



**Models for Information Assurance Education and Outreach:
Year 3 and Summative Report***

Jianjun Wang

School of Social Sciences and Education

California State University, Bakersfield

September 30, 2015

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

Abstract

Over the past three years, California State University, Bakersfield received NSF funding to support hands-on explorations in *network security* and *cryptography* through Research Experience Vitalizing Science -University Program (REVS-UP). In addition to the summer bridge component, the grant included development of *Multidisciplinary Information Assurance Curriculum* at the undergraduate level and offered Information Assurance (IA) education for community members. In this summative report, a Results-Based Accountability (RBA) model is employed to examine six research questions: (1) How much has been done in the delivery of REVS-UP learning opportunities for high school students during the four-week summer sessions? (2) What strengths did the project demonstrate to support IA education? (3) What is the program impact on key stakeholders? (4) How much has been done through the Dissemination Workshop for K-12 teachers? (5) How well did the program perform in the service delivery? (6) Is anyone better off due to this outreach effort? To sustain the program improvement, qualitative and quantitative data are triangulated to assess *what works, for whom, and in which context* under a Context, Input, Process, and Product (CIPP) paradigm. The report concludes with a *Future Direction* section to examine the program setting on the REVS-UP platform.

**Models for Information Assurance Education and Outreach:
Year 3 and Summative Report**

Table of Content

Abstract	2
Literature Review	6
Research Questions	9
Evaluation Findings	10
Future Direction	24
References	28
Appendix 1: Poster Presentations of Four IA Research Projects	30

**Models for Information Assurance Education and Outreach:
Year 3 and Summative Report**

As the society rushes to embrace technology development in cyberspace, demands on Information Assurance (IA) education have been strengthened to cope with network safety and computer vulnerability. With three-year funding from NSF, “Models for Information Assurance Education and Outreach” (MIAEO) is designed to combine *research exploration*, *community outreach*, and *program development* for key stakeholders of IA education. The first two components involve high school students, K-12 teachers, and community members to strengthen capacity building in the general public. The third component represents an innovative approach within California State University, Bakersfield (CSUB) to develop a broad-based, hands-on IA curriculum beyond existing programs in *Computer Science*, *Mathematics*, and *Global Intelligence and National Security*. Altogether MIAEO has addressed dual foci of the *CyberCorps: Scholarship for Service* program, i.e., support cybersecurity education and workforce development (NSF, 2014).

Evaluation reports for first two years of the grant operation have been reviewed and disseminated by the Education Resource Information Center of U.S. Department of Education (<http://files.eric.ed.gov/fulltext/ED545559.pdf> & <http://files.eric.ed.gov/fulltext/ED546861.pdf>). During the third year, three adjustments have been made in MIAEO to adapt to contextual changes within the local setting:

1. The *research exploration* component used to include both high school students and K-12 teachers under a platform of Research Experience Vitalizing Sciences - University Program (REVS-UP). In addition to IA education, REVS-UP concurrently uses funding from the Chevron Cooperation to support hands-on, research explorations in other STEM

fields. Due to decrease of the Chevron funding, no K-12 teachers were invited to participate in REVS-UP in 2015. To conform to this REVS-UP adjustment, the IRB protocol for MIAEO has been revised to eliminate teacher data collection from the four-week summer session.

2. The *community outreach* component was expanded using the budget surplus from scaling down the REVS-UP operation. In 2014, a total of 22 community members took part in a Dissemination Workshop. In 2015, the attendee pool was expanded to 30, including 15 teachers from last year and 15 new teachers this year. Additional data are gathered from teachers to assess the workshop impact on enhancement of IA education in K-12 school settings.
3. The *program development* component was initiated in the first year, and has completed curriculum approval in the second year. Meanwhile, new Knowledge Units were stipulated by the National Security Agency and Department of Homeland Security (2013) for *Centers of Academic Excellence in Cyber Defense/Information Assurance Education* (CAE-CD). In preparing for CSUB transition to a semester system in 2016, minor revisions are needed in 2015 to strengthen curriculum alignment with the new Knowledge Units for CAE-CD.

While the *program development* component is pending on the upcoming transition to a semester system, this summative report primarily addresses the first two components of MIAEO that have added outcome data in the third year. In this final evaluation report, assessment of program effectiveness is not only grounded on a review of the aggregated results from the past evidence, but also supported by analyses of new empirical data that have never been released before.

Literature Review

Although summative reports are expected to justify accountability of program funding, Tom Angelo (1999), former director of the national assessment forum, maintained, “Though accountability matters, learning still matters most” (¶. 1). In this regard, Sloane (2008) advocated that “We change the basic research question from what works to what works for whom and in what contexts” (p. 43). Instead of delimiting the evaluation effort on “what works”, a Context, Input, Process, and Product (CIPP) paradigm is adopted in this report to sustain the mechanism of program learning.

Researchers noted that “The CIPP evaluation model belongs in the improvement/accountability category” (Zhang et al. 2011, p. 59). It was initially conceptualized in the mid-1960s for evaluating federal grants (see Stufflebeam, 1983). This theoretical framework matured during development of national evaluation standards over the past four decades (Program Evaluation Standards, 2010). The standards have been approved by the American National Standards Institute (ANSI) and sponsored by 17 North American professional organizations (Yarbrough, Shulha, Hopson, & Caruthers, 2010). In this section, literature review is guided on the CIPP platform to support evaluation of the MIAEO program.

It was highlighted in the MIAEO proposal that “California State University, Bakersfield (CSUB) has made great strides in improving educational opportunities for underrepresented minorities and women” (see Project Summary for Grant No. DUE – 1241636). In this service region, Bakersfield has surpassed the population size of well-known cities like St. Louis and Kern County covers a land area as large as the state of New Jersey (Wang, 2014). More importantly, Kern County has been ranked as one of the lowest regions in adult education across the United States (Brookings Institution, 2010), and Bakersfield was ranked as one of the least

educated metropolitan areas in the nation (Zumbrun, 2008). CSUB is the only public university within a radius of two-hour driving in all directions. Hence, community outreach plays an important role in enhancing IA education under this *context*.

Below the college level, two schools from Kern County were ranked among the worst 10 schools in California (see <http://www.schooldigger.com/go/CA/schoolrank.aspx?pagetype=bottom10>). Studies across the nation confirmed strong needs to strengthen learning experiences in STEM education, particularly at high-needs schools (National Center for Educational Statistics, 2006). MIAEO offered concurrent enrollments for high school students to conduct hands-on research in the IA fields during a four-week summer session. The early engagement has demonstrated potential to support school-to-college transition. As Pittaoulis (2012) noted, "it is understandable that a sense that college is 'the logical' or 'next step' after high school may develop" (p. 107). Thus, another outcome measure of MIAEO is reflected by the enhancement of individual commitment to higher education.

The local context inevitably impacts development of student attributes toward STEM education. Bottia et al. (2015) revealed that "STEM experiences of inspiration/reinforcement/preparation during high school interact with demographic variables to moderate students' interest in STEM" (p. 1). As a new field, IA education is closely related to the reinforcement of STEM inspiration (Portman, 2006). Hence, consideration has been given to the *input* factor as indicated by student demographic backgrounds at the program entry.

To enhance the equity of school-based learning, a new challenge is to attract more students, particularly females, in STEM fields. After entering the 21st century, the National Women's Law Center (2005) reported that "more than 30 years after Congress outlawed sex discrimination in education, the gender divide in career and technical education (CTE) has

narrowed barely at all" (p. 2). While MIAEO was designed to guide student pursuit of careers in IA fields, it was acknowledged in the research literature that "Computing has one of the worst gender representations of any STEM discipline" (Robelen, 2012, p. 17).

Despite its persistency, the gender gap can be altered through an education *process*. At the high school stage, "College major choices are often made during freshman or sophomore year" (Pittaoulis, 2012, p. 238). The timing also overlaps with a typical transition of student cognitive development from a concrete operational level to a formal operational level (Neo-Piagetian Theories of Development, 2009). The inquiry-based learning often involved "if ... then ..." inference and can facilitate the cognitive development. Since the Piagetian theory is not gender-specific, Legewie and DiPrete (2014) asserted that "these actual [learning] experiences will offset prior beliefs about gender differences and reduce the gender gap in interest and plans to study STEM fields in college" (p. 262).

