**0**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**37,412**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Facilities and administrative (Rate: 42.1000, Base: 37412)**					
TOTAL INDIRECT COSTS (F&A)				**15,750**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**53,162**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**53,162**	

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

PI/PD NAME
John Dean

ORG. REP. NAME*
Laura Kleiman

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
Park University

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
John Dean

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. **John Dean**	0.75	0.00	0.00	**4,800**	
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	0.75	0.00	0.00	**4,800**	
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. (**1**) GRADUATE STUDENTS				**1,500**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**2**) OTHER				**20,320**	
TOTAL SALARIES AND WAGES (A + B)				**26,620**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**8,792**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**35,412**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**4,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**0**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**39,412**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Facilities and administrative (Rate: 42.1000, Base: 39412)**					
TOTAL INDIRECT COSTS (F&A)				**16,592**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**56,004**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**56,004**	

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

PI/PD NAME
John Dean

ORG. REP. NAME*
Laura Kleiman

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: **Park University**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **John Dean**

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. **John Dean**	1.50	0.00	0.00	**9,600**	
2.					
3.					
4.					
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	1.50	0.00	0.00	**9,600**	
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. (**2**) GRADUATE STUDENTS				**3,000**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**4**) OTHER				**40,640**	
TOTAL SALARIES AND WAGES (A + B)				**53,240**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**17,584**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**70,824**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. U.S. POSSESSIONS)				**6,000**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**0**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**76,824**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**32,342**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**109,166**	
K. SMALL BUSINESS FEE				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				**109,166**	

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

PI/PD NAME: **John Dean**

ORG. REP. NAME*: **Laura Kleiman**

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

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

BUDGET JUSTIFICATION
Park University

PERSONNEL

A. SENIOR/KEY PERSONNEL

Dr. John Dean, Associate Professor, PI
Year 1: $4,800 ($40 per hour/3 weeks)
Year 2: $4,800 ($40 per hour/3 weeks)
(Based on $83,000 12 month salary at 40 hours per week)

Co-PI Dean will be responsible for managing curriculum development at Park, interactions between Park University and RIT, and collecting educational assessment information for Senior Personnel Sparkman.

Course Developer – Cyber Security, Faculty member to be hired, Senior Personnel
Year 1: $15,200 ($38 per hour/10 weeks)
Year 2: $15,200 ($38 per hour/10 weeks)
(Based on $60,000 9 month salary at 40 hours per week)

Course Developer – Mobile Computing, Faculty member to be hired, Senior Personnel
Year 1: $5,120 ($32 per hour/4 weeks)
Year 2: $5,120 ($32 per hour/4 weeks)
(Based on $50,000 9 month salary at 40 hour per week)

These faculty members will design, create, and evaluate a yet to be developed cybersecurity curriculum at Park University. Although Park University wishes to create a cybersecurity program, they currently lack the resources to do so.

Total Salary for Senior/Key Personnel Charged to the Grant: $50,240

Fringe Benefits for Senior/Key Personnel

Park University calculates fringe benefits based on an institutional rate of 35%. Those benefits include: Social Security, Medicare, health insurance, dental insurance, life insurance, accidental death and dismemberment, tuition reimbursement, retirement, and Unemployment Insurance.

$X Total Salaries * 0.35

Total Fringe Benefits for Senior/Key Personnel Charged to the Gran: **$17,584**

TOTAL SENIOR/KEY PERSONNEL COSTS $67,824

B. OTHER PERSONNEL

Teaching Assistant
$3,000 ($12 per hour/50 weeks)

The Teaching Assistants will help new instructors set up, and run the new security courses at Park University. These TAs will assist with grading, help set up and create activities, and collect necessary assessment data.

