Models for Information Assurance Education and Outreach:

A Report on Year 1 Implementation*

Jianjun Wang

School of Social Sciences and Education

September 1, 2013

* This program is funded by National Science Foundation under Grant No. DUE – 1241636.

Abstract

On September 22, 2012, NSF announced its decision to fund a three-year project, *Models for Information Assurance Education and Outreach* (MIAEO). In the first year of grant operation, MIAEO has invited 18 high school students, two K-12 teachers, and two CSUB student assistants to conduct research explorations in the fields of *network security* and *cryptography*. The hands-on investigation was led by the PI and Co-PI in 2013 summer, and produced five poster presentations through *Research Experience Vitalizing Science - University Program* (REVS-UP) at California State University, Bakersfield. In addition, MIAEO faculty worked on curriculum developments in *Information Assurance* (IA) across multiple departments, and organized a public symposium to expand IA education for approximate 120 community members. Methods employed in this evaluation report include document examinations, participant surveys, and social network analyses. The qualitative and quantitative findings lead to four recommendations to sustain the ongoing progress.

Models for Information Assurance Education and Outreach:
A Report on Year 1 Implementation

Table of Content

Models for Information Assurance Education and Outreach:

A Report on Year 1 Implementation

Development of cyberspace has extensively impacted our national priorities in commerce, education, energy, financial services, healthcare, manufacturing, and defense. In response, NSF has designated a *CyberCorps: Scholarship for Service* (SFS) program to support cybersecurity education and workforce development. On September 22, 2012, NSF awarded a standard grant to California State University, Bakersfield (CSUB). The project, "Models for Information Assurance Education and Outreach" (MIAEO), is designed to enhance capacity of cybersecurity in higher education.

This report provides a summary of MIAEO accomplishments during the first year of NSF funding. In particular, MIAEO includes three core components to address the dual emphasis of SFS on preparation of cybersecurity professionals:

(1) High School Outreach: Concurrent enrollment of high school students to support hands-on research in a four-week summer program;

(2) College Curriculum Development: Enhancement of multidisciplinary IA education for undergraduate students of Computer Science (CS) and Global Intelligence and National Security (GINS) programs;

(3) Community Education Opportunity: Engagement of community partners to create a free course and a lecture series for increasing IA literacy.

While Component (1) is built on expansion of Research Experience Vitalizing Sciences - University Program (REVS-UP) sponsored by Chevron in 2013 summer session, components (2) and (3) represent expansion of cybersecurity education beyond the capacity of existing programs at CSUB.

Creative Features of MIAEO

Unlike most local projects with limited impact, a goal of MIAEO is to "develop models for information assurance and outreach that can be implemented on a regional and national scale to increase interest in the field of information assurance and increase the capacity for high-quality education."[1] Starting in the first year, the project has adopted both confirmatory and exploratory approaches in capacity building. More specifically, *high school outreach* efforts facilitated reconfirmation of REVS-UP accomplishment through team-based research inquiries. Meanwhile, MIAEO included exploratory components to enrich *curriculum development* at CSUB and *education opportunities* for the greater Bakersfield community. Besides addressing the local needs, MIAEO followed professional practice with proven records in community engagement.

REVS-UP

REVS-UP originated from a grant award from NSF's Geosciences *Opportunities for Enhancing Diversity* program in 2004. The seed money has led to recruitment of additional funding from Chevron to (1) increase content knowledge of K-12 science teachers and (2) expand pipelines of professionals in science, technology, engineering, and mathematics (STEM). The impact of REVS-UP has been demonstrated in four fronts during past seven years: (1) The number of applications has grown from 38 in 2007 to 386 in 2013; (2) A total of 26 faculty, 90 CSUB students, 84 K-12 teachers and 384 high school students participated in authentic scientific inquiries at college labs; (3) Over 70% of student participants were in college-bound, more than twice of the state-reported 33.2% for Kern High School District; (4) Almost 50% of the college-bound students were admitted in the University of California system, more than 10

[1] p. 3 of http://www.cs.csub.edu/~melissa/cv.pdf

times of the college-admission rate for this region.

Merit of the summer bridge program hinges on concurrent enrollment of high school students in higher education. Although countries in East Asia have shown better student performance in international assessments (see Martin, Mullis, Foy, & Stanco, 2012; Mullis, Martin, Foy, & Arora, 2012), concurrent enrollment was not allowed in those education systems. Consequently, high school students in those countries have to confine their learning experiences within a rigid boundary of College Entrance Examination. In reflection, researchers found that concurrent enrollment in the U.S. offered students an early start of higher education (Berliner & Biddle, 1995), and thus, "high school students are encouraged to dig into the rich mine of knowledge from college curricula" (Wang, 2013a, p. 13). Despite the claim of education crisis in a well-known report, "A Nation at Risk", trend data from the past three decades showed persistent support of science and mathematics education to sustain vitality of U.S. economy in global market competition (Berliner, 2013).

In addition to the involvement of high school students, REVS-UP sponsored participation of K-12 teachers and CSUB student assistants in hands-on investigations. With the NSF funding, REVS-UP has added *network security* and *cryptography* as new dimensions of inquiry in 2013 summer session. The team-based research has supported 18 high school students to rejuvenate IA research interest, two CSUB students to gain internship experiences, and two K-12 teachers to enhance subject competency through project developments.

Curriculum Development

IA is defined as a set of measures that protect and defend information systems to ensure their availability, integrity, authentication, confidentiality, and nonrepudiation (Stamm, 2011).

Because of the widespread needs, “The development of a model curriculum in Information Assurance would directly benefit academia, industry, and government agencies” (Park, 2010, p. 17).

Since security is more dependent on people than on technology, MIAEO has embedded the multidisciplinary nature in curriculum development. As Cegielski (2008) acknowledged, “The interdisciplinary nature of the professional practice of information assurance increases the complexity associated with modeling a curriculum designed to prepare students for professional practice” (p. 44). In the first year, the P.I. (professor of computer science) and Co-P.I. (professor of mathematics) gained their department endorsement to share a new IA course, *MATH/CMPS 475 - Applied Cryptography*. Two elective courses, *CMPS 445 - Data Mining and Visualization* and *CMPS 451 - Vulnerability Analysis* (CMPS 474 in the grant proposal), have been added to broaden the IA knowledge base. Those course proposals have gone through a multilevel approval process.

In addition, development of new IA courses also includes consideration of professional pedagogy. Momeau (2006) pointed out, “In the traditional training approach, the idea is to be able to transfer a body of knowledge of the profession to learners. Unfortunately, this does not take into consideration how people become professionals” (p. 22). To solve this issue, Goel et al. (2006) suggested,

> Objectivism and constructivism are two distinct theories about learning that can be applied to IA education. ... Objectivism propagates rote learning via memorization and feedback. … In the constructivist approach, students construct their own knowledge by actively participating in learning. This approach values collaboration, the autonomy of the student, reflectivity, and active engagement. Such a teaching philosophy provides a

> rich learning environment for students, in which they may explore learning independently and draw conclusions for themselves. (p. 4)

In all new courses developed from MIAEO, a 150-munite lab session has been included each week to accommodate hands-on activities in IA research. A cybersecurity research laboratory has already been established to support inquiries in those elective courses for Computer Science majors. Hence, the merit of the new IA curriculum is built on generalizable practices of hands-on learning. As Bhagyavati (2006) pointed out, “Information assurance courses are most effective when they utilize hands-on activities” (p. 5).

Community Outreach

National Research Council (2011a) pointed out, “Personal and societal decisions in the 21st century increasingly require scientific and technological understanding. … Targeting all students, not just those who will pursue postsecondary education or careers in STEM or STEM-related fields, will better prepare citizens to face the challenges of a science- and technology-driven society” (p. 5). Thus, enhancement of public education cannot be solely confined within students of the professional field. To broaden the outreach effort, the third component of MIAEO is to offer a community course and a lecture series for increases of IA knowledge among general citizens.

As Geo et al. (2006) observed, “Developing course material for IA requires experts from several disciplines. Students interested in the curriculum also come from a variety of backgrounds, including public policy, law, computer science, business, and information science” (p. 10). Besides using the expertise of PI and Co-PI in computer science and mathematics, development of the community course (PLSI 377) was led by Dr. Mark A. Martinez, Director of the Global Intelligence and National Security program and Professor in the Department of Political Science. The PLSI 377 course setting covers generic topics of cybersecurity concerns[2].

In addition, first session of the public lecture series was held on May 15, 2013 by a panel of experts from *CSUB, the local FBI field office, the FBI Sacramento region office, Edwards Air Force Base,* and *Aera Energy*. This collaborative endeavor not only expanded the partnership building among the local stakeholders, but also reflected the virtue of STEM education for both specialists and general citizens (National Council of Teachers of Mathematics, 2000; National Research Council, 2011b).

Research Questions

The NSF guideline stipulates that "All proposals must describe plans for data management and sharing of the products of research."[3] Following the proposed plan of MIAEO, Year 1 implementation includes completion of the first REVS-UP summer session in 2013, as well as initiation of the *course development* and *community outreach* components. Accordingly, three research questions are developed for this annual evaluation report:

1. What are the accomplishments of 2013 REVS-UP projects in IA inquiries?
2. What is the impact of course development and community outreach?
3. What recommendations are derived from this report to sustain the ongoing progress?

Methods

Multilevel data have been gathered to assess the impact of REVS-UP during 2013 summer session. The team-based research products are represented by poster presentations to summarize project development in *network security* and *cryptography*. Quality of the IA

[2] p. 11 of http://www.csub.edu/PoliSci/programinfo/gradreq.doc
[3] http://www.nsf.gov/pubs/2012/nsf12585/nsf12585.htm

projects is evaluated on six dimensions, *Context of and Purpose for the Poster, Content Development, References and Evidence, Composition and Format, Conclusions and Related Outcomes,* and *On-site Explanation.* In each dimension, a project is rated at four levels, *Emerging, Basic, Proficient,* and *Exemplary.* In combination, the instrument incorporates important features of a widely-used rubric, "Valid Assessment of Learning in Undergraduate Education" (VALUE). Over past three years, this instrument has been field-tested successfully by both REVS-UP and Student Research Scholarship (SRS) programs at CSUB (Wang, 2013b).

To triangulate evaluation findings within the local context, a school rating scale is adopted from greatschools.com according to student performance on state-required tests. A *NetDraw* software package has been employed to support a social network analysis (SNA) of student affiliations across different high schools (Borgatti, 2002). In addition, survey responses have been collected to assess attitude improvements of REVS-UP participants under a pretest/posttest setting (Question 1).

As an ongoing process, *curriculum development* is described in this report to support improvement of MIAEO implementation according to the *Utility, Propriety, Feasibility,* and *Accuracy* standards from Joint Committee on Standards for Educational Evaluation (Yarbrough, Shulha, Hopson, & Caruthers, 2010). Meanwhile, baseline records have been established from participant feedback to track enhancement of *community outreach* during Year 1 implementation (Question 2). On basis of the quantitative and qualitative findings for Questions 1 and 2, this report concludes with four recommendations to sustain program effectiveness (Question 3).