As MIAEO adds new lab-based learning opportunities, it is anticipated in the *product* phase that "The training provided by REVS-UP will lay the foundation for academic and career interest in information assurance at the high school level" (see Project Summary for Grant No. DUE – 1241636). Nonetheless, student preparation is inseparable from teacher training (Robelen, 2012). Liou, Kirchhoff, and Lawrenz (2010) observed that "students in high need schools are much more likely to be taught by unqualified teachers" (p. 453). In the field of IA education, few teachers were fully prepared from their credential programs. Hence, MIAEO includes learning experiences for teachers through a process of developing and delivering Dissemination Workshops.

In summary, MIAEO not only engages high school students in IA explorations, but also supports teachers to "disseminate the [IA] ideas back to their classes during the school year"

(Project Summary for Grant No. DUE – 1241636). Following the CIPP paradigm, student and school information is incorporated in this report to examine MIAEO outcomes from the process of service delivery in both REVS-UP inquiries and community outreach activities.

Research Questions

Since publication of a well-known book, “Trying Hard Is Not Good Enough” (Friedman, 2006), a model of Results-Based Accountability (RBA) has gained popularity in the field of program evaluation. Friedman (2009) noted that “The RBA framework has been used in over 40 states and countries around the world” (p. 1). In particular, RBA is practical, asking three simple questions to get the most important performance measures: (1) How much did we do? (2) How well did we do it? (3) Is anyone better off? (see <http://resultsleadership.org/what-is-results-based-accountability-rba/>).

Following the RBA model, parallel questions have been adduced in this report to evaluate the *REVS-UP* and *community outreach* components of MIAEO:

REVS-UP

1. How much has been done in the delivery of REVS-UP learning opportunities for high school students during a four-week summer session?
2. What strengths did the MIAEO component demonstrate in IA education?
3. What is the impact of this summer bridge program on key stakeholders?

Community Outreach

4. How much has been done through the Dissemination Workshop to support IA education for K-12 teachers?
5. How well did the program perform in service delivery?
6. Is anyone better off due to this outreach effort?

According Miklas (2014), the RBA model and the CIPP paradigm extend mutual reinforcement to address both aspects of *funding accountability* and *program improvement*. From the RBA perspective, Miklas (2014) proposed a formula, “Result = A Population + Geographic Area + Condition of Well Being” (p. 17), to illustrate the articulation of Context (geographic area), Input (population features), Process (condition of wellbeing), and Product (program results) under the CIPP paradigm. The alignment ensures literature-based support for addressing the six RBA-stipulated questions in evaluation results.

Evaluation Findings

To facilitate result tracking in this report, evaluation findings are categorized sequentially in this section to match six research questions on page 9.

1. How much has been done in the delivery of REVS-UP learning opportunities for high school students during a four-week summer session?

At end of the third year, a total of four university student assistants, four K-12 teachers, and 51 high school students participated in development of 14 IA research projects under the leadership of two CSUB professors. The involvement of university student assistants not only supported the lab-based inquiries, but also introduced role models for high school students to pursue IA education.

Although participation of K-12 teachers was discontinued in the third year due to changes at the REVS-UP side, the evaluator had a chance to interviews past teacher participants. One mathematics teacher indicated a teaching module he developed from the REVS-UP experience to expand student learning opportunities at a local high school. Another teacher guided past students in her science classes to pursue professional careers in IA fields. The REVS-UP

activities have supported both curriculum development and student advising in high school settings.

As part of the REVS-UP offerings at CSUB, the P.I. and Co-P.I. worked with two cohorts of students each year to conduct hands-on research in *Computer/Network Security* and *Cryptography*. Descriptions of the IA exploration were posted online:

1. Explorations in Network Security and Vulnerability Analysis

Advisor: Dr. Melissa Danforth

This program focuses on several issues within information assurance and computer security. Basic topics will be discussed and the students will conduct introductory simulations and experiments relating to the topics. This year will focus on digital forensics and incident response, with topics such as investigating computer systems, analyzing disk images, analyzing network data, recovery, and response. Key focus will be paid to professional ethics and legal uses of security tools.
(see <https://www.csub.edu/revsup/Computer%20Science/index.html>)

2. Explorations in Number Theory and Cryptography

Advisor: Dr. Charles Lam

This program explores the evolution of cryptology from simple substitution ciphers to public-key cryptography. Students will be introduced to basic number theory, and its use in modern-day encryption methods. In addition, different uses of cryptography in cases such as authentication and digital signatures will be explored. Participants will investigate on weaknesses in encryption schemes using basic cryptanalysis techniques.
(see <https://www.csub.edu/revsup/Mathematics/index.html>)

Within each week, lectures and lab activities were included in a daily agenda:

Week 1: Lecture for 1-2 hours in the morning, hands-on activities the rest of the day (Day 1: getting used to the computer systems, Days 2-3: introducing projects, Days 3-4: splitting into project groups)

Week 2: Talk about major cybersecurity compromises for an hour in the morning, break into sub-groups to work on projects for the rest of the day

Week 3: Talk for 1-2 hours in the morning, including an overview of cybersecurity careers; projects for the rest of the day. The afternoon of Day 4 they start to work on their project posters

Week 4: Days 1-2 are all about the project posters, Day 3 is movies/documentaries about cybersecurity and poster presentation prep, Day 4 includes a cybersecurity movie and poster presentations

Table 1 shows the Scope of Work (SOW) for the two REVS-UP research teams.

Table 1: SOW for Two Tracks of Cyber Security Projects

	Week 1	Week 2	Week 3	Week 4
Cryptography	Simple Substitution Cipher, Polyalphabetic Substitution Cipher, Euclidean Algorithm, Modular Arithmetic, Worksheets on Topics	Fermat's Little Theorem, Modular Exponentiation Algorithm, RSA Encryption Algorithm and Proof, Worksheets on Topics	Hands-on Activities, including Programming and Experimentation	Prepare Poster on Hands-on Activities
Computer/ Network Security	Ethics and Legality, Security Concepts, Authentication Protocols, Password Hashing and Cracking, Using Linux, Hands-on Activities	Password Practices, Secure Authentication Protocols, TCP/IP Networking, Network Attacks, Social Engineering, Hands-on Activities	Malware, Access Control, Protecting Information, "Best Practices" for Security, More on Social Engineering, Hands-on Activities	Prepare Poster on Hands-on Activities, Watch Videos on Recent Security Topics (e.g. SmartTV hack, DefCon, etc.)

Source: <https://www.usenix.org/system/files/conference/cset14/cset14-paper-danforth.pdf>

In summary, the REVS-UP component has been systematically designed to expand IA learning opportunities for high school students during a four-week summer session. The mechanism was delineated by SOW each week, as well as daily lectures and lab explorations within a week. The lecture part was designed to conform to professional practice, and the lab activities supported hands-on explorations to fulfill an IA research agenda.

2. What strengths did the MIAEO component demonstrate in IA education?

In this summative report, strengths of MIAEO are reflected in both *process* and *product* phases of the service delivery. From the process perspective, MIAEO supports network development for students across a dozen high schools. The school background information has

been gathered from well-established resources, such as <http://www.greatschools.org> and <http://www.schooldigger.com>. The information triangulation is needed because not all schools have their performance data available at multiple web sites. For instance, private schools are not ranked according to state test scores. Thus, local community ratings are needed to assess school status. Network plots for the first two years were presented in the 2013 and 2014 annual reports (Wang, 2013; 2014). Table 2 shows the network of students across *gender*, *ethnic*, *grade level*, and *school rank* dimensions in the third year. According to Hanson, Guilfooy, and Pillai (2009), social networking is an effective approach to break gender and ethnicity barriers. The involvement of students at different grade levels also supports heterogeneity of the participant grouping for cooperative learning (Dotson, 2011).

Table 2: Network Attributes of REVS-UP Participants

School Rank*	Network of School Affiliation		Legend
	Minority	Non-Minority	
8			<p>Node Color: Pink=Female Blue=Male</p> <p>Node Shape: Up-triangle=Sophomore Diamond=Junior Down-triangle=Senior</p> <p>Student nodes are aligned in columns according to ethnic status;</p> <p>School nodes are clustered by ratings from greatschools.com that place the best schools in Rank 10 and the worst schools in Rank 1</p>
6			
5			

*The school ranks were anchored by information from greatschools.org.