Fringe Benefits for Other Personnel
Total Fringe Benefits for Other Personnel Charged to the Grant: N/A

TOTAL OTHER PERSONNEL COSTS $3,000

TRAVEL

Domestic Travel Costs:

Conference Attendance and Travel
Project Director
1 Conference: Air Fare, Lodging and Meals ($51 per day): $2,000
Course Developer – Cyber Security
2 Conferences: Air Fare, Lodging and Meals ($51 per day): $4,000

Traveling to conferences will help Park to share observations from creating a cybersecurity program, and will allow them to attend presentations and interact with institutions that already have these programs in place. Some example conferences include ICSE, SIGCSE, ITiCSE, CISSE, SIGITE, and ASEE

TOTAL TRAVEL COSTS…….... $6,000

DIRECT COSTS

(Senior/Key Personnel + Other Personnel + Equipment + Travel + Other Direct Costs)

TOTAL DIRECT COSTS $76,824

INDIRECT COSTS

Indirect Costs are calculated at a rate of 42.1% of Modified Total Direct Costs
$X Modified Direct Cost * .421
TOTAL INDIRECT COSTS $32,343

TOTAL DIRECT AND INDIRECT COSTS

TOTAL DIRECT AND INDIRECT COSTS $109,166

Current and Pending Support

Daniel Krutz

Support: Current
Title: Supporting Education Using a Public Oracle of Vulnerable Mobile Apps
Source of Support: ACM Special Interest Group on Computer Science Education
Program:
Amount Requested: $2,400
Project Period: 2/1/2016 - 9/1/2016
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:** 0 **Acad:** 0 **Sumr:** 0

Support: Current
Title: Inclusive Apps: Supporting Mobile Accessibility Standards Through Educational Exercises
Source of Support: ACM Special Interest Group on Computer Science Education
Program:
Amount Requested: $3,800
Project Period: 2/1/2016 - 9/1/2016
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:** 0 **Acad:** 0 **Sumr:** 0

Support: Pending
Title: SaTC: EDU: Collaborative: PLASMA: Practical LAbs in Security for Mobile Applications
Source of Support: NSF-National Science Foundation
Program: 16-580
Amount Awarded: $ 277,051.00
Project Period: 05/1/201 - 4/30/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:** **Acad:** **Sumr:** 2.0

Current and Pending Support

John Dean

Support: Pending
Title: SaTC: EDU: Collaborative: PLASMA: Practical LAbs in Security for Mobile Applications
Source of Support: NSF-National Science Foundation
Program: 16-580
Amount Awarded: $ 277,051.00
Project Period: 05/1/201 - 4/30/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.75

Current and Pending Support

Mehdi Mirakhorli

Support: Current
Title: Common Architecture Weakness Enumerations (CAWE)
Source of Support: NSF-National Science Foundation [Prime] / Ball State University [Pass-Through]
Program:
Contract Number: IIP-1464654 / G0635
Amount Awarded: $43,050
Project Period: 2/1/2016 - 1/31/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:____** **Acad:____** **Sumr:____**

Support: Current
Title: EAGER: Bringing Design Thinking into Developers' Coding Activities through an Architectural Tactic Recommender System.
Source of Support: NSF-National Science Foundation
Program:
Contract Number: CCF-1543176
Amount Awarded: $80,000
Project Period: 7/1/2015 - 6/30/2017
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:____** **Acad:____** **Sumr:____**

Support: Current
Title: CI-P: Collaborative Research: Planning and Prototyping a Community-Wide Software Architecture Instrument
Source of Support: NSF-National Science Foundation
Program:
Contract Number: CNS-1629810
Amount Awarded: $29,999
Project Period: 8/1/2016 - 7/31/2018
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:____** **Acad:____** **Sumr:** 1

Support: Pending
Title: Resilient Architectures for System Assurance and Lightweight Security of Deeply-Embedded Systems
Source of Support: DOD.U.S. Army Materiel Command

Program: W911NF-12-R-0012
Amount Requested: $404,273
Project Period: 9/1/2017 - 8/31/2020
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 1

Support: Pending
Title: SaTC: EDU: Collaborative: PLASMA: Practical LAbs in Security for Mobile Applications
Source of Support: NSF-National Science Foundation
Program: 16-580
Amount Awarded: $ 277,051.00
Project Period: 05/1/201 - 4/30/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.25