Evaluation Findings

REVS-UP Project

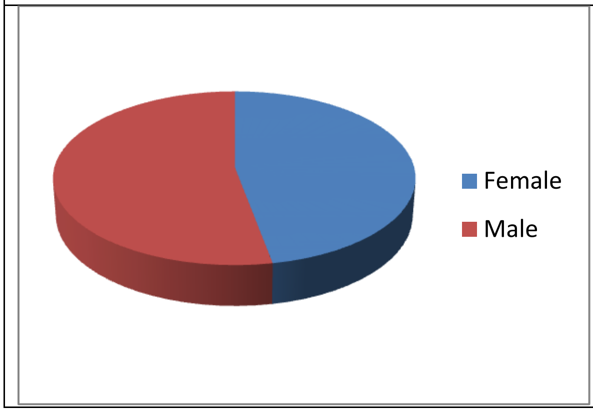
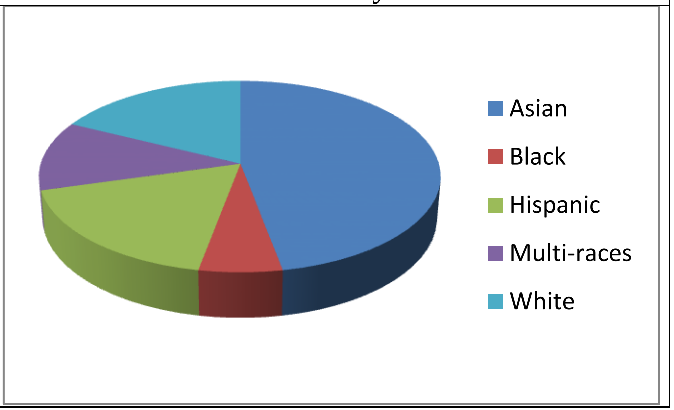
In 2013 summer session, the PI worked with eight high school students, one teacher, and one CSUB student to conduct research in the area of *network security*. The team-based inquiries resulted in two poster presentations, “Crack Me If You Can: Using GPU Machines to Crack Passwords” (CMIYC) and “Defense Against Human Hacking”, at conclusion of the summer session. The Co-PI concurrently worked with 10 high school students, one teacher, and one CSUB student on research projects in *cryptography*, and produced three poster presentations, “Zero Knowledge, We Know Everything ... !”, “Elliptic Enigma”, and “Factor Fiction”. NSF funding has been employed to compensate faculty mentors, CSUB student assistants, and high school teachers.

According to the original MIAEO budget allocation, NSF contributes $500 to support each high school student. Since high school students traditionally received $700 for their REVS-UP participation in other STEM projects, additional funding has been provided by Chevron Cooperation to amend the gap of $200 per student, and thus, maintain the equity of project support. Acknowledgement of those supports has been made in *Appendix 1: Poster Presentations of Five IA Research Projects*.

All REVS-UP projects entered a competition for research awards. One of the IA projects, CMIYC, has been rated at the highest *Exemplary* rank on five dimensions, (1) Context of and Purpose for the Poster, (2) Content Development, (3) Composition and Format, (4) Conclusions and Related Outcomes, and (5) On-site Explanation. In the sixth dimension, CMIYC also reached the *Proficient* level for *References and Evidence Examinations*. On a scale of 1 (lowest) to 4 (highest), the peer-review results show an average of 2.9 rating across five IA projects. Hence, the Year 1 outcome already showed a near 3.0 (or “proficient”) rating at the MIAEO program level.

More importantly, to enhance generalizability of the REVS-UP model for IA education, MIAEO did not confine high school participants within a particular gender or ethnic group. Table 1 shows participation of an approximately equal number of male and female students from five different ethnic groups.

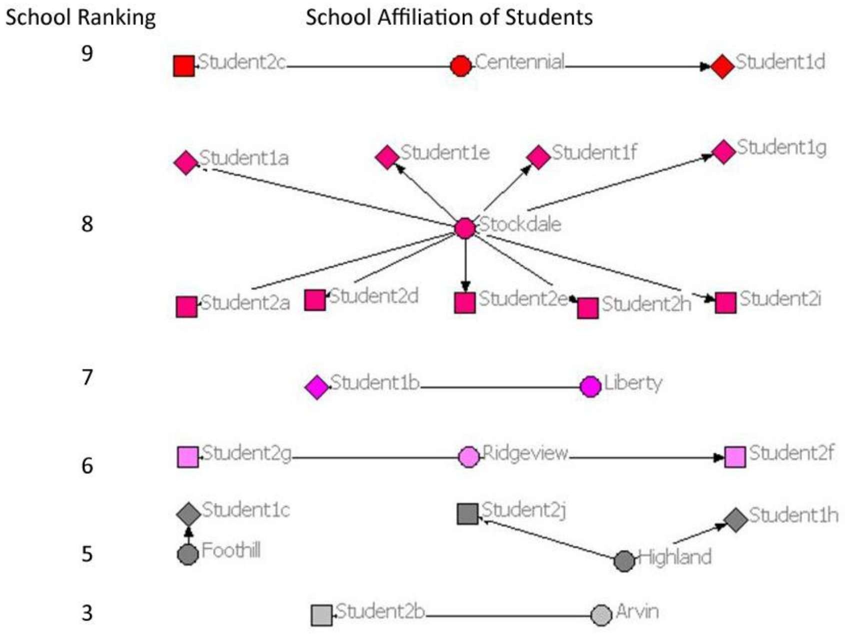
Table 1: Student Distribution across Gender and Ethnic Categories*

Gender	Ethnicity
	

*One missing response occurred in the gender and ethnicity data collection.

In addition, student participants are drawn from diversified high schools. In Figure 1, school names are indicated by circles, and students in the *network security* and *cryptography* groups are represented by diamond and square symbols, respectively. School rankings range from 1 for the *worst* to 10 for the *best*, and are developed by greatschools.com according to student performance in state-mandated tests. The plot of *Netdraw* (Borgatti, 2002) shows involvement of traditionally-underserved students from high-needs schools, such as Arvin, Foothill, and Highland high schools (Figure 1).

Figure 1: Student Affiliation Across Diversified Schools



Accompanied to the background evaluation is an assessment of attitude changes among high school students toward IA investigation. Under a pretest/posttest setting, high school students selected Likert-scale responses (5 = strongly agree, 3 = neutral, 1 = strongly disagree) to two statements:

A. I am excited about this activity.
B. I feel confident that I am prepared for this activity.

At the introductory stage of REVS-UP investigation, IA exploration could strengthen humble attitudes among students. As Confucius pointed out, "The more a man learns, the more he knows his ignorance"[4]. According to the assessment outcome, the mean responses to Statements A and B were 4.35 and 3.59 in pretest, respectively. The corresponding results changed to 4.31 and 3.38 in the posttest. Although the sample size was too small to test statistical significance, the descriptive results have confirmed a reciprocal relationship between

[4] p. 1 of http://novel.jschina.com.cn/yingyuwenxue/yinghmy/yinghanmingyan15.htm

IA learning and attitude adjustment during 2013 REVS-UP session.

Meanwhile, there was no change in average responses of high school students toward the following items:

C. I am interested in computer security.
D. I am interested in going to college.

For Statement C, the average response remained in the “agree” category for both pretest and posttest. For Statement D, students unanimously chose the “strongly agree” option as their responses. Hence, while students developed more humble attitudes toward IA inquiries, they demonstrated stronger positive attitudes toward college education.

The multiple-choice results are supported by open-ended responses from REVS-UP participants. Both teachers and high school students indicated the IA investigation as a new field of their learning experiences. Teachers recognized the benefit of hands-on research for high school students in the university setting. CSUB faculty mentors and student assistants were also rated in “very supportive” or “supportive” categories by high school participants. In combination, the results indicated that a community of learners has emerged from the REVS-UP platform to extend mutual support in the process of team-based IA inquiries.

Curriculum Development

For more than three decades, Joint Committee on Standards for Educational Evaluation advocated four attributes, *utility, feasibility, propriety,* and *accuracy*, to guide program improvement (Yarbrough, Shulha, Hopson, & Caruthers, 2010). Those attributes are articulated in this section to facilitate enhancement of IA education across multiple disciplines.

In the first year of MIAEO implementation, *utility* consideration is reflected by alignment of course sequence for IA-related programs in the university catalog. In the MIAEO proposal, CMPS 474 was the label for a new IA course on *vulnerability analysis*. Because the content is highly complementary to *CMPS 450 - Compilers*, the course number has been changed into CMPS 451 to improve program coherence.

Meanwhile, course sequence has been established to streamline knowledge development. Two new courses, *CMPS 445 - Data Mining and Visualization* and *MATH/CMPS 475 - Applied Cryptography*, are arranged sequentially in Winter and Fall of 2014 prior to the offering of CMPS 451. To strengthen IA education in the GINS program, *PLSI 304 - International Relations* and *CRJU 440 - Terrorism* have been converted from electives to required courses.

Another change to the original proposal is to reversely move CMPS 476 and MATH/CMPS 475 from program requirements to elective courses. Because those courses are offered every other year, this change has enhanced *feasibility* of program completion for computer science majors. In addition, GEOL 450 has been incorporated in the GINS program to provide GIS tools. This change has reduced excessive requirements of both *GIS* and *behavioral analysis* tools in the cognate courses. Other improvements to strengthen feasibility include adding *CMPS 295 - Discrete Mathematics* as a parallel course option for *CMPS 215 - Unix Programming Environment*. Similarly, *CMPS 350 - Programming Languages* has been adopted as an alternative option for *CMPS 376 - Computer Networks*. Students are allowed to take those parallel or alternative courses toward program completion.

Given the multidisciplinary nature of MIAEO, the *propriety* feature is illustrated by development of a useful website to facilitate dissemination of advisory handouts for students of all IA-education groups[5]. While the grant proposal indicated 193-198 units for concentration in information security, the *accuracy* consideration has led to adjustment of the total unit to 180 to

[5] http://www.cs.csubak.edu/~melissa/gins.php

conform to unit reductions in general education. As a result, curriculum development activities in the first year include content alignment, course scheduling, curriculum adjustment, and information dissemination to support enhancement of IA education at CSUB.