Across three years, Table 3 shows a trend comparison on gender, ethnicity, and median school ranks of REVS-UP participants. Consent has been obtained to support the multiyear data collection from 17 students in 2013, 16 students in 2014, and 12 students in 2015.

The trend results show more of effort of MIAEO to engage students from schools with a lower median rank (see Table 3). In the third year, a student reported that “I want to experience in collaborating with other individuals to fulfill the project goal to research.” Another student concurred that “I expect to learn different types of mathematic problems and work with other people.” The results supported Harwood’s (2011) observation, i.e., *academic isolation of adolescents* was a primary issue of high-needs schools.

Qualitative data also indicated more positive student comments on the networking part, such as “I liked working with others to solve the codes”, “All the time spent together with teens from other schools”, and “Meeting new people and knowing they have the same interest.” Hence, an important strength of REVS-UP hinges on the opportunity of networking beyond the boundary of a specific high school.

Table 3: Background of REVS-UP Student Participants across Three Years

Context Factors	2013	2014	2015
Proportion of female students	47.06	47.06	33.33
Proportion of minority students	0.84	0.78	0.67
Median of school ranking*	8	8	5.5

*School rankings are based on information from greatschools.org.

In the product phase, quality of poster presentations is another indicator of REVS-UP strength. Contents of the first 10 presentations from 2013 and 2014 were examined in the first two annual evaluation reports (Wang, 2013; 2014). In the third year, four new projects have been completed through IA research explorations (Table 4). In the first project, students examined an electronic payment scheme that had potential to become currency of the future for

transactions among three key stakeholders, i.e., trusted third party, merchant, and customer. Benefits and drawbacks were investigated along with implementation of RSA-based encryptions. In the second project, complexity of Enigma was disentangled by a thorough analysis of possible configurations from a combination of different rotors, sequences, initial positions and plug boards for information exchanges. In the third project, students had a chance to investigate a “Digital Crime Scenes” project. Different tools, such as *virtual machines*, *live CDs*, *Sleuthkit*, *WinHex*, *grep*, and *gcore*, were introduced during the hands-on explorations to access protected data, recover corrupted or deleted documents, and view otherwise unreadable files. In addition, students learned to hide a message, image, or video within the code of another file through a steganography process. In the fourth project, students learned to input passwords into a hashing algorithm to disguise them from attackers. Built on the four-week summer training, students were able to crack approximate 60% of the password hashes. The poster presentations are included in Appendix 1 to show a broad spectrum of IA inquires. It is clear that students have gained learning experiences that are not otherwise available from the existing high school curriculum.

Table 4: Poster Presentations from the REVS-UP Component of MIAEO

2013	2014	2015
1. Crack Me If You Can: Using GPU Machines to Crack Passwords	1. Network Scanning	1. E-cash: The Transition to Paperless Currency
2. Defense Against Human Hacking	2. Bitcoin and the SHA-256 Hashing Function	2. The Enigma Machine
3. Zero Knowledge, We Know Everything!	3. Integer Factorization Problem: An Attack on the RSA Public-Key Encryption Scheme	3. Digital Crime Scenes
4. Elliptic Enigma	4. How Secure is Your Password? GPU Password Cracking	4. Cracking Password Hashes
5. Factor Fiction	5. Hacking the Human Element	

While intellectual merits have been maintained in these REVS-UP projects, it is worth noting the decrease of median school ranking in the third year (see Table 3). Despite the involvement of more students from high-needs schools, students were well-engaged in the learning process, and unanimously decided to recommend this program in 2015 (Figure 1). The networking could have contributed to the development of student consensus.

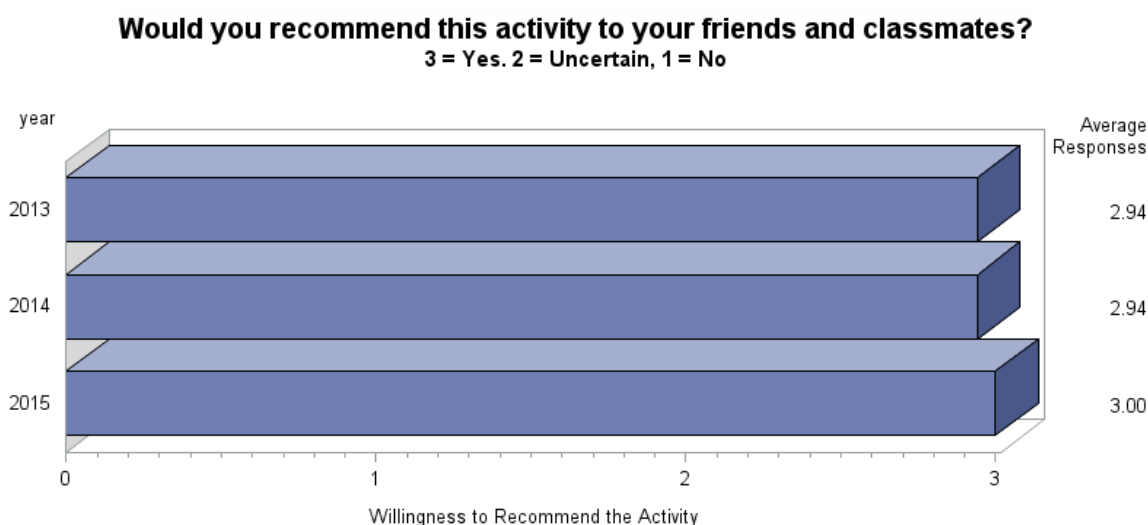


Figure 1. Trend of Program Recommendation from REVS-UP Participants.

3. What is the impact of this summer bridge program on key stakeholders?

Without involvement of K-12 teachers in the third year, key beneficiaries of REVS-UP have been delimited to high school students and university student assistants. Selection of high school students was handled by a REVS-UP panel that supported the four-week summer training since 2007. The track record has demonstrated consistent inclusion of quality candidates with GPA above 3.5.

Prior to the REVS-UP session, students had a chance to indicate their agreement to a statement, “I am interested in cryptography”. The outcome was measured on a five-point scale (1=strongly disagree, ... 5=strongly agree). Although more students came from high-needs

schools in the third year, the interest level did not drop in comparison to the result from the second year (Figure 2). More importantly, the gender gap was narrowed to almost zero, which fit MIAEO's objective of eliminating disparity of student interest (see Project Summary for Grant No. DUE – 1241636). In Figure 2, it should be noted that the higher interest in 2013 was largely expected because MIAEO was treated as a new offering. A female student confirmed the *new program* impression in her 2013 survey responses.

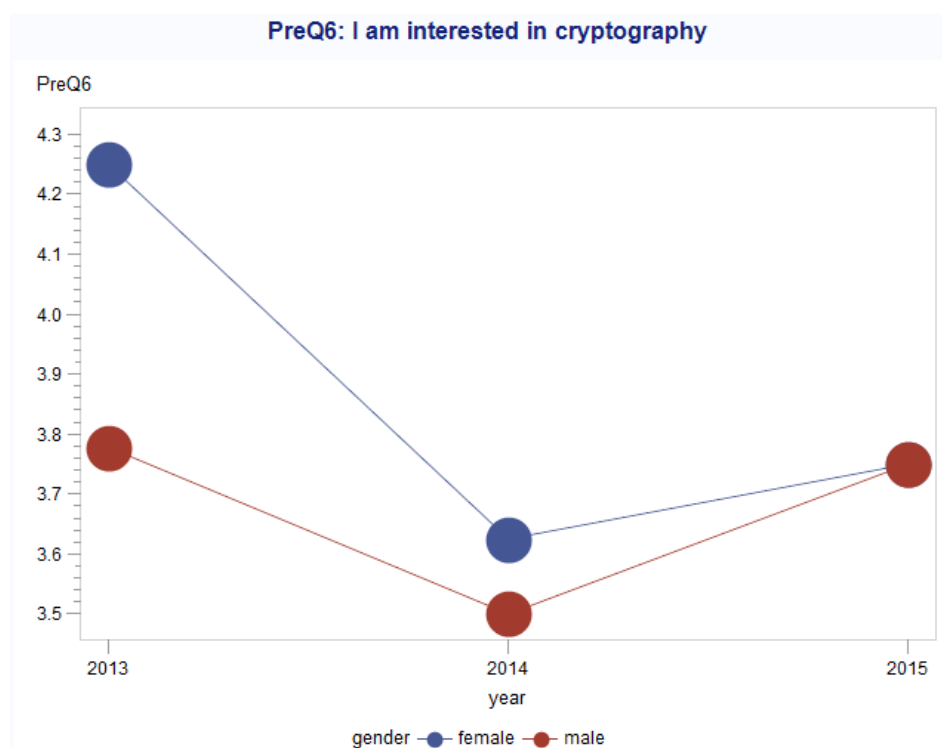


Figure 2. Trend of Student Interest in Cryptography

The impact of MIAEO is further indicated by more assessment data from the third year. Figure 3 shows that students become more interested in attending college, cryptography, and cyber security due to the program impact.