Current and Pending Support

Torrence Sparkman

Support: Pending
Title: SaTC:EDU:Collaborative: Collegiate Penetration Testing Competition (CPTC)
Source of Support: NSF-National Science Foundation
Program: 16-580
Amount Awarded: $202,362.00
Project Period: 07/1/201 - 6/30/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.25

Support: Pending
Title: SaTC: EDU: Collaborative: PLASMA: Practical LAbs in Security for Mobile Applications
Source of Support: NSF-National Science Foundation
Program: 16-580
Amount Awarded: $ 277,051.00
Project Period: 05/1/201 - 4/30/2019
Location of Project: Rochester Institute of Technology
Person-Months Per Year Committed to the Project: **Cal:**____ **Acad:**____ **Sumr:** 0.75

Facilities, Equipment, and Other Resources

Center for Cybersecurity and Computer Support

PI Krutz has worked with the RIT's PhD IT support staff on several projects. This group will provide project support when needed. PI Krutz and Senior Personnel Mirakhorli will collaborate to use necessary resources from the Center for Cyber Security at RIT. The Center has lab space and dedicated administrative support.

University- and College-wide Resources

Rochester Institute of Technology (RIT) provides and administers advanced campus-wide computing resources in support of both teaching and research activities. These resources include a campus wide telecommunication infrastructure (with off-campus access), a distributed computer cluster, and a large number of I/O peripherals (e.g., smart terminals, printers).

RIT is home to many student groups including Women in Computing (WiC), the Society of Software Engineers (SSE) and Women in Technology. The B. Thomas Golisano College of Computer and Information Sciences (GCCIS) at RIT provides technical support for developing and maintaining laboratory IT systems. The college is comprised of nine undergraduate seven graduate programs and one PhD programs.

Rochester Institute of Technology

PLASMA: Practical LAbs in Security for Mobile Applications

Data Management Plan

Expected Data

The expected data to be generated during the course of this project are:

1. Created modules and supporting materials
2. Technical papers describing our findings
3. Course observations and student feedback
4. User feedback generated from course and outreach usage
5. Course materials, such as lectures and slides, homework assignments, and projects
6. Student participation and retention rates
7. Aggregate scores from provided quizzes
8. Adoption information from non-partner institutions

Data Retention and Storage

To protect student privacy, we only will share the student learning data in summary form so that we can monitor the level of dissemination for any required reporting. We will also protect the feedback from instructors and use the anonymous responses only for continuous improvement efforts. We will share the results of the surveys and the assessment instruments we develop. Relevant survey instruments will 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 anonymous form and used to generate annual reports and the final report to NSF. Once the project has concluded, this data will be retained for one year, then purged. All non-confidential data generated by this project will be retained for a minimum of three years after the conclusion of the award, including data that is not specifically disseminated as described in the following section. We will use file storage services provided by RIT to ensure secure preservation of data during the retention period.

Data Dissemination

Technical papers generated during the course of the project will be published in academic journals and conference proceedings. Papers published in venues without archival proceedings, as well as technical reports not otherwise published, will be disseminated via arXiv.

Data produced from the proposed research activities will be made available either publicly on PI Krutz's website or, for sensitive data, available upon request by other researchers. All created project materials will be made available through the project's website.

Standard reports for the NSF will be generated and electronically submitted through normal channels. We may use summary reports for pedagogical purposes so that other approved institutions may see our results and lessons learned. Annual and final reports will evaluate our adherence to this Data Management Plan.