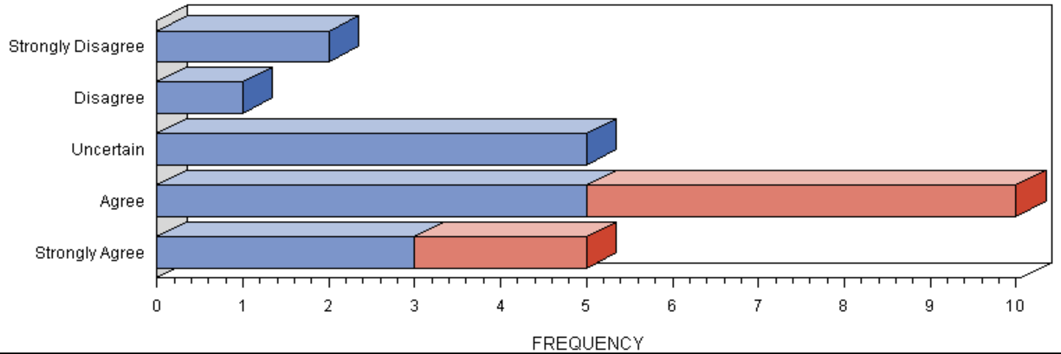
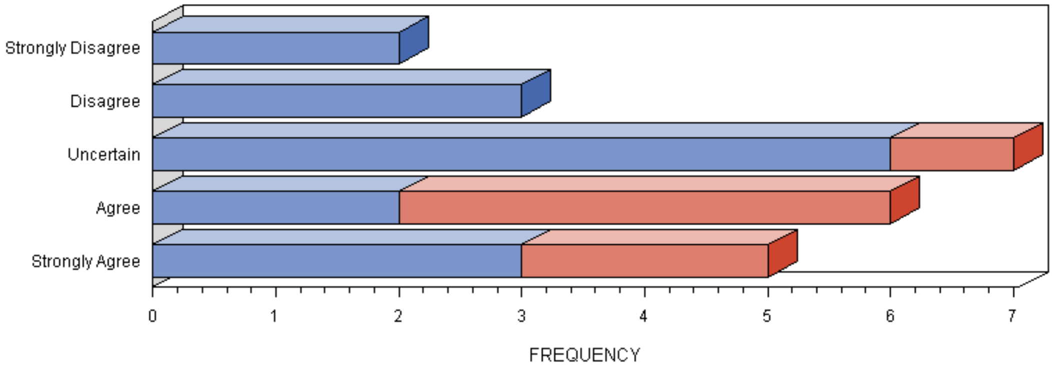
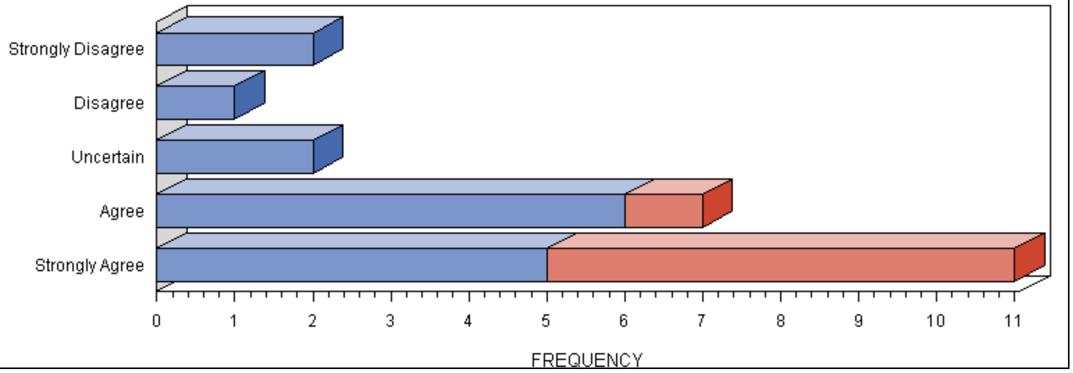
Community Engagement

"It is envisioned that IA will work with state and local government entities, healthcare providers throughout the state, and the other state institutions of higher learning (as well as the K-12 community) to improve the security of all of our data networks and computer systems" (Carr, 2010, p. 1). Therefore, community engagement is an integral part of MIAEO implementation.

In the evening of May 15, 2013, a Cyber Security Panel Discussion was held for the public to strengthen community engagement in IA education[6]. Approximately 120 audiences attended this event. Table 2 shows positive feedback from students of CMPS 340 and PLSI 377 toward the panel discussion. In particular, the survey results reconfirmed attractiveness of this event – more than 78% of the respondents would attend similar events in the future (Table 2).

[6] http://www.csub.edu/pac/news/2013/spring/CSUB-hosts-panel-discussion-on-Cyber-Security-Challenges.shtml.shtml

Table 2: Student Feedback from Cybersecurity Panel Discussion on May 15, 2013

Item	Frequency of Student Responses (Blue: CMPS 340; Red: PLSI 377)
The panel met my expectations	
I learned helpful information at this event	
I would take similar events in the future	

According to Lev Vygotsky (1978), a seminal educator, learning outcomes are more positive when teaching activities can be clearly designated within “the zone of proximal development” (ZPD). ZPD represents distance between the actual development level of the learners and the level of potential development in collaboration with more capable peers and experts. In comparison, PLSI 377 is designed for novices, and thus, ZPD is easier to identify at the introductory level. CMPS 340 is built on CMPS 215, and covers investigative techniques, evidence handling procedures, forensics tools, digital crime reconstruction, and legal guidelines. Table 2 indicates that the panel discussion for community members seems to fit the ZPD of most PLSI 377 students, leading them to express more appreciation of this event than their peers in CMPS 340.

In summary, MIAEO has achieved positive outcomes in all three components, *REVS-UP*, *Curriculum Development*, and *Community Outreach*. More importantly, those accomplishments were made cost-effectively: (1) **REVS-UP** has leveraged additional funding from Chevron Cooperation to support participation of high school students in IA research projects; (2) Features of *utility, feasibility, propriety,* and *accuracy* are incorporated in **curriculum development** to support additional program improvements under the original budget configuration; (3) In preparing for the **community outreach** event, staff of CSUB President's office arranged various logistics with no cost to the grant, including (i) getting the university library to donate the Reading Room for the panel discussion, (ii) getting Associated Students Inc. (ASI) to sponsor the reception before the event, and (iii) having student clubs help with the event setting up and cleaning up. Altogether, the broad-based support is grounded on a close alignment between this NSF grant and CSUB's vision statement, i.e., "By 2014-15, CSU Bakersfield will be the leading campus in the CSU system in terms of faculty and academic excellence and diversity, quality of the student experience, and community engagement" [7].

Recommendations

Year 1 implementation of MIAEO has completed two tracks of research inquiries in *network security* and *cryptography,* and produced five poster presentations in 2013 REVS-UP session. New course proposals have passed approval processes at the *department, school,* and

[7] http://president.csub.edu/index.cfm?fuseaction=menu&menu_id=65

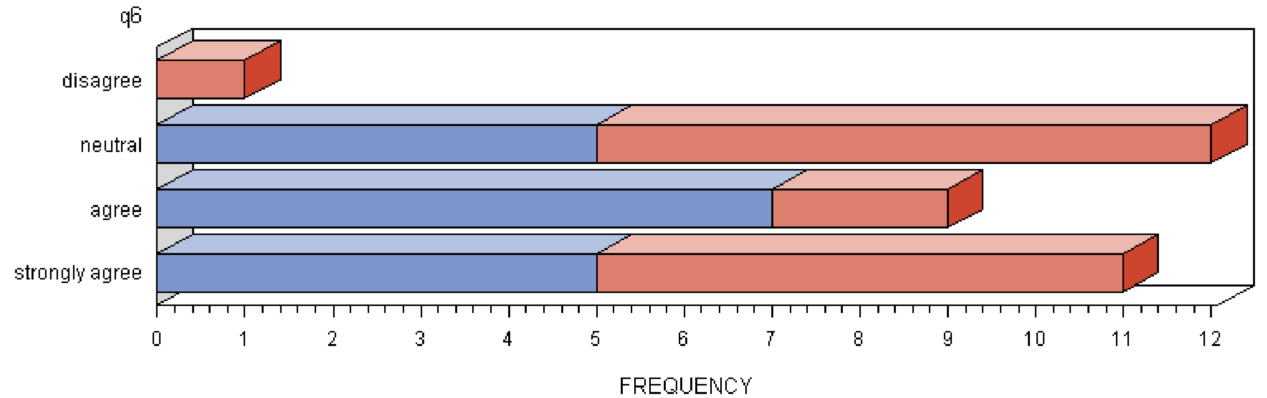
university levels. A well-attended cybersecurity symposium has been organized to expand IA education for the general public. The multilevel evaluation of Year 1 implementation leads to four recommendations to sustain the ongoing progress.

(1) Incorporate More Hands-on Activities in REVS-UP

In 2013 summer, student and teacher participants indicated needs of incorporating more hands-on activities in REVS-UP. School administrators have been advocating alignment of school curricula with state-mandated paper-and-pencil tests in recent years, which inadvertently deprived student learning opportunities from hands-on exploration (Wang, 2013b). As professors of past REVS-UP projects indicated, "It remains true that students are attracted more to the STEM fields when applications and hand-on experiences are an integral part of the curriculum" (Meyer & Gasparayan, 2010, p. 77).

Figure 2: Attitude Change in Crytography

Response Item: Q6 – I am interested in cryptography (Blue: pretest; Red: posttest)



Nonetheless, when a Likert scale was employed to assess student agreement to a statement "I am interested in cryptography", the mode of responses dropped from "agree" in the pretest to “neutral” in the posttest (Figure 2). Qualitative comments from students, such as the one below, indicated that the interest decrease was not due to lack of team mentoring:

> Thank you Dr. Lam, and thank you Frank Madrid for the amazing experiences. Never thought I would learn so much in a program before. You altered my mentality, and you have inspired me.

Hence, hands-on activities become a teaching approach to help reverse the interest change in Figure 2.

(2) Recruit Qualified Teaching Assistants for the IA Program

To implement the established curriculum, MIAEO has incorporated a plan of hiring teaching assistants (TA). While faculty qualifications are justified in the NSF proposal, criteria for TA hiring need to be constantly reviewed to strengthen the IA education capacity at CSUB.

Since the whole could be larger than the sum of its parts, MIAEO might benefit from the support of other STEM projects across the campus, including *posting advertisement at their websites* and/or *using their track records to help identify potential TA candidates*. The requirements in the current job posting are:

* Established Junior, Senior, or Post-Bacc standing
* Declared major or minor in Computer Science, Computer Engineering or Mathematics
* Completed the required 200-level courses for their Computer Science, Computer Engineering or Mathematics degree
* Retained 3.0 GPA in their Computer Science, Computer Engineering and/or Mathematics courses

Because the job responsibility is designated to support *research* and *tutoring*, past participants of *REVS-UP* or *other STEM inquiry projects* might possess additional research experiences to feed the TA pipeline.

(3) Expand Community Outreach Approaches for Local Residents

From a systematic perspective, outreach activities span across multiple tiers of the service community. In particular, the majority of REVS-UP participants come from K-12 school community. In 2013 summer, 18 high school students collaborated on IA inquires in REVS-UP. The capacity can be expanded next year to accommodate 20 students according to the MIAEO budget planning.

Unlike other IA courses, PLSI 377 is scheduled in evenings for community members to attend. In the first year, all students of this class came from CSUB. Thus, public awareness of the course offering can be expanded to attract more community members in the future. In addition, Cyber Security Panel Discussion is designed for the general public. Positive feedback from the first symposium has justified multiple offerings of similar learning opportunities each year.