While high school students remain at an initial stage to develop academic interest, the four university student assistants have already entered the IA pipeline for professional training.

With MIAEO funding from NSF, these students collaborated with professors to enhance their subject competency. As a result, one student tied at the first rank in the national ERN 2014 poster competition for Computer Science, and was rated at the first place during the 2014 CSUB Student Research Competition for Computer Science. Another student achieved the first place in the 2015 CSUB Student Research Poster Competition. The third student was recognized as the 2015 outstanding graduating senior in research by School of Natural Sciences and Mathematics at CSUB. The fourth student has entered a Master's program in National Security while accumulating experiences in cybersecurity consulting. Internships in information security have been offered to two of the students in summer, 2015. Altogether four student assistants have demonstrated academic excellence in this funding period, which met an important expectation in the original MIAEO proposal, i.e., “The unique, multidisciplinary curriculum will produce well-rounded graduates who will be excellent candidates for careers in federal and local agencies” (p. 1 of Project Summary for Grant No. DUE – 1241636).

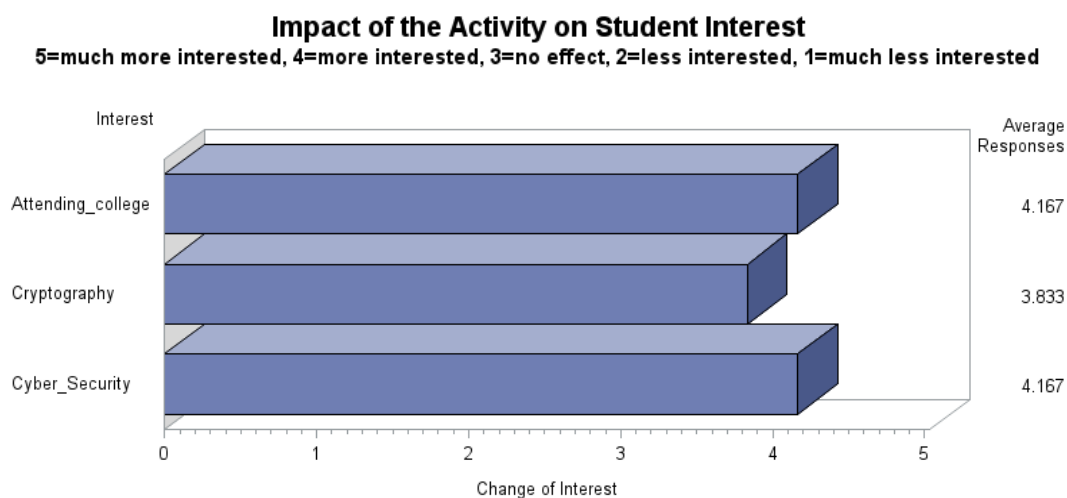


Figure 3. Program Impact on Academic Interest of REVS-UP Participants

In summary, REVS-UP created a teamwork opportunity for both high school students and university student assistants. The benefit was not only reflected on IA career training at the

college level, but also supported recognition of high school students on the college bound. One of the high school participants was highlighted online by local news media prior to her college entry (see <http://www.bakersfield.com/BakersfieldLife/2015/05/29/High-School-Senior-Ebony-Turner.html>).

4. How much has been done through the Dissemination Workshop to support IA education for K-12 teachers?

It was acknowledged in the original grant proposal that “Another key area for information assurance outreach is general education of the local community and the region as a whole” (see Project Summary for Grant No. DUE – 1241636). Over the past three years, transition occurred in the approaches between “giving fish” and “teaching fishing”. Initially, a Cyber Security Panel Discussion was held for the public in 2013 to strengthen community engagement in IA education.

Unlike the mathematics and science parts of the STEM field, no specific courses are designated for *technology* and *engineering* subjects in compulsory education. The IA knowledge update also occurred fast, which made it impossible to retain the routine course offerings. MIAEO was quick at adapting to the strong need for “teaching fishing”, and implemented the first Dissemination Workshop on August 1, 2014 to introduce REVS-UP projects to K-12 teachers. The workshop for the third year occurred on July 31, 2015.

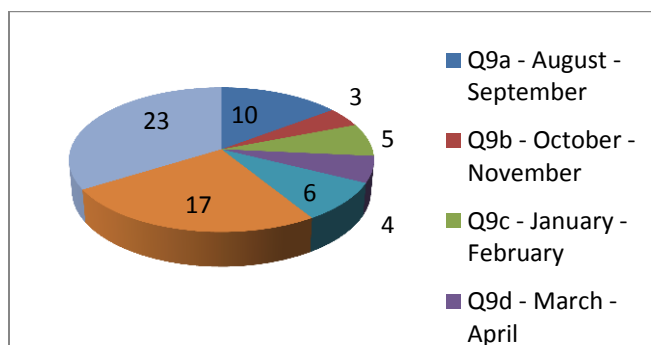


Figure 4. Teachers' Preferred Times for Cybersecurity Training

To fit teacher schedule, new data were gathered to survey teacher availability. Figure 4 showed that 73.53% of the responses supported the workshop offering during summer months of June, July, and August. In addition, the outreach effort was extended to K-12 school settings. The involvement of lower grade levels was based on fact that children started using technology tools, such as iPads and computers, prior to high school years. Nonetheless, the need seemed to become stronger at the high school level because cyberspace learning “helped engage students, cut down on paper, and allowed absent students to keep up with classwork” (Koebler, 2011, p. 2). The variation of service demand across grade levels is in agreement with the distribution of 30 teacher participants in the workshop setting (Figure 5).

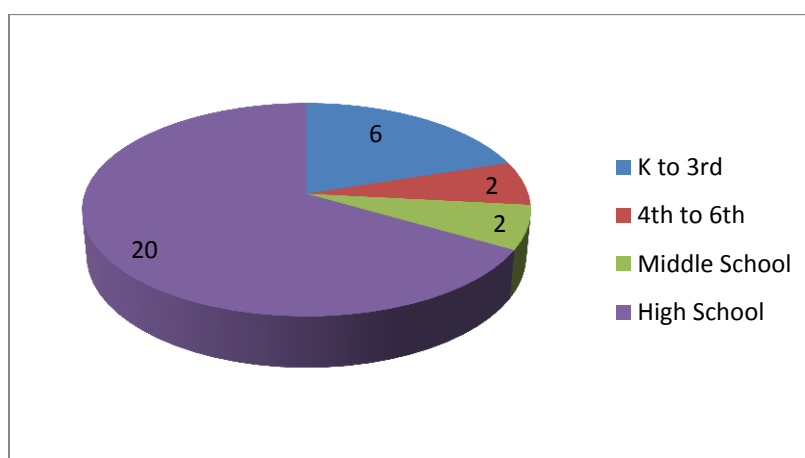


Figure 5. Teaching Levels of the Workshop Participants in 2015.

The teacher engagement has also been indicated by retention half of the past attendees in the Dissemination Workshop for the third year. In addition to sharing new projects from REVS-UP explorations, special attention was given to the returning attendees to assess the impact from their past learning experiences. With the final year support from NSF, attendees were guided to discuss future directions of K-12 cybersecurity education. The workshop agenda is listed in Table 5.

Table 5: Agenda of the 2015 Dissemination Workshop

9:30am	Room is open for early arrivals
10:00-10:15am	Welcome remarks and Introductions
10:15-11:00am	Discussion with returning attendees from 2014 workshop
11:00-Noon	Materials from REVS-UP sections
Noon-1:00pm	Working lunch: Break into small groups to discuss materials REVS-UP survey results poster on display
1:00-1:45pm	Report back from groups and Discuss results from REVS-UP surveys
1:45-2:45pm	Future directions for K-12 cybersecurity activities
2:45-3:00pm	Attendee surveys and turn in completed stipend paperwork

In summary, preparations have been made for participating teachers of the Dissemination Workshop to sustain the impact of IA education in K-12 settings. The impact on teachers may help strengthen the technology and engineering components of STEM instruction at the level of compulsory education.