Topic Areas

- Cryptography, applied
- Intrusion detection
- Privacy, theory
- Privacy, applied
- Software

Project Personnel

1. Daniel Krutz; Rochester Institute of Technology; PI
2. Mehdi Mirakhorli; Rochester Institute of Technology; Senior Personnel
3. Torrence Sparkman; Rochester Institute of Technology; Senior Personnel
4. John Dean; Park University; PI at collaborating institution
5. Thomas Richards; Cigital; Paid Consultant
6. Lana Vershage; Rochester Institute of Technology; Unpaid Collaborator
7. Christopher Doss; North Carolina A&T State University; Unpaid Collaborator

Collaboration Plan
PLASMA: Practical Labs in Security for Mobile Applications

1 Roles of the PIs

PI Krutz and Co-PI Dean have known each other for approximately ten years, and frequently discuss pedagogical topics. PI Krutz and Senior Personnel Mirakhorli have worked together in the Department of Software Engineering at RIT for over three years and have collaborated on two publications [1, 2]. Consultant Richards has been a regular guest speaker in PI Krutz's courses for the last four years. PI Krutz and Senior Personnel Sparkman regularly meet to plan, and evaluate some of the preliminary outreach events and assessment information.

PI Krutz will be responsible for leading the initial module creation efforts at RIT. Senior Personnel Mirakhori and Consultant Richards will provide guidance on which modules should be created and provide feedback on the created modules to PI Krutz. After the modules have been evaluated, PI Krutz and Senior Personnel Mirakhori will work with Co-PI Dean to integrate these modules into the curriculum at RIT and Park University. Senior Personnel Mirakhori will provide guidance to Co-PI Dean during Park University's Cybersecurity curriculum development. Senior Personnel Sparkman will work with other project personnel to collect and share educational findings and ensure that the project is meeting the defined educational objectives.

2 Management Plan

Our collaboration has already been successful due to a number of factors: PI Krutz and Senior Personnel Mirakhori meet in person several times a week to discuss project matters. PI Krutz and Co-PI Dean interact several times a week via emails and phone calls to discuss the project, and how it will be used in collaboration between RIT and Park University. We intend to continue our tradition of regular group web-conferences and in person meetings involving all project personnel and participating students. Interactions will also take place at venues where we are disseminating our work in the form of publications, and through tutorials at various conferences. Furthermore, we will continue our use of cloud-based repositories that allow us to easily share data, papers, and other project results.

Our proposal includes support for outreach events through NC A&T (HBCU) and Women in Computing (WiC) at RIT. To provide guidance to NC A&T, we will work with Professor Chris Doss. We will hold regular Skype sessions to train both Professor Doss, and his student employees on the most appropriate ways to conduct the activities and collect appropriate module feedback. Using WiC volunteers,

we have already conducted several events for WiC students and underrepresented urban High School students in the Rochester, NY area. We will hire one WiC student to be the primary manager of outreach activities, and two other WiC students to help conduct outreach events. Although we will be in regular communication about each event, selecting a WiC student to manage these activities will allow us to delegate these responsibilities and allow the WiC student to gain valuable project management experience.

3 Timeline Highlights

According to the described time line in the project description, we have described a plan for our project, which is dependent on the collaboration as outlined in this document. The modules will be defined, created, evaluated and released in an iterative fashion. This will allow us to receive early feedback on our modules, allowing for their early inclusion both in the classroom and at outreach events. An overview of our module creation process is shown in Figure 1.

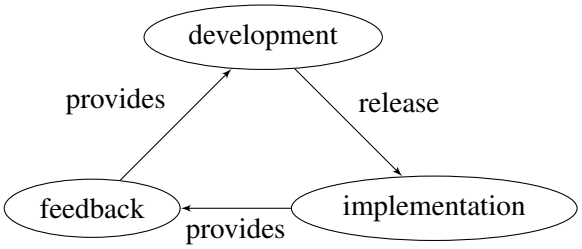


Figure 1: Development Process

References

[1] D. E. Krutz and M. Mirakhorli. Architectural clones: toward tactical code reuse. In *Proceedings of the 31st Annual ACM Symposium on Applied Computing, Pisa, Italy, April 4-8, 2016*, pages 1480–1485, 2016.

[2] D. E. Krutz, M. Mirakhorli, S. A. Malachowsky, A. Ruiz, J. Peterson, A. Filipski, and J. Smith. A dataset of open-source android applications. In *2015 IEEE/ACM 12th Working Conference on Mining Software Repositories*, pages 522–525, May 2015.