(4) Improve Student Engagement

Improvement of student engagement hinges on a proper consideration of student academic preparation. For instance, regarding the Cyber Security Panel Discussion on May 15, 2013, students of CMPS 340 indicated needs of focusing on specific topics, and their peers in PLSI 377 wished to see involvement of more people from various fields. Thus, no single approach can concurrently address the split requests pertaining to different “zones of proximal development” (ZPD) (Vygotsky, 1978). In this regard, student engagements are aligned with the dual emphases of science education (i.e., *science for scientists* and *science for everyone*) advocated by National Standards for Science Education (National Research Council, 2011b).

References

Berliner, D. C. (2013). *Three decades of lies*. Retrieved from http://dianeravitch.net/2013/04/24/david-berliner-on-a-nation-at-risk-three-decades-of-lies/

Berliner, D. C, & Biddle, B. J. (1995). *The manufactured crisis: Myths, fraud, and the attack on America's public schools*. Redding, MA: Addison-Wesley.

Bhagyavati, B. (2006). Laboratory exercises in online information assurance courses. *ACM Journal of Educational Resources in Computing, 6* (4), 1-5.

Borgatti, S.P. (2002). *NetDraw: Software for network visualization*. Lexington, KY: Analytic Technologies.

Carr, M. (2010). *Information assurance*. Retrieved from http://it.unm.edu/organization/factsheets/infoassurance.pdf

Cegielski, C.G. (2008). Toward the development of an interdisciplinary information assurance curriculum: knowledge domains and skill sets required of information assurance professionals. *Decision Sciences Journal of Innovative Education*, *6* (1), 29-49.

Goel, S., Pon, D., Bloniarz, P., Bangert-Drowns, R., Berg, G., Delio, V., Iwan, L., Hurbanek, T., Schuman, S., Gangolly, J., Baykal, A., & Hobbs, J. (2006). Innovative model for information assurance curriculum: A teaching hospital. *ACM Journal of Educational Resources in Computing*, *6*(3), 1-15.

Martin, M.O., Mullis, I.V.S., Foy, P., & Stanco, G.M. (2012). *TIMSS 2011 international results in science.* Chestnut Hill, MA: TIMSS & PIRLS International Study Center, Boston College.

Meyer, T., & Gasparayan, V. (2010). Summer REVS-UP: Project in physics. In A. Gebauer (Ed.), *2010 Chevron report*. Bakersfield, CA: CSUB.

Momeau, K. (2006). *Preparing the future technologist: Critical features of experiential learning activities in an undergraduate information assurance (IA) program*. Malibu, CA: Pepperdine University.

Mullis, I.V.S., Martin, M.O., Foy, P., & Arora, A. (2012). *TIMSS 2011 international results in mathematics*. Chestnut Hill, MA: TIMSS & PIRLS International Study Center, Boston College.

National Council of Teachers of Mathematics (2000). *Principles and standards for school mathematics*. Reston, VA: Author

National Research Council. (2011a). *Successful K-12 STEM education: Identifying effective approaches in science, technology, engineering, and mathematics.* Committee on Highly Successful Science Programs for K-12 Science Education. Board on Science Education and Board on Testing and Assessment, Division of Behavioral and Social Sciences and Education. Washington, DC: The National Academies Press.

National Research Council (2011b). *A framework for K-12 science education: Practices, crosscutting concepts, and core ideas*. Washington, DC: National Academies Press.

Park, I. (2010). *Essays on information assurance: Examination of detrimental consequences of information security, privacy, and extreme event concerns on individual and organizational use of systems*. Buffalo, NY: State University of New York at Buffalo.

Stamm, D. (2011). *Information assurance practice and standards for commercial business*. Minneapolis, MN : Walden University.

Vygotsky, S. L. (1978.) *Mind in society*. *The development of higher psychological processes*. Cambridge: Harvard University Press.

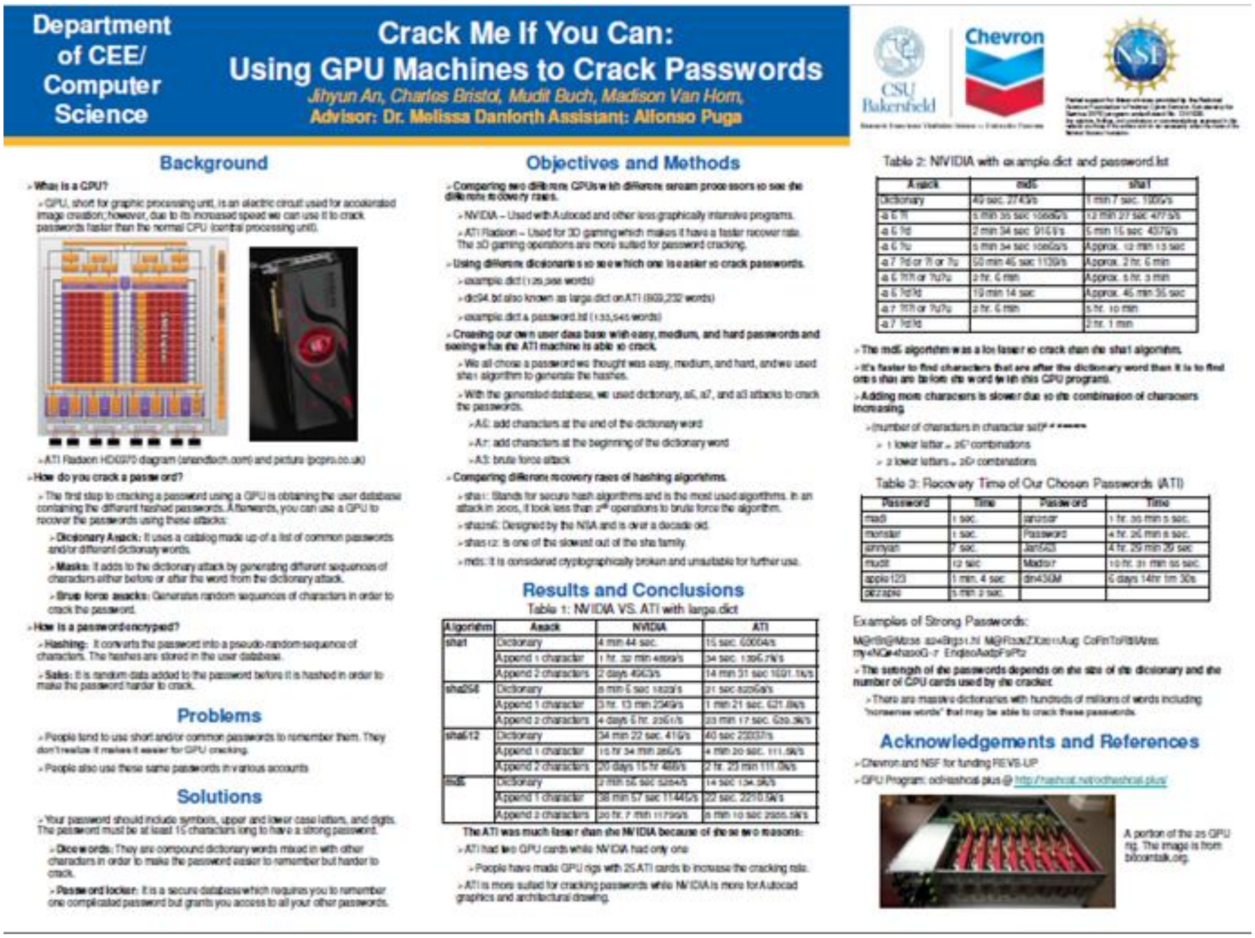
Wang, J. (2013a). An assessment of education quality beyond dinner table discussions. *International Education Studies*, *6* (1), 111-116.

Wang, J. (2013). *Creative collaboration between Chevron and CSUB: Research Experience Vitalizing Science – University Program*. Bakersfield, CA: California State University, Bakersfield (ERIC Document Reproduction Service No. ED 543 805).

Yarbrough, D. B., Shulha, L. M., Hopson, R. K., & Caruthers, F. A. (2010). *The program evaluation standards* (3rd ed.). Thousand Oaks, CA: Sage & the Joint Committee on Standards for Educational Evaluation.

Appendix 1: Poster Presentations of Five IA Research Projects

1. Crack Me If You Can: Using GPU Machines to Crack Passwords
2. Defense Against Human Hacking
3. Zero Knowledge, We Know Everything ... !
4. Elliptic Enigma
5. Factor Fiction



Department of CEE/ Computer Science

Crack Me If You Can: Using GPU Machines to Crack Passwords

Jihyun An, Charles Bristol, Mudit Buch, Madison Van Horn,
Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

CSU Bakersfield

Chevron

[illegible]

Background

- **What is a GPU?**
  - GPU, short for graphic processing unit, is an electric circuit used for accelerated image creation; however, due to its increased speed we can use it to crack passwords faster than the normal CPU (central processing unit).
  - ATI Radeon HD6970 diagram (anandtech.com) and picture (pcpro.co.uk)
- **How do you crack a password?**
  - The first step to cracking a password using a GPU is obtaining the user database containing the different hashed passwords. Afterwards, you can use a GPU to recover the passwords using these attacks:
    - **Dictionary Attack:** It uses a catalog made up of a list of common passwords and/or different dictionary words.
    - **Masks:** It adds to the dictionary attack by generating different sequences of characters either before or after the word from the dictionary attack.
    - **Brute force attacks:** Generates random sequences of characters in order to crack the password.
- **How is a password encrypted?**
  - **Hashing:** It converts the password into a pseudo-random sequence of characters. The hashes are stored in the user database.
  - **Salts:** It is random data added to the password before it is hashed in order to make the password harder to crack.

Problems

- People tend to use short and/or common passwords to remember them. They don't realize it makes it easier for GPU cracking.
- People also use these same passwords in various accounts.

Solutions

- Your password should include symbols, upper and lower case letters, and digits. The password must be at least 15 characters long to have a strong password.
  - **Dicewords:** They are compound dictionary words mixed in with other characters in order to make the password easier to remember but harder to crack.
  - **Password locker:** It is a secure database which requires you to remember one complicated password but grants you access to all your other passwords.

Objectives and Methods

- **Comparing two different GPUs with different stream processors to see the different recovery rates.**
  - NVIDIA – Used with Autocad and other less graphically intensive programs.
  - ATI Radeon – Used for 3D gaming which makes it have a faster recover rate. The 3D gaming operations are more suited for password cracking.
- **Using different dictionaries to see which one is easier to crack passwords.**
  - example.dict (129,988 words)
  - dic94.txt also known as large.dict on ATI (869,232 words)
  - example.dict & password.lst (133,545 words)
- **Creating our own user data base with easy, medium, and hard passwords and seeing what the ATI machine is able to crack.**
  - We all chose a password we thought was easy, medium, and hard, and we used sha1 algorithm to generate the hashes.
  - With the generated database, we used dictionary, a6, a7, and a3 attacks to crack the passwords.
    - A6: add characters at the end of the dictionary word
    - A7: add characters at the beginning of the dictionary word
    - A3: brute force attack
- **Comparing different recovery rates of hashing algorithms.**
  - sha1: Stands for secure hash algorithms and is the most used algorithms. In an attack in 2005, it took less than 2^{69} operations to brute force the algorithm.
  - sha256: Designed by the NSA and is over a decade old.
  - sha512: Is one of the slowest out of the sha family.
  - md5: It is considered cryptographically broken and unsuitable for further use.