5. How well did the program perform in service delivery?

Outcomes of the service delivery are reflected by *depth of learning* among the workshop participants. According to Bloom's taxonomy, the lowest level of learning is confined in *fact remembering* and the highest level involves a component of *creation* (Figure 6).

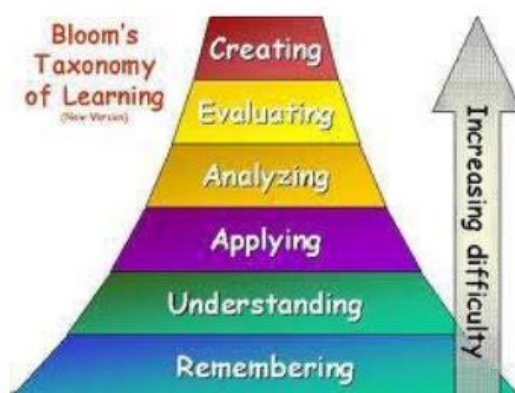


Figure 6. Revised Bloom's Taxonomy (Wilson, 2013).

In addition to passing on new information from REVS-UP poster presentation, the workshop guided its participants to consider creating cybersecurity activities in after-school settings. As a result, 22 out of 30 teachers clearly expressed their interest in after-school activities (see Figure 7).

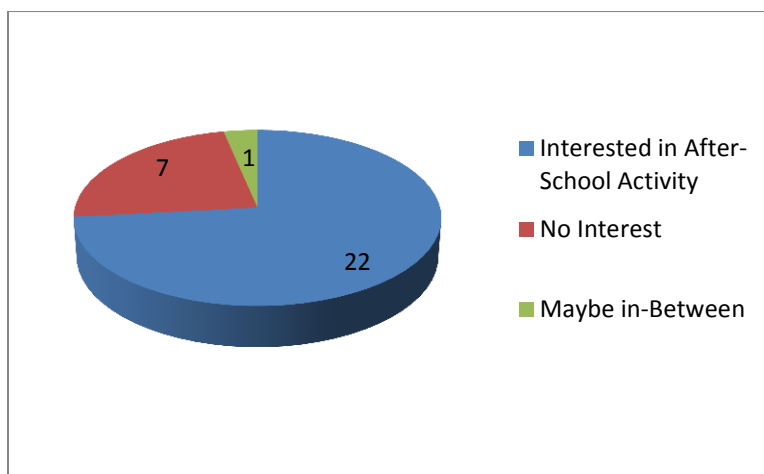


Figure 7. Participant Willingness to Create Cybersecurity After-School Activities in 2015

More specifically, participants indicated choices of different activities, and Cyber Patriot was selected by most teachers (Figure 8).

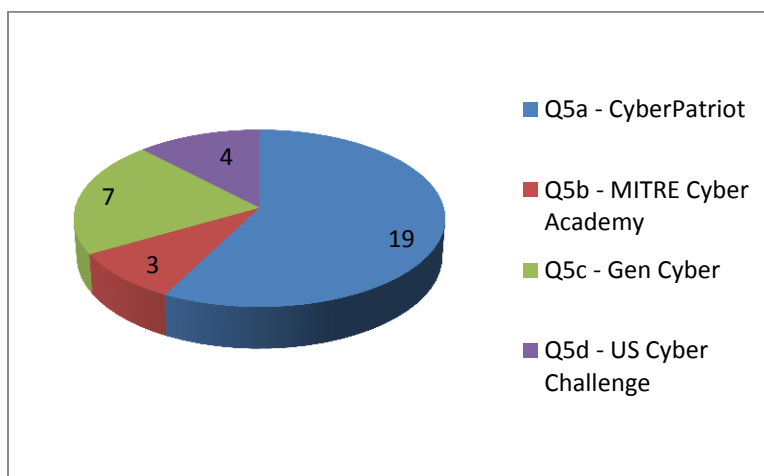


Figure 8. Teacher's Choice of Cyber Security Activities.

The activities identified from the survey instrument were backed by supportive comments from teachers, such as the following:

Competition, education and the ability to elevate student interests above online gaming.

It would be great to expose my students to this to give them an experience they have never had.

Opportunities for students to get involved in something so relevant.

Our students today are interested in technology and this would be a great activity to teach students about cyber security.

I work with Elementary school age students who need exposure to diverse fields. It looks like a good way to build excitement about a STEM career

Exposing HS students to cybersecurity would open doors to new interests as well as possible higher education and employment opportunities.

In combination, the results show effective engagement of K-12 teachers in IA education.

In the end, the depth of learning was not confined in remembering what was done in REVS-UP poster presentations. On the contrary, teachers were led to consider creating new activities, such as Cyber Patriot, at the level of compulsory education.

6. Is anyone better off due to this outreach effort?

Teacher participants had a chance to identify the most beneficial aspects of the Dissemination Workshop. Most of them indicated that they benefited from “Review on password safety”, “Basic cybersecurity info”, and “Ways in which I can make this topic relevant to my students and different career paths”. They were impressed by the latest development of learning camps, research competitions, and career potentials for students in IA education.

The learning outcomes supported incorporation of the workshop materials in K-12 school settings. In addition to recognizing the importance of cyber security and password strength, the past workshop participants included “How to create a more secure password” in their lesson

plans and encouraged students to “look into cyber security as a major in college”. In 2015, the curriculum impact occurred with 10 out of the 15 workshop participants from last year, and all 30 workshop participants indicated their desire to attend future cybersecurity training at CSUB (Figure 9).

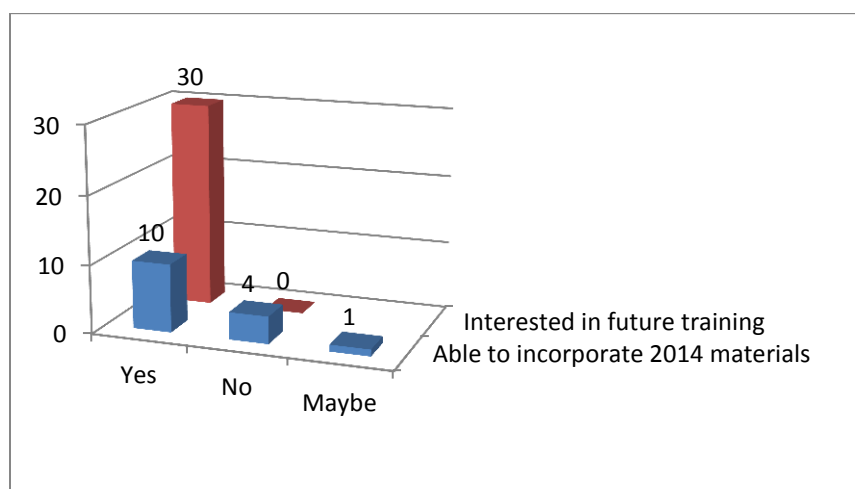


Figure 9. Impact of the Dissemination Workshop on Teachers

In conclusion, MIAEO has offered REVS-UP training to develop academic and career interest in information assurance for high school students. CSUB student assistants received support from this grant to continue their education and career paths in the cyber security field. The community outreach effort has raised awareness of information assurance in K-12 school settings.

Future Direction

Over the past three years, California State University, Bakersfield (CSUB) received NSF funding to support hands-on explorations in *network security* and *cryptography* during a four-week summer session. The research process also involved CSUB student assistants and professors in charge of developing a new curriculum in IA education. The product was

represented by poster presentations for the Dissemination Workshop in the community. To sustain the coherent articulation across different IA education components in MIAEO, future directions are examined in this report to support student learning beyond the period of NSF funding.

Before incorporation of MIAEO, REVS-UP offered hands-on research experiences in STEM fields for high school students since 2007. Each year, REVS-UP invited news media to announce the summer learning opportunity in an opening reception. In 2013 and 2014, REVS-UP also contributed \$200 per high school student to amend a compensation gap between MIAEO and other STEM exploration projects. Using this existing platform has saved MIAEO budget for program advertisement, student screening, and summer session scheduling. The REVS-UP setting allowed high school students to receive five units of college-level science credit for participating in MIAEO explorations. These supports were covered by private funding from the Chevron Cooperation, and strengthened NSF funding outcomes.