Information Technology Services

David Whittaker
Chief Information Officer
8700 NW River Park Dr
Parkville, MO 64152
816-584-6710
Dave.whittaker@park.edu

If the proposal submitted by Dr. Dean entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to collaborate and/or commit resources as detailed in the Project Description or the Facilities, Equipment or Other Resources section of the proposal.

Dave Whittaker
Chief Information Officer
816-584-6710

SYRACUSE UNIVERSITY

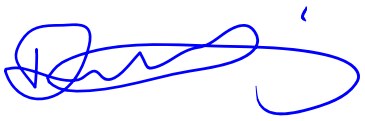
DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

December 8, 2016

To whom it may concern,

If the proposal submitted by Dr. Krutz entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to commit a Virtual Machine and other resources as detailed in the Project Description section of the proposal.

Sincerely yours



Wenliang Du, Ph.D.
Professor
Department of Electrical Engineering & Computer Science
Syracuse University
wedu@syr.edu. Tel: 315-443-9180

R·I·T

Rochester Institute of Technology

B. Thomas Golisano College of Computing
and Information Sciences
Women in Computing
20 Lomb Memorial Drive
Rochester, New York 14623-5608

If the proposal submitted by Dr.Krutz entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to collaborate as detailed in the proposal.

Sincerely,
Lana Verschage
Director of Women in Computing
585-475-7155

R·I·T

Rochester Institute of Technology
B. Thomas Golisano College of Computing
and Information Sciences

Software Engineering
134 Lomb Memorial Drive
Rochester, New York 14623-5608
585-475-2705 Fax: 585-475-7909
andy@se.rit.edu

November 14, 2016

If the proposal submitted by Dr.Krutz entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to collaborate and/or commit resources as detailed in the Project Description or the Facilities, Equipment or Other Resources section of the proposal.

Sincerely,

Andrew Meneely, Ph.D.
Assistant Professor, Department of Software Engineering
Extended Faculty to the Department of Computing Security

NORTH CAROLINA
AGRICULTURAL AND TECHNICAL
STATE UNIVERSITY

www.ncat.edu

A LAND-GRANT UNIVERSITY *and* A CONSTITUENT INSTITUTION *of* THE UNIVERSITY *of* NORTH CAROLINA

If the proposal submitted by Dr. Krutz entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to collaborate and/or commit resources as detailed in the Project Description or the Facilities, Equipment or Other Resources section of the proposal.

Sincerely,

Dr. Christopher Doss
Associate Professor
Director, Mobile Health Interoperability Lab
Department of Electrical and Computer Engineering

Electrical And Computer Engineering
North Carolina Agriculture And
Technial State University

McNair Hall
Room 551

1601 East Market Street
Greensboro, NC 27411

Office 336-285-3711
Fax 336-334-7716

California State University, Chico
400 W. 1st St.
Chico, California 95929-0410

Department of Computer Science
Tel. 530 898-6442 Fax. 530 898-5995
http://csci.ecst.csuchico.edu

If the proposal submitted by Dr.Krutz entitled “PLASMA: Practical LAbs in Security for Mobile Applications” is selected for funding by NSF, it is my intent to collaborate as detailed in the proposal.

David Zeichick
Lecturer, Department of Computer Science
CSU, Chico
Chico, California 95929-0410

dzeichick@csuchico.edu
www.ecst.csuchico.edu/~dzeichick

tel: 530.898.4342
fax: 530.419.0676
mobile: 530.592.6001

Hillside

Hillside Work-Scholarship Connection

December 13, 2016

To Whom It May Concern:

If the proposal submitted by Dr. Krutz entitled "PLASMA: Practical LAbs in Security for Mobile Applications" is selected for funding by NSF, it is my intent to collaborate as detailed in the proposal.

Sincerely,

John Sheible
Career Specialist II
Hillside Work-Scholarship Connection
Office #: 654-1636
Cell #: 752-6409
jsheible@hillside.com