Results and Conclusions

Table 1: NVIDIA VS. ATI with large.dict

Algorithm	Attack	NVIDIA	ATI
sha1	Dictionary	4 min 44 sec.	15 sec. 63004/s
	Append 1 character	1 hr. 32 min 4898/s	34 sec. 1396.7k/s
	Append 2 characters	2 days 4963/s	14 min 31 sec 1601.1k/s
sha256	Dictionary	8 min 5 sec 1822/s	21 sec. 8206k/s
	Append 1 character	3 hr. 13 min 2349/s	1 min 21 sec. 621.8k/s
	Append 2 characters	4 days 6 hr. 2361/s	23 min 17 sec. 629.3k/s
sha512	Dictionary	34 min 22 sec. 416/s	40 sec 23037/s
	Append 1 character	15 hr 34 min 265/s	4 min 20 sec. 111.9k/s
	Append 2 characters	20 days 15 hr 466/s	2 hr. 23 min 111.0k/s
md5	Dictionary	2 min 56 sec 5264/s	14 sec 134.9k/s
	Append 1 character	38 min 57 sec 11445/s	22 sec. 2210.5k/s
	Append 2 characters	20 hr. 7 min 11799/s	5 min 10 sec 2505.5k/s

The ATI was much faster than the NVIDIA because of these two reasons:

- ATI had two GPU cards while NVIDIA had only one
  - People have made GPU rigs with 25 ATI cards to increase the cracking rate.
- ATI is more suited for cracking passwords while NVIDIA is more for Autocad graphics and architectural drawing.

Table 2: NIVIDIA with example.dict and password.lst

Attack	md5	sha1
Dictionary	49 sec. 2743/s	1 min 7 sec. 1006/s
-a 6 ?l	5 min 35 sec 10686/s	12 min 27 sec 4775/s
-a 6 ?d	2 min 34 sec 9161/s	5 min 15 sec 4379/s
-a 6 ?u	5 min 34 sec 10660/s	Approx. 12 min 13 sec
-a 7 ?d or ?l or ?u	50 min 45 sec 1139/s	Approx. 2 hr. 6 min
-a 6 ?l?l or ?u?u	2 hr. 6 min	Approx. 5 hr. 3 min
-a 6 ?d?d	19 min 14 sec	Approx. 45 min 35 sec
-a 7 ?l?l or ?u?u	2 hr. 6 min	5 hr. 10 min
-a 7 ?d?d		2 hr. 1 min

- **The md5 algorithm was a lot faster to crack than the sha1 algorithm.**
- **It's faster to find characters that are after the dictionary word than it is to find ones that are before the word with this GPU program.**
- **Adding more characters is slower due to the combination of characters increasing.**
  - (number of characters in character set)$^{\#\ of\ characters}$
    - 1 lower letter = 26^1 combinations
    - 2 lower letters = 26^2 combinations

Table 3: Recovery Time of Our Chosen Passwords (ATI)

Password	Time	Password	Time
madi	1 sec.	janosar	1 hr. 36 min 5 sec.
monster	1 sec.	Password	4 hr. 26 min 8 sec.
jinnyan	7 sec.	Jan523	4 hr. 29 min 29 sec
mudit	12 sec	Madis7	10 hr. 31 min 55 sec.
apple123	1 min. 4 sec	dm430M	6 days 14hr 1m 30s
pizzapie	5 min 2 sec.		

Examples of Strong Passwords:

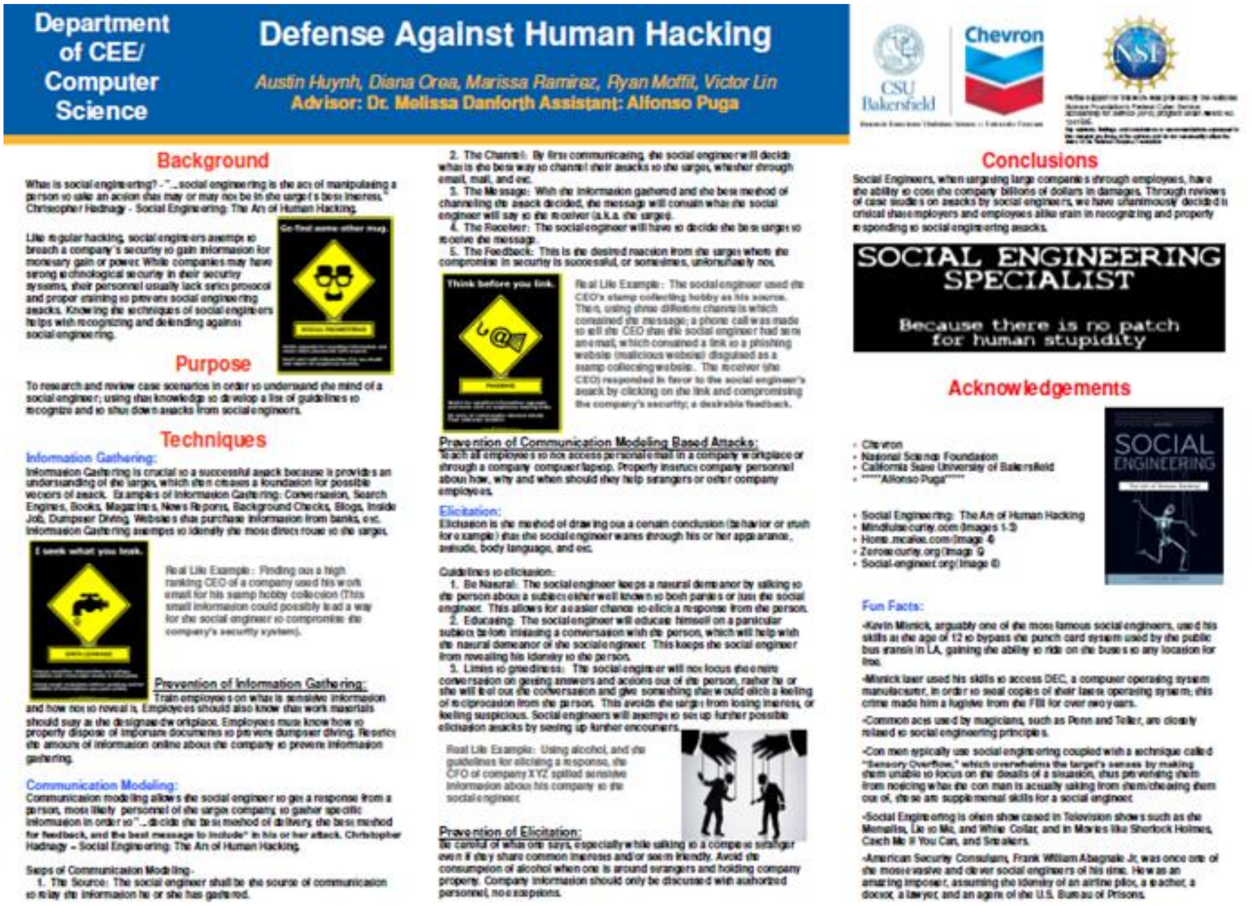
M@rtin@Mose a24Brg51.h! M@Ro2eZXoe11Aug CoRnToRtilAres my4NC#4hasoG-7 EngleoAwdpFoPtz

- **The strength of the passwords depends on the size of the dictionary and the number of GPU cards used by the cracker.**
  - There are massive dictionaries with hundreds of millions of words including "nonsense words" that may be able to crack these passwords.

Acknowledgements and References

- Chevron and NSF for funding REVS-UP
- GPU Program: oclHashcat plus @ http://hashcat.net/oclhashcat-plus/

A portion of the 25 GPU rig. The image is from bitcointalk.org.


CSU Bakersfield
Chevron
NSF
Go find some other mug.
I seek what you leak.
Think before you link.
SOCIAL ENGINEERING

Department of CEE/ Computer Science

Defense Against Human Hacking

Austin Huynh, Diana Orea, Marissa Ramirez, Ryan Moffit, Victor Lin

Advisor: Dr. Melissa Danforth Assistant: Alfonso Puga

Background

What is social engineering? - "...social engineering is the act of manipulating a person to take an action that may or may not be in the target's best interest." Christopher Hadnagy - Social Engineering: The Art of Human Hacking.

Like regular hacking, social engineers attempt to breach a company's security to gain information for monetary gain or power. While companies may have strong technological security in their security systems, their personnel usually lack strict protocol and proper training to prevent social engineering attacks. Knowing the techniques of social engineers helps with recognizing and defending against social engineering.

Purpose

To research and review case scenarios in order to understand the mind of a social engineer; using that knowledge to develop a list of guidelines to recognize and to shut down attacks from social engineers.

Techniques

Information Gathering:

Information Gathering is crucial to a successful attack because it provides an understanding of the target, which then creates a foundation for possible vectors of attack. Examples of Information Gathering: Conversation, Search Engines, Books, Magazines, News Reports, Background Checks, Blogs, Inside Job, Dumpster Diving, Websites that purchase information from banks, etc. Information Gathering attempts to identify the most direct route to the target.

Real Life Example: Finding out a high ranking CEO of a company used his work email for his stamp hobby collection (This small information could possibly lead a way for the social engineer to compromise the company's security system).

Prevention of Information Gathering:

Train employees on what is sensitive information and how not to reveal it. Employees should also know that work materials should stay at the designated workplace. Employees must know how to properly dispose of important documents to prevent dumpster diving. Restrict the amount of information online about the company to prevent information gathering.

Communication Modeling:

Communication modeling allows the social engineer to get a response from a person, most likely personnel of the target company, to gather specific information in order to "...decide the best method of delivery, the best method for feedback, and the best message to include" in his or her attack. Christopher Hadnagy – Social Engineering: The Art of Human Hacking.

Steps of Communication Modeling:

1. The Source: The social engineer shall be the source of communication to relay the information he or she has gathered.
2. The Channel: By first communicating, the social engineer will decide what is the best way to channel their attacks to the target, whether through email, mail, and etc.
3. The Message: With the information gathered and the best method of channeling the attack decided, the message will contain what the social engineer will say to the receiver (a.k.a. the target).
4. The Receiver: The social engineer will have to decide the best target to receive the message.
5. The Feedback: This is the desired reaction from the target where the compromise in security is successful, or sometimes, unfortunately not.

Real Life Example: The social engineer used the CEO's stamp collecting hobby as his source. Then, using three different channels which contained the message; a phone call was made to tell the CEO that the social engineer had sent an email, which contained a link to a phishing website (malicious website) disguised as a stamp collecting website. The receiver (the CEO) responded in favor to the social engineer's attack by clicking on the link and compromising the company's security; a desirable feedback.

Prevention of Communication Modeling Based Attacks:

Teach all employees to not access personal email in a company workplace or through a company computer/laptop. Properly instruct company personnel about how, why and when should they help strangers or other company employees.

Elicitation:

Elicitation is the method of drawing out a certain conclusion (behavior or truth for example) that the social engineer wants through his or her appearance, attitude, body language, and etc.