While acknowledging these advantages, it is worth noting that REVS-UP is not stagnant platform. To cope with the increase of local demand, three adjustments have been made by REVS-UP that impacted MIAEO operation in the third year:

- (1) No high school teachers were invited as team members to support the REVS-UP exploration;
- (2) No freshman students from local high school were allowed to apply for REVS-UP participation;
- (3) Students were discouraged from participating in REVS-UP explorations on the same research track.

These changes seemed necessary under the reduced budget for REVS-UP.

Although MIAEO was not funded by Chevron, the **contextual** change inevitably altered the outcome of its participant selection. For instance, the P.I. of MIAEO noted that “I found out during introductions today that almost the entire group are seniors who just finished high school. I know that was the direction REVS-UP was taking as a whole, but I had asked for more 10th/11th grade students to keep the demographics similar to the past two years” (personal communication on July 13, 2015).

Besides the aspects of **context** and **input**, elimination of high school teachers also impacted the **process** and **product** phases of REVS-UP service delivery. Regarding the merit of teacher involvement, the REVS-UP Director noted that “We re-vitalize their interest in science and give them ideas for hands-on projects and experiences that they introduce in their classrooms. Teachers are very excited about this opportunity and have already included many of their experiences into the classroom” (https://www.csub.edu/insideCSUB/cc/andreas_gebauer.shtml).

Prior to the Chevron sponsorship, REVS-UP was originated from a NSF grant in geoscience (NSF Grant No. GEO 0303324). The recent changes in REVS-UP need to be examined for following reasons:

- (1) Since MIAEO includes a Dissemination Workshop for teachers, involvement of high school teachers in REVS-UP may help make poster presentations more relevant to the workshop attendees;
- (2) Based on the evaluator’s interview notes from August 2015, high school teachers indicated the needs of engaging younger students in IA education. However, REVS-UP made a decision to only admit older students above the freshman level;

(3) Since IA education never occurred as key STEM component in K-12 curricula, teachers suggested the “dosage” increase by inviting students to continue REVS-UP explorations across multiple years. The past records showed completion of different research projects each year (see Table 4), which could support the “dosage” accumulation.

The examination of MIAEO connection with REVS-UP may help clarify the need of continuing the “one size fit all” approach in the future direction. In particular, MIAEO may need to reverse the REVS-UP change in 2015 by encouraging students to continue engagement in IA explorations across multiple years.



References

- Angelo, T. (1999, May). Doing assessment as if learning matters most. *American Association for Higher Education Bulletin*, pp. 1-2.
- Bottia, M., Stearns, E., Mickelson, R., Moller, S., & Parker, A. (2015). The relationships among high school STEM learning experiences and students' intent to declare and declaration of a STEM major in college. *Teachers College Record*, 117, 1-46.
- Brookings Institution (2010). *The state of metropolitan America: Educational attainment*. Retrieved from <http://www.brookings.edu/metro/MetroAmericaChapters/education.aspx>.
- Dotson, J. (2011). *Cooperative learning structures can increase student achievement*. Retrieved from http://www.kaganonline.com/free_articles/research_and_rationale/increase_achievement.php.
- Friedman, M. (2006). *Trying hard is not good enough: How to produce measurable improvements for customers and communities*. Victoria, B.C.: Trafford.
- Friedman, M. (2009). *Trying hard is not good enough*. Retrieved from <http://www.amazon.com/Trying-Hard-Not-Good-Enough/dp/1439237867>.
- Hanson, K., Guilfooy, V., & Pillai, S. (2009). *More than Title IX: How equity in education has shaped the nation*. Lanham, MD: Rowman & Littlefield Publishers.
- Harwood, T. (2011). *Examination of factors contributing to the achievement gap of native American students in select school districts in Michigan*. Retrieved from <http://commons.emich.edu/cgi/viewcontent.cgi?article=1363&context=theses>.
- Koebler, J. (2011). *More high schools implement iPad programs*. Retrieved from <http://www.usnews.com/education/blogs/high-school-notes/2011/09/07/more-high-schools-implement-ipad-programs>.
- Legewie, J., & DiPrete, T. (2014). The high school environment and the gender gap in science and engineering. *Sociology of Education*, 87(4), 259–280.
- Liou, P.-Y., Kirchoff, A., & Lawrenz, F. (2010). Perceived effects of scholarships on STEM majors' commitment to teaching in high needs schools. *Journal of Science Teacher Education*, 21(4), 451-470.
- Miklas, J. (2014). *Using data to make decisions: Results-Based Accountability & the collective impact toolkit*. Retrieved from <http://www.collaborationforimpact.com/wp-content/uploads/2014/03/Results-Based-Accountability-the-Collective-Impact-toolkit.pdf>.
- National Education Foundation (2006). *U.S. Department of Education's Carl D. Perkins Career and Technical Education Improvement Act of 2006 (Perkins IV)*. Retrieved from <http://perkins4.org>.
- National Security Agency & Department of Homeland Security (2013). *National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) education: Program criteria for measurement*. Retrieved from <http://www.cisse.info/pdf/2014/2014%20CAE%20IA-CD%20Criteria.pdf>
- National Women's Law Center. (2005). *Tools of the trade: Using the law to address sex segregation in high school career and technical education*. Washington, DC: Author.
- Neo-Piagetian Theories of Development*, (2009). Retrieved from <http://www.education.com/reference/article/neo-piagetian-theories-of-development/>

- NSF (2014). *Program solicitation*. Retrieved from <http://www.nsf.gov/pubs/2014/nsf14586/nsf14586.htm>.
- Pittaoulis, M. (2012). *Getting through school: A study of how students select their college majors and plan for the future*. Philadelphia, PA: Temple University (UMI 3494134).
- Portman, R. (2006). *2008 Planning Guidance for Math and Science Education Programs*. Washington, DC: Executive Office of the President. Retrieved from <https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-24.pdf>.
- Program Evaluation Standards* (2010). Retrieved from <http://www.jcsee.org/program-evaluation-standards>.
- Robelen, E. (2012). Gender gaps persist in STEM education. *Education Week*, 37, 17-19.
- Sloane, F. (2008). Through the looking glass: Experiments, quasi-experiments, and the medical model. *Educational Researcher*, 37 (1), 41-46
- Stufflebeam, D. L. (1983). The CIPP Model for program evaluation. In G. F. Madaus, M. S. Scriven & D. L. Stufflebeam (Eds.), *Evaluation models: Viewpoints on educational and human service evaluation* (pp.117-142). Boston: Kluwer-Nijhoff
- Wang, J. (2013). *Models for Information Assurance Education and Outreach: A report on Year 1 implementation*. Retrieved from <http://files.eric.ed.gov/fulltext/ED545559.pdf>.
- Wang, J. (2014). *Models for Information Assurance Education and Outreach: A report on Year 2 implementation*. Retrieved from <http://files.eric.ed.gov/fulltext/ED546861.pdf>.
- Wilson, L. (2013). *Anderson and Krathwohl – Bloom’s taxonomy revised*. Retrieved from <http://thesecondprinciple.com/teaching-essentials/beyond-bloom-cognitive-taxonomy-revised/>
- 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.
- Zhang, G., Zeller, N., Griffith, R., Metcalf, D., Williams, J., Shea, C., & Misulis, K. (2011). Using the Context, Input, Process, and Product Evaluation Model (CIPP) as a comprehensive framework to guide the planning, implementation, and assessment of service-learning programs. *Journal of Higher Education Outreach and Engagement*, 15, 57-83.
- Zumbrun, J. (2008, November 28). *America's best-and worst-educated cities*. Retrieved from <http://www.forbes.com>.

Appendix 1: Poster Presentations of Five IA Research Projects


1. E-cash: The Transition to Paperless Currency

E-cash: The Transition to Paperless Currency

Callayah Flowers, Ryan Crowley, Isabel Suarez Acosta, Brett Hashim

Advisor: Dr. Charles Lam Assistant: Frank Madrid




Partial support for this work was provided by the National Science Foundation's Federal Cyber Service Scholarship for Services (FS2) program under Award No. 1245185. All actions, thoughts, and conclusions of the author(s) are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

What is E-cash?

Created in 1990 by David Chaum, E-cash is an electronic payment scheme with similar properties to physical currency. It uses advanced cryptographic principles to hide the identity of the users and their spending habits. E-cash has been implemented in certain parts of Europe, Australia, and South Africa due to the lack of credit cards in these regions. This form of payment removes the need for a middleman (i.e. a bank) in a transaction. E-cash has the potential to be the currency of the future. [3]


E-cash Benefits

- Anonymity/Privacy
- No transaction fees
- Transcends national currencies
- Easily transferrable
- Change no longer necessary



E-cash Drawbacks

- Can't use system without internet access
- Anonymity may lead to illegal activities
 - Money laundering
 - Double spending
 - Tax evasion
- Costly to implement software [5]



Protocol Source Code

```

// Generates random integers
function generateRandomInteger(digitCount)
{
    return Math.floor(Math.random() * 10^digitCount);
}

// Generates random strings
function generateRandomString(n, k, i)
{
    return generateRandomInteger(n, k, i);
}

// Generates random keys
function generateRandomKey(n, k, i)
{
    return generateRandomString(n, k, i);
}

// Generates random coins
function generateRandomCoin()
{
    return generateRandomKey(256, 256);
}

// Generates random coins
function generateRandomCoins(k)
{
    return generateRandomCoin();
}

// Generates random coins
function generateRandomCoins(k)
{
    return generateRandomCoin();
}
                    
```

Untraceable Electronic Cash Protocol

1. Bank publishes an integer n which is the product of two sufficiently large primes p and q and a sufficiently large integer k .

2. Alice obtains an electronic coin C_i .

3. Alice pays Bob with the electronic coin C_i .

Transaction Process

In a typical E-cash transaction, there are three participants: a trusted third party, a merchant, and a customer. The process is detailed in the flowchart below. The algorithm it follows allows for secure minting of an E-coin but prevents double-spending by tracing back the variables used by the consumer to make the actual coin. [4]

RSA-based Algorithm

Untraceable Cash Protocol

Bank publishes an integer n which is the product of two sufficiently large primes p and q and a sufficiently large integer k .

$n = \text{generatePublicKey}(\text{primeDigitCount})$

$k = \text{generateRandomInteger}(\text{digitCount})$

Alice Obtains an Electronic Coin

Alice generates strings a_i, r_i, c_i , and d_i with length i where $1 \leq i \leq k$ independently and uniformly and random from residues mod n .

$a_i = \text{generateRandomKey}(n, k, i)$ $r = \text{generateRandomKey}(n, k, i)$

$c_i = \text{generateRandomKey}(n, k, i)$ $d = \text{generateRandomKey}(n, k, i)$

Alice generates and sends to the bank B_i which consists of k blinded candidates $B_i = r_i^{-1} \cdot f(x_i, y_i) \text{ mod } n$ for $1 \leq i \leq k$ where

$x_i = g(a_i, c_i)$ $y_i = g(a_i \oplus (n \parallel (v + i)), d_i)$

and f and g are any suitable one-way function.

The bank then chooses a random subset of $k/2$ blinded candidate indices $R = \{i_j | 1 \leq i_j \leq k \text{ for } 1 \leq j \leq k/2\}$ and transmits it to Alice.

Alice displays the r_i, a_i, c_i , and d_i values $\forall i \in R$, where the bank confirms their values since $n \parallel (v + i)$ is known to the bank.

The bank gives Alice

$$\prod_{i \in R} B_i^{1/3} \text{ mod } n$$

and charges Alice's account by one dollar. The bank also increments Alice's counter v by k .

Alice can then extract the electronic coin C

$$C = \prod_{i \in R} f(x_i, y_i)^{1/3} \text{ mod } n$$

Alice Pays Bob With the Electronic Coin

Alice sends C to Bob.

Bob chooses a binary string $x_1, x_2, \dots, x_{k/2}$

Alice responds as follows for all $1 \leq i \leq k/2$

If $x_i = 1$, then Alice sends Bob a_i, c_i , and y_i .


If $x_i = 0$, then Alice sends Bob $x_i, a_i \oplus (n \parallel (v + i))$ and d_i .

Bob verifies that C is of the proper form and that Alice's response fits C .

Bob later sends C and Alice's response to the bank, which verifies their correctness and credits his account. [2]

Blind Signatures

Blind signatures are a form of digital signature that utilizes RSA encryption to disguise a message before it is verified. When the consumer uses a "blind signature", the bank can't link withdrawals and deposits. This blind signature allows the bank to verify a message without actually reading it. [1] This idea was first implemented by David Chaum and is based upon RSA encryption. [2]



Double Spending

"Double-spending" is the process of using an E-cash "coin" to purchase more than what currency amount is registered on the coin itself. Verification of E-cash is sometimes done after the transaction is made, allowing the consumer to "double-spend." A solution to this problem is to ensure the verification of the E-cash coin during the transaction process. If a coin is used more than once, the owner of the coin's identity will be revealed and reviewed. [4]

Conclusion

E-cash is a versatile form of electronic currency. In contrast to gift cards, it doesn't require a database to complete a transaction. As opposed to credit cards, it offers privacy for the user and eliminates transaction fees. Since credit cards have established a reputation of convenience and reliability amongst many countries, the implementation of E-cash will be a challenge. Despite its flaws, E-cash could become the next major payment scheme.

References

1. Bellare, Rebecca. "Cryptography: Authentication, Blind Signatures, and Digital Cash." *Cryptography: Authentication, Blind Signatures, and Digital Cash*. (n.d.). n. pag. Web. 30 July 2015.
2. Chaum, David, Amos Fiat, and Moni Naor. "Untraceable Electronic Cash." *Advances in Cryptology – CRYPTO' 88 Lecture Notes in Computer Science* (1990): 319-27. Web. 30 July 2015.
3. Goshligan, Patrick G. "E-Cash." *E-Cash*. n.p., n.d. Web. 30 July 2015.
4. Law, Laurie, and Susan Sabett. "HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH." *How To Make A Mint: The Cryptography of Anonymous Electronic Cash*. n.p., n.d. Web. 30 July 2015.
5. Sheehan, Kevin P. "Electronic Cash." SpringerReference (2011): n. pag. Web. 29 July 2015.

2. The Enigma Machine



Partial support for this work was provided by the National Science Foundation's Federal Cyber Services Scholarship for Service (FCS) program under Award No. 1243630. All names, logos, and trademarks are used herein in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

The Enigma Machine

Navneeth Dosanjh, Ramiro Hernandez, Jasmine Bernal, Damarice Herrera

Advisor: Dr. Charles Lam Assistant: Frank Madrid



How it all began?



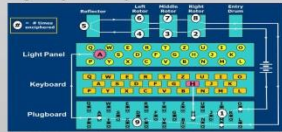
German engineer, Arthur Scherbius, invented one of the greatest electric mechanical cipher machines in the 1920s [5]. The Enigma machine was envisioned for commercial use but instead it was commonly used for World War II. The machine allowed its operator to type a message, then randomized it using a cipher substitution system produced by variable rotors and an electronic circuit. Over the years German code experts modified the machine to make it more complex by adding plug boards and making it more transportable for war-time purposes.



What is in it?

Enigma contains rotors, plug boards, lamp panels[2]:

- Rotors- When a character enters the rotor it causes the rotor to rotate one position forward, preventing the letter from encrypting into itself. Three rotors are chosen from five available rotors.
- Plug boards- The machine contains 10 plugs allowing two different letters to exchange.
- Reflectors- The reflector receives the input and reflects the electrical signal transmitting it back to the rotors.
- Lamp boards- The electric signal arrives to the lamp board which lights up the enciphered character.



This shows the internal structure of the Enigma machine.

Cryptographic Principles

The key sheet (shown below) is the private key which contains[2]:

- Walzenlage(roll location): choice and order of the wheels
- Ringstellung(ring position) : the position of the rotor wiring, relative to the alphabet rings
- Steckerverbindungen(plug connections): the plug connections on the plug board
- Kenngruppen(characteristic groups):groups to classify the key to the receiver

- It is a symmetric encryption scheme.
- The machine is a polyalphabetic substitution cipher.
- The secret key for the scheme is in how you set the machine up.
- The machines have to be identically set up in each session, for correct communication.

How many settings?

The combinations of the different rotors, their order, their initial positions and the plug board help to increase the complexity or the size of the amount of possible configurations the machine can hold [6].