Guidelines to elicitation:

1. Be Natural: The social engineer keeps a natural demeanor by talking to the person about a subject either well known to both parties or just the social engineer. This allows for a easier chance to elicit a response from the person.
2. Educating: The social engineer will educate himself on a particular subject before initiating a conversation with the person, which will help with the natural demeanor of the social engineer. This keeps the social engineer from revealing his identity to the person.
3. Limits to greediness: The social engineer will not focus the entire conversation on getting answers and actions out of the person, rather he or she will feel out the conversation and give something that would elicit a feeling of reciprocation from the person. This avoids the target from losing interest, or feeling suspicious. Social engineers will attempt to set up further possible elicitation attacks by setting up further encounters.

Real Life Example: Using alcohol, and the guidelines for eliciting a response, the CFO of company XYZ spilled sensitive information about his company to the social engineer.

Prevention of Elicitation:

Be careful of what one says, especially while talking to a complete stranger even if they share common interests and/or seem friendly. Avoid the consumption of alcohol when one is around strangers and holding company property. Company information should only be discussed with authorized personnel, no exceptions.

Conclusions

Social Engineers, when targeting large companies through employees, have the ability to cost the company billions of dollars in damages. Through reviews of case studies on attacks by social engineers, we have unanimously decided it critical that employers and employees alike train in recognizing and properly responding to social engineering attacks.

SOCIAL ENGINEERING
SPECIALIST

Because there is no patch
for human stupidity

Acknowledgements

- Chevron
- National Science Foundation
- California State University of Bakersfield
- *****Alfonso Puga*****

- Social Engineering: The Art of Human Hacking
- Mindfulsecurity.com (Images 1-3)
- Home.mcafee.com/(Image 4)
- Zerosecurity.org (Image 5)
- Social-engineer.org/(Image 6)

Fun Facts:

-Kevin Mitnick, arguably one of the most famous social engineers, used his skills at the age of 12 to bypass the punch card system used by the public bus transit in LA, gaining the ability to ride on the buses to any location for free.

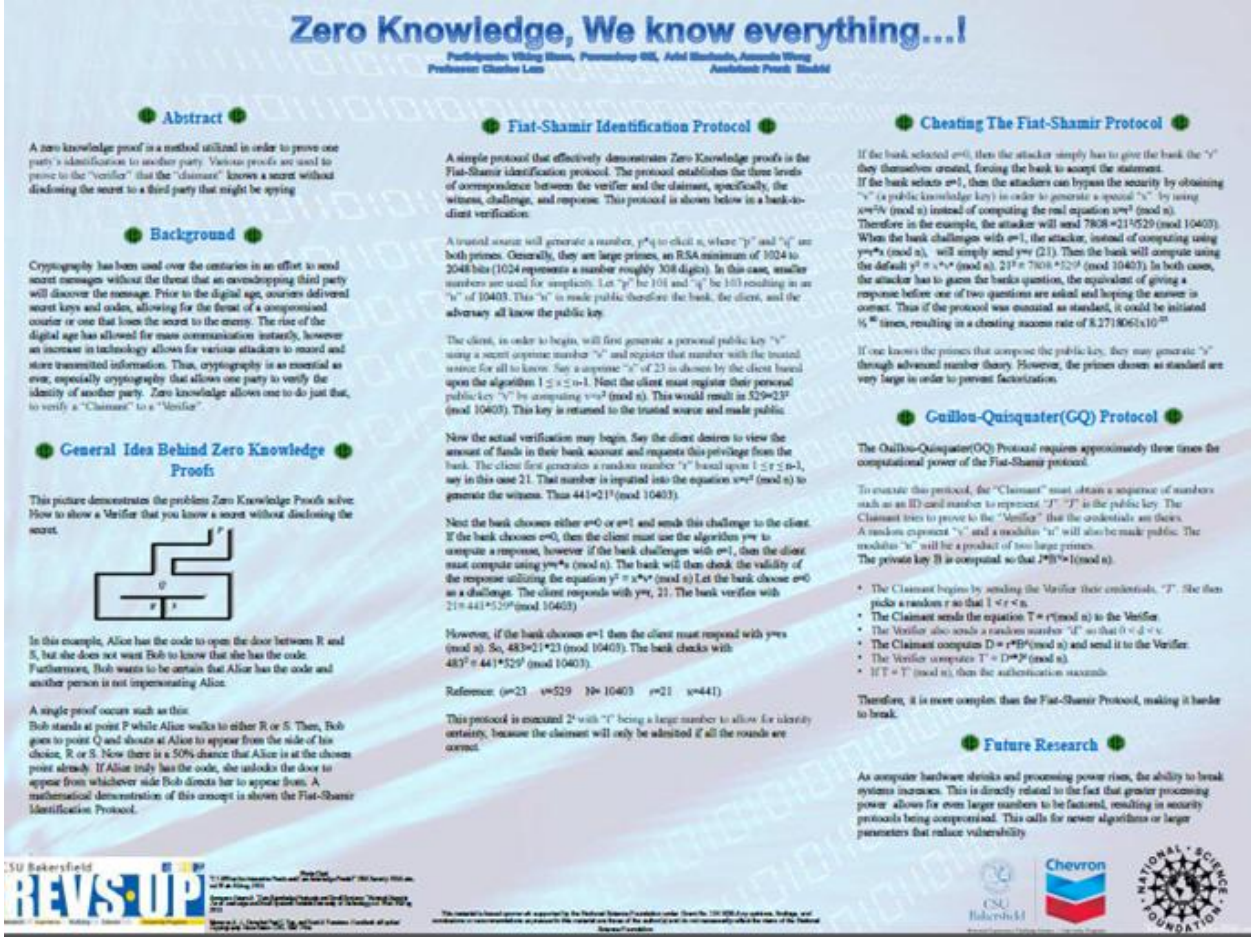
-Mitnick later used his skills to access DEC, a computer operating system manufacturer, in order to steal copies of their latest operating system; this crime made him a fugitive from the FBI for over two years.

-Common acts used by magicians, such as Penn and Teller, are closely related to social engineering principles.

-Con men typically use social engineering coupled with a technique called "Sensory Overflow," which overwhelms the target's senses by making them unable to focus on the details of a situation, thus preventing them from noticing what the con man is actually taking from them/cheating them out of, these are supplemental skills for a social engineer.

-Social Engineering is often showcased in Television shows such as the Mentalist, Lie to Me, and White Collar, and in Movies like Sherlock Holmes, Catch Me If You Can, and Sneakers.

-American Security Consultant, Frank William Abagnale Jr, was once one of the most evasive and clever social engineers of his time. He was an amazing imposter, assuming the identity of an airline pilot, a teacher, a doctor, a lawyer, and an agent of the U.S. Bureau of Prisons.



Zero Knowledge, We know everything...!

Participants: [illegible], [illegible] Gill, [illegible], Amanda Wong
Professor: Charles Lam Assistant: Frank [illegible]

Abstract

A zero knowledge proof is a method utilized in order to prove one party's identification to another party. Various proofs are used to prove to the "verifier" that the "claimant" knows a secret without disclosing the secret to a third party that might be spying

Background

Cryptography has been used over the centuries in an effort to send secret messages without the threat that an eavesdropping third party will discover the message. Prior to the digital age, couriers delivered secret keys and codes, allowing for the threat of a compromised courier or one that loses the secret to the enemy. The rise of the digital age has allowed for mass communication instantly, however an increase in technology allows for various attackers to record and store transmitted information. Thus, cryptography is as essential as ever, especially cryptography that allows one party to verify the identity of another party. Zero knowledge allows one to do just that, to verify a "Claimant" to a "Verifier".

General Idea Behind Zero Knowledge Proofs

This picture demonstrates the problem Zero Knowledge Proofs solve: How to show a Verifier that you know a secret without disclosing the secret.

In this example, Alice has the code to open the door between R and S, but she does not want Bob to know that she has the code. Furthermore, Bob wants to be certain that Alice has the code and another person is not impersonating Alice.

A single proof occurs such as this:
Bob stands at point P while Alice walks to either R or S. Then, Bob goes to point Q and shouts at Alice to appear from the side of his choice, R or S. Now there is a 50% chance that Alice is at the chosen point already. If Alice truly has the code, she unlocks the door to appear from whichever side Bob directs her to appear from. A mathematical demonstration of this concept is shown the Fiat-Shamir Identification Protocol.

Fiat-Shamir Identification Protocol

A simple protocol that effectively demonstrates Zero Knowledge proofs is the Fiat-Shamir identification protocol. The protocol establishes the three levels of correspondence between the verifier and the claimant, specifically, the witness, challenge, and response. This protocol is shown below in a bank-to-client verification.

A trusted source will generate a number, $p*q$ to elicit n, where "p" and "q" are both primes. Generally, they are large primes, an RSA minimum of 1024 to 2048 bits (1024 represents a number roughly 308 digits). In this case, smaller numbers are used for simplicity. Let "p" be 101 and "q" be 103 resulting in an "n" of 10403. This "n" is made public therefore the bank, the client, and the adversary all know the public key.

The client, in order to begin, will first generate a personal public key "v" using a secret coprime number "s" and register that number with the trusted source for all to know. Say a coprime "s" of 23 is chosen by the client based upon the algorithm $1 \leq s \leq n-1$. Next the client must register their personal public key "V" by computing $v=s^2 \pmod{n}$. This would result in $529=23^2 \pmod{10403}$. This key is returned to the trusted source and made public.

Now the actual verification may begin. Say the client desires to view the amount of funds in their bank account and requests this privilege from the bank. The client first generates a random number "r" based upon $1 \leq r \leq n-1$, say in this case 21. That number is inputted into the equation $x=r^2 \pmod{n}$ to generate the witness. Thus $441=21^2 \pmod{10403}$.

Next the bank chooses either $e=0$ or $e=1$ and sends this challenge to the client. If the bank chooses $e=0$, then the client must use the algorithm $y=r$ to compute a response, however if the bank challenges with $e=1$, then the client must compute using $y=r*s \pmod{n}$. The bank will then check the validity of the response utilizing the equation $y^2 \equiv x*v^e \pmod{n}$ Let the bank choose $e=0$ as a challenge. The client responds with $y=r$, 21. The bank verifies with $21^2 \equiv 441*529^0 \pmod{10403}$

However, if the bank chooses $e=1$ then the client must respond with $y=rs \pmod{n}$. So, $483=21*23 \pmod{10403}$. The bank checks with $483^2 \equiv 441*529^1 \pmod{10403}$.

Reference: ($s=23$ $v=529$ $N=10403$ $r=21$ $x=441$)

This protocol is executed 2^t with "t" being a large number to allow for identity certainty, because the claimant will only be admitted if all the rounds are correct.

Cheating The Fiat-Shamir Protocol

If the bank selected $e=0$, then the attacker simply has to give the bank the "r" they themselves created, forcing the bank to accept the statement.
If the bank selects $e=1$, then the attackers can bypass the security by obtaining "v" (a public knowledge key) in order to generate a special "x" by using $x=r^2/v \pmod{n}$ instead of computing the real equation $x=r^2 \pmod{n}$.
Therefore in the example, the attacker will send $7808 = 21^2/529 \pmod{10403}$.
When the bank challenges with $e=1$, the attacker, instead of computing using $y=r*s \pmod{n}$, will simply send $y=r$ (21). Then the bank will compute using the default $y^2 \equiv x*v^e \pmod{n}$. $21^2 \equiv 7808*529^1 \pmod{10403}$. In both cases, the attacker has to guess the banks question, the equivalent of giving a response before one of two questions are asked and hoping the answer is correct. Thus if the protocol was executed as standard, it could be initiated $\frac{1}{2}^{80}$ times, resulting in a cheating success rate of 8.271806×10^{-25}

If one knows the primes that compose the public key, they may generate "s" through advanced number theory. However, the primes chosen as standard are very large in order to prevent factorization.

Guillou-Quisquater(GQ) Protocol

The Guillou-Quisquater(GQ) Protocol requires approximately three times the computational power of the Fiat-Shamir protocol.

To execute this protocol, the "Claimant" must obtain a sequence of numbers such as an ID card number to represent "J". "J" is the public key. The Claimant tries to prove to the "Verifier" that the credentials are theirs.
A random exponent "v" and a modulus "n" will also be made public. The modulus "n" will be a product of two large primes.
The private key B is computed so that $J*B^v=1 \pmod{n}$.

- The Claimant begins by sending the Verifier their credentials, "J". She then picks a random r so that $1 < r < n$.
- The Claimant sends the equation $T = r^v \pmod{n}$ to the Verifier.
- The Verifier also sends a random number "d" so that $0 < d < v$.
- The Claimant computes $D = r*B^d \pmod{n}$ and send it to the Verifier.
- The Verifier computes $T' = D^v*J^d \pmod{n}$.
- If $T = T' \pmod{n}$, then the authentication succeeds.

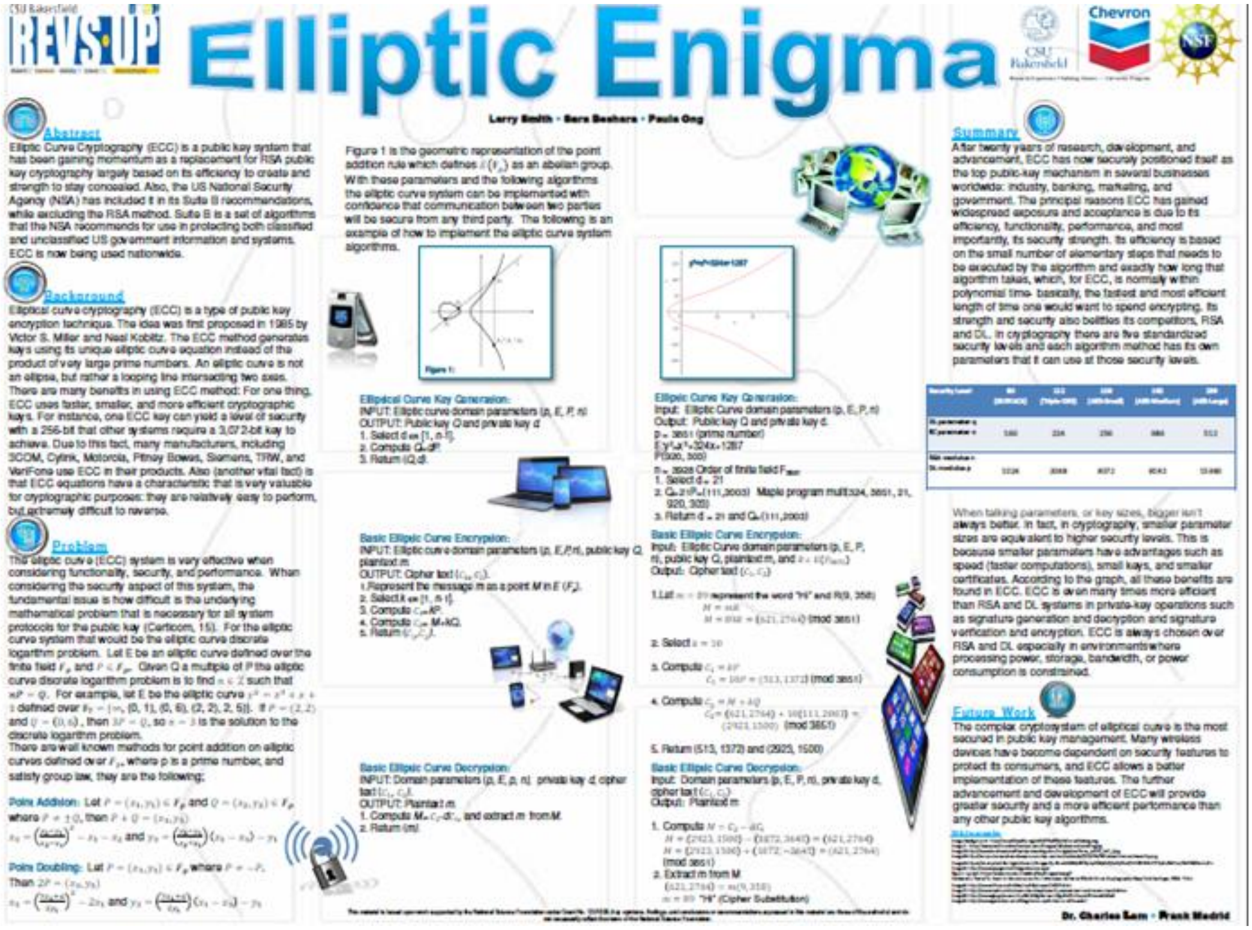
Therefore, it is more complex than the Fiat-Shamir Protocol, making it harder to break.

Future Research

As computer hardware shrinks and processing power rises, the ability to break systems increases. This is directly related to the fact that greater processing power allows for even larger numbers to be factored, resulting in security protocols being compromised. This calls for newer algorithms or larger parameters that reduce vulnerability.

[illegible]

This material is based upon work supported by the National Science Foundation under Grant No. [illegible]. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.



CSU Bakersfield REVS-UP

Elliptic Enigma

Larry Smith · Sara Beshara · Paula Ong

Abstract

Elliptic Curve Cryptography (ECC) is a public key system that has been gaining momentum as a replacement for RSA public key cryptography largely based on its efficiency to create and strength to stay concealed. Also, the US National Security Agency (NSA) has included it in its Suite B recommendations, while excluding the RSA method. Suite B is a set of algorithms that the NSA recommends for use in protecting both classified and unclassified US government information and systems. ECC is now being used nationwide.

Background

Elliptical curve cryptography (ECC) is a type of public key encryption technique. The idea was first proposed in 1985 by Victor S. Miller and Neal Koblitz. The ECC method generates keys using its unique elliptic curve equation instead of the product of very large prime numbers. An elliptic curve is not an ellipse, but rather a looping line intersecting two axes. There are many benefits in using ECC method: For one thing, ECC uses faster, smaller, and more efficient cryptographic keys. For instance, one ECC key can yield a level of security with a 256-bit that other systems require a 3,072-bit key to achieve. Due to this fact, many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone use ECC in their products. Also (another vital fact) is that ECC equations have a characteristic that is very valuable for cryptographic purposes: they are relatively easy to perform, but extremely difficult to reverse.

Problem

The elliptic curve (ECC) system is very effective when considering functionality, security, and performance. When considering the security aspect of this system, the fundamental issue is how difficult is the underlying mathematical problem that is necessary for all system protocols for the public key (Certicom, 15). For the elliptic curve system that would be the elliptic curve discrete logarithm problem. Let E be an elliptic curve defined over the finite field F_p and $P \in F_p$. Given Q a multiple of P the elliptic curve discrete logarithm problem is to find $n \in \mathbb{Z}$ such that $nP = Q$. For example, let E be the elliptic curve $y^2 = x^3 + x + 1$ defined over $F_7 = \{\infty, (0,1), (0,6), (2,2), (2,5)\}$. If $P = (2,2)$ and $Q = (0,6)$, then $3P = Q$, so $n = 3$ is the solution to the discrete logarithm problem.

There are well known methods for point addition on elliptic curves defined over F_p, where p is a prime number, and satisfy group law, they are the following:

Point Addition: Let $P = (x_1, y_1) \in F_p$ and $Q = (x_2, y_2) \in F_p$ where $P \neq \pm Q$, then $P + Q = (x_3, y_3)$

$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$ and $y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$

Point Doubling: Let $P = (x_1, y_1) \in F_p$ where $P \neq -P$. Then $2P = (x_3, y_3)$

$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$ and $y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$

Figure 1 is the geometric representation of the point addition rule which defines $E(F_p)$ as an abelian group. With these parameters and the following algorithms the elliptic curve system can be implemented with confidence that communication between two parties will be secure from any third party. The following is an example of how to implement the elliptic curve system algorithms.

Figure 1:

Elliptical Curve Key Generation:

```
INPUT: Elliptic curve domain parameters (p, E, P, n)
OUTPUT: Public key Q and private key d
1. Select d ∈ [1, n−1].
2. Compute Q=dP.
3. Return (Q,d).
```

Basic Elliptic Curve Encryption:

```
INPUT: Elliptic curve domain parameters (p, E,P,n), public key Q, plaintext m
OUTPUT: Cipher text (c1, c2).
1.Represent the message m as a point M in E (Fp).
2. Select k ∈ [1, n−1].
3. Compute c1= kP.
4. Compute c2= M+kQ.
5. Return (c1,c2).
```

Basic Elliptic Curve Decryption:

```
INPUT: Domain parameters (p, E, p, n), private key d, cipher text (c1, c2).
OUTPUT: Plaintext m
1. Compute M= c2−dc1, and extract m from M.
2. Return (m)
```

Elliptic Curve Key Generation:

```
Input: Elliptic Curve domain parameters (p, E, P, n)
Output: Public key Q and private key d.
p = 3851 (prime number)
E:y^2=x^3+324x+1287
P(920, 303)
n = 3928 Order of finite field F_3851
1. Select d = 21
2. Q=21P=(111,2003)  Maple program mult(324, 3851, 21, 920, 303)
3. Return d = 21 and Q=(111,2003)
```

Basic Elliptic Curve Encryption:

```
Input: Elliptic Curve domain parameters (p, E, P, n), public key Q, plaintext m, and k ∈ Z(F_3851)
Output: Cipher text (c1, c2)
1.Let m = 89 represent the word "Hi" and R(9, 358)
      M = mR
      M = 89R = (621, 2764) (mod 3851)
2. Select k = 10
3. Compute c1 = kP
      c1 = 10P = (513, 1372) (mod 3851)
4. Compute c2 = M + kQ
      c2 = (621,2764) + 10(111,2003) =
           (2923,1500) (mod 3851)
5. Return (513, 1372) and (2925, 1500)
```

Basic Elliptic Curve Decryption:

```
Input: Domain parameters (p, E, P, n), private key d, cipher text (c1, c2)
Output: Plaintext m
1. Compute M = c2 − dc1
   M = (2923,1500) − (1872,3640) = (621,2764)
   M = (2923,1500) + (1872,−3640) = (621,2764)
   (mod 3851)
2. Extract m from M
   (621,2764) = m(9,358)
   m = 89 "Hi" (Cipher Substitution)
```

Summary

After twenty years of research, development, and advancement, ECC has now securely positioned itself as the top public-key mechanism in several businesses worldwide: industry, banking, marketing, and government. The principal reasons ECC has gained widespread exposure and acceptance is due to its efficiency, functionality, performance, and most importantly, its security strength. Its efficiency is based on the small number of elementary steps that needs to be executed by the algorithm and exactly how long that algorithm takes, which, for ECC, is normally within polynomial time- basically, the fastest and most efficient length of time one would want to spend encrypting. Its strength and security also belittles its competitors, RSA and DL. In cryptography there are five standardized security levels and each algorithm method has its own parameters that it can use at those security levels.

Security Level	80 (SKIPJACK)	112 (Triple-DES)	128 (AES-Small)	192 (AES-Medium)	256 (AES-Large)
EC parameter q EC parameter n	160	224	256	384	512
RSA modulus n DL modulus p	1024	2048	3072	8192	15360

When talking parameters, or key sizes, bigger isn't always better. In fact, in cryptography, smaller parameter sizes are equivalent to higher security levels. This is because smaller parameters have advantages such as speed (faster computations), small keys, and smaller certificates. According to the graph, all these benefits are found in ECC. ECC is even many times more efficient than RSA and DL systems in private-key operations such as signature generation and decryption and signature verification and encryption. ECC is always chosen over RSA and DL especially in environments where processing power, storage, bandwidth, or power consumption is constrained.

Future Work

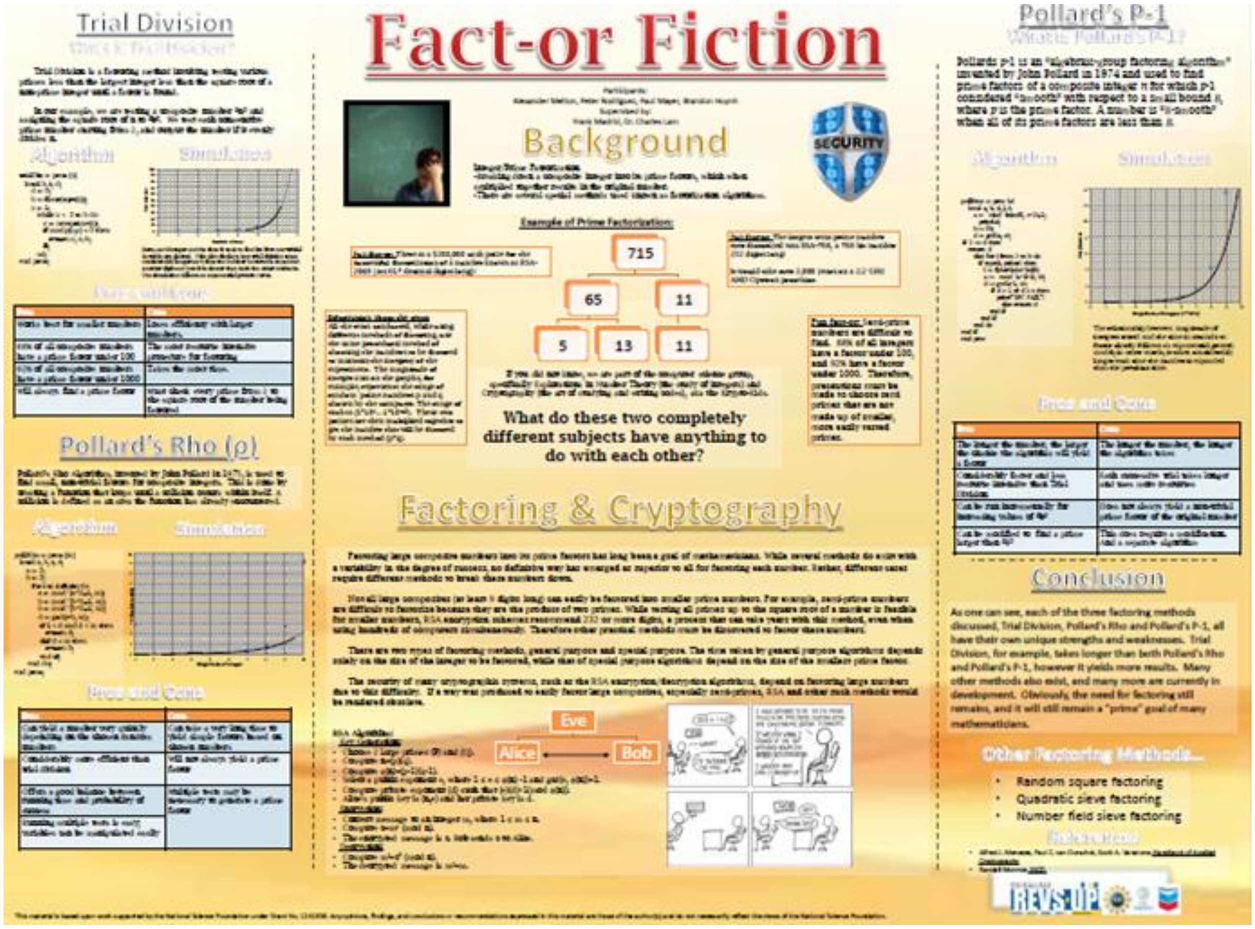
The complex cryptosystem of elliptical curve is the most secured in public key management. Many wireless devices have become dependent on security features to protect its consumers, and ECC allows a better implementation of these features. The further advancement and development of ECC will provide greater security and a more efficient performance than any other public key algorithms.

Bibliography

[illegible]

This material is based upon work supported by the National Science Foundation under Grant No. [illegible]. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Dr. Charles Lam · Frank Madrid



Fact-or Fiction

Participants: [illegible]
Supervised by: [illegible]

Background

Integer Prime Factorization
-[illegible] a composite integer into its prime factors, which when multiplied together results in the original number.
-There are several special methods used known as factorization algorithms.

Example of Prime Factorization:

715
65 11
5 13 11

[illegible]

Fun Fact: Semi-prime numbers are difficult to find. 88% of all integers have a factor under 100, and 92% have a factor under 1000. Therefore, precautions must be made to choose semi primes that are not made up of smaller, more easily varied primes.

If you did not know, we are part of the integrated [illegible] group, specifically [illegible] in Number Theory (the study of integers) and Cryptography (the art of creating and writing codes), aka the Crypto-Kids.

What do these two completely different subjects have anything to do with each other?

Trial Division

What is Trial Division?

Trial Division is a factoring method involving testing various primes less than the largest integer less than the square root of a composite integer until a factor is found.

In our example, we are testing a composite number 'N' and [illegible] the square root of it as 'M'. We test each consecutive prime number starting from 2, and output the number if it evenly divides N.

Algorithm

```
[illegible]
```

Simulation

[illegible]

Pros and Cons

Pros	Cons
Works best for smaller numbers	Loses efficiency with larger numbers.
88% of all composite numbers have a prime factor under 100	The most tedious iterative procedure for factoring
92% of all composite numbers have a prime factor under 1000	Takes the most time.
Will always find a prime factor	Must check every prime from 2 to the square root of the number being factored

Pollard's Rho (ρ)

Pollard's Rho algorithm, invented by John Pollard in 1975, is used to find small, non-trivial factors for composite integers. This is done by creating a function that loops until a collision occurs, within itself; a collision is defined as an [illegible] the function has already encountered.

Algorithm

```
[illegible]
```

Simulation

Pros and Cons

Pros	Cons
Can yield a number very quickly depending on the chosen number	Can take a very long time to yield single factors based on chosen numbers
Considerably more efficient than trial division	Will not always yield a prime factor
Offers a good balance between running time and probability of success	Multiple tests may be necessary to generate a prime factor
Running multiple tests is easy; variables can be manipulated easily	

Factoring & Cryptography

Factoring large composite numbers into its prime factors has long been a goal of mathematicians. While several methods do exist with a variability in the degree of success, no definitive way has emerged as superior to all for factoring each number. Rather, different cases require different methods to break these numbers down.

Not all large composites (at least [illegible] digits long) can easily be factored into smaller prime numbers. For example, semi-prime numbers are difficult to factorize because they are the product of two primes. While testing all primes up to the square root of a number is feasible for smaller numbers, RSA encryption schemes recommend 232 or more digits, a process that can take years with this method, even when using hundreds of computers simultaneously. Therefore other practical methods must be discovered to factor these numbers.

There are two types of factoring methods, general purpose and special purpose. The time taken by general purpose algorithms depends solely on the size of the integer to be factored, while that of special purpose algorithms depend on the size of the smallest prime factor.

The security of many cryptographic systems, such as the RSA encryption/decryption algorithms, depend on factoring large numbers due to this difficulty. If a way was produced to easily factor large composites, especially semi-primes, RSA and other such methods would be rendered obsolete.

RSA Algorithm:
Key Generation
- Choose 2 large primes (P) and (Q).
- Compute n=(p)(q).
- Compute [illegible]
- Select a public exponent e, where 1 < e < [illegible] and gcd(e, [illegible])=1.
- Compute private exponent (d) such that [illegible]
- Alice's public key is (n,e) and her private key is d.

Encryption
- Convert message to an integer m, where 1 ≤ m ≤ n.
- Compute $c = m^e$ (mod n).
- The encrypted message is c, [illegible]

Decryption
- Compute $m = c^d$ (mod n).
- The decrypted message is m.

Eve
Alice ⟷ Bob

Pollard's P-1

What is Pollard's P-1?

Pollards p-1 is an "algebraic-group factoring algorithm" invented by John Pollard in 1974 and used to find prime factors of a composite integer n for which p-1 considered "smooth" with respect to a small bound B, where p is the prime factor. A number is "B-smooth" when all of its prime factors are less than B.

Algorithm

```
[illegible]
```

Simulation

[illegible]

Pros and Cons

Pros	Cons
The larger the number, the larger the chance the algorithm will yield a factor	The larger the number, the longer the algorithm takes
Considerably faster and less iterative than Trial Division	[illegible]
Can be run incrementally for increasing values of 'B'	Does not always yield a non-trivial prime factor of the original number
Can be modified to find a prime larger than 'B'	This does require a modification and a separate algorithm

Conclusion

As one can see, each of the three factoring methods discussed, Trial Division, Pollard's Rho and Pollard's P-1, all have their own unique strengths and weaknesses. Trial Division, for example, takes longer than both Pollard's Rho and Pollard's P-1, however it yields more results. Many other methods also exist, and many more are currently in development. Obviously, the need for factoring still remains, and it will still remain a "prime" goal of many mathematicians.

Other Factoring Methods...

- Random square factoring
- Quadratic sieve factoring
- Number field sieve factoring

References

- Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography
- [illegible]

This material is based upon work supported by the National Science Foundation under Grant No. [illegible]. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.