Rotor

When considering the amount of permutations when choosing 5 out of 3 rotors we have:

$$\binom{5}{3} = \frac{5!}{2!} = 5 \cdot 4 \cdot 3 = 60 \text{ combinations}$$

Rotor Initial Position

Since each rotor has 26 unique initial configurations, we have:

$$26 \times 26 \times 26 \times = 26^3 = 17,576 \text{ positions}$$

Plug board

The plug board can connect up to ten pairs of letters where no letter can connect to itself, we have:

$$\binom{10}{10} \cdot \binom{26}{2 \ 2 \ 2 \ 2 \ 2} = \frac{26!}{2^{10} \cdot 10! \cdot 6!} = 150,738,274,937,250 \text{ combinations}$$

Therefore, the total amount of possibilities is approximately 1.59×10^{20} .

Breaking the Unbreakable

- Enigma machine was first broken by the Polish Cipher Bureau, including Marian Rejewki, Jerzy Rozycki, and Henryk Zygalki[4].
- Rejewki discovered that the wiring connections between the machine's keyboard and encoding mechanism were in alphabetical order. He made his major breakthrough by formulating equations to match permutations in the settings of the machine.
- Rejewki used theoretical mathematics to reverse engineer the device and created numerous devices to break the ciphers.

Bombe

- Alan Turing used an electro-mechanical device to assist in deciphering German's secret communications[3].
- An electronic current would flow through the machine. In every wrong deduction or assumption made, the machine would "click", indicating that it is incorrect and it would redirect to the next option.
- Using process of elimination, an individual would check the remaining options.
- Over 200 bombes were created but after the war all the original bombes were destroyed.



Flaws in the Machine

- A certain character could not be encrypted to itself [1].
- Operators reused keys that had been used before.
- Operators often used keys that were easily defined on the keyboard.
- No rotor was allowed to be in the same position on consecutive days.
- Plug board cables were not able to connect to itself.
- The third rotor wheel hardly shifted position.



References




- "Enigma." *Enigma*. Crypto Museum, 31 May 2014. Web. 03 Aug. 2015.
- "Enigma Procedure." *Enigma Procedure*. Dirk Rijmenants, 2004-2014. Web. 03 Aug. 2015.
- Flaw in the Enigma Code- Numberphile*. Perf. Dr. James Grime. *YouTube*. YouTube, 2013. Web. 03 Aug. 2015.
- Horlock, Alex. "Bletchley Park Doesn't Deserve All the Code-cracking Credit": Poles Claim They Worked out Enigma Code FIRST." *Mail Online*. Associated Newspapers, 09 Oct. 2012. Web. 03 Aug. 2015.
- Lycett, Andrew. "Enigma." *BBC News*. BBC, 2015. Web. 03 Aug. 2015.
- 158,962,555,217,826,360,000 (*Enigma Machine*) *Numberphile* Dr. James Grime. *YouTube*. YouTube, 10 Jan. 2013. Web. 04 Aug. 2015.

3. Digital Crime Scenes

Digital Crime Scenes

Jacob Abbott, Joshua Cancellier, Taylor Redden

Advisor: Dr. Melissa Danforth Assistants: Polo Melendez and Mark Stevens

Partial support for this work was provided by the National Science Foundation's Federal Cyber Service Scholarship for Service (SP3) program under Award No. 1241636. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

What is digital forensics?

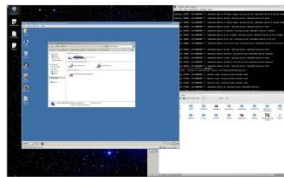
Digital forensics involves the retrieving and analyzing of hidden or protected information in electronic devices. The processes it encompasses often involve investigating a crime scene or finding exploits in vulnerable systems to prevent such crimes. For example, an exploit was recently found in certain Chrysler vehicles that allowed attackers to have complete control over the car, even from a great distance, using wireless networks.

Digital forensics usually includes three general steps: acquisition, extraction, and analysis. First we must gain access to and acquire the data, next we must extract the data we are looking for and put it into a readable format, and last we must analyze the data to make a conclusion about its significance.

Before we can do any of this, however, we must first organize a toolkit to help us do each of these steps. The toolkit allows us to access protected data, recover corrupted or deleted files, and view otherwise unreadable files, which is related to the acquisition and extraction steps. A danger with using tools that are already on whatever device you are accessing is that they may have been tampered with to provide false or misleading evidence. Because of this we put a toolkit together before hand with whatever we may need and then load it onto the device we are accessing. The tools we used in our project included: virtual machines, live CDs, Sleuthkit, WinHex, grep, and gcore.

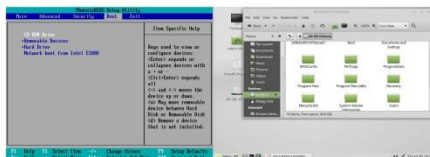
Tools

- Virtual Machines** - Allow us to simulate operating systems and safely use different tools and programs without the risk of damaging the machine we are working on.

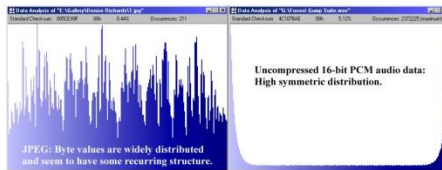


- Sleuthkit** - A set of tools that allows us to analyze disk images and recover files from them, even ones that have been deleted or corrupted.

- Live CDs** - If a computer requires some kind of security key to access, we can boot the computer from our live CD and access the contents of the hard drive, bypassing the needed user credentials. Below are the contents of a Windows computer accessed through a Linux live CD.



- WinHex** - If a file is corrupted and unreadable, WinHex can analyze its data distribution and help determine what kind of file it is, thereby allowing us to reconstruct the file so it becomes readable again.



- gcore** - A utility in the Linux terminal which is designed to dump or copy system memory to a console, text, or binary file. This is one of the many methods used to obtain a user's credentials or recover volatile data. While this output file can be quite lengthy, a simple search can reveal desired information easily, as shown below with a search for a phrase such as "password=".

```
student@student-virtual-machine ~ # strings core.2950 | grep password=
username=stevens5@csu.edu mypass5testcookies=1
student@student-virtual-machine ~ #
```

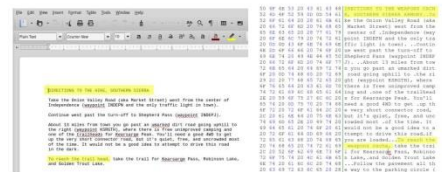
Steganography

Steganography is the practice of hiding a message, image, or video within the code of another file. This embedding process allows for the concealing of important or perhaps incriminating information such as the credentials to a company's database or the plans for criminal activity. Sometimes these hidden messages can leave "artifacts" or small distortions in the image. Searching through a file or an image for hidden information is a common step for analysis within Digital Forensics. See if you can spot the artifact in the image below.



```
54 58 43 08 18 70 68 07 54 .....[b]k..[V
FA 28 89 AD 69 96 06 18 2E .....281[.....K
52 52 72 23 0F 67 75 6B 62 .....9...A...K...58 04ab
56 A5 A8 47 71 79 6E 23 D0 .....1301:80a0...Dr...ogga*
57 62 74 74 72 28 28 9F 0...57:88...0...57:11e...
65 62 69 74 65 72 65 64 20 The package base name: dist@redhat
AC 97 28 AC 07 12 98 18 81 56 7339 Parker Stearns.....
70 50 81 C2 88 0F 43 30 28 .....A...K...E...
95 9A 59 37 10 09 C8 28 AD 3B...E...8B...20...Y7...
10 5A C2 70 82 CD 43 30 28 .....970:0...A...E...E...B...
AA 5A 7F 20 10 82 3A .....0...0...1...
E7 8D 72 87 5E 14 80 80 94 .....7...1...8...9...1...0...
89 49 26 AC D9 CD 0C 6D 84...g...D...d...d...d...d...
```

Even text files can have a completely different message hidden underneath. Microsoft Word is infamous for not actually deleting content that the user thought was deleted.



REFERENCES

- Winhex - <http://www.winhex.com/winhex/>
- Virtual Machine - <https://www.vmware.com/>
- Sleuthkit - <http://www.sleuthkit.org/>
- Bless Hex Editor - <http://home.gna.org/blless/>
- Linux Mint - <http://www.linuxmint.com/>

4. Cracking Password Hashes

Cracking Password Hashes

Martin Mendoza, Kyle Johnson, Tue Le, Amaris Maestas

Advisor: Dr. Melissa Danforth Assistants: Polo Melendez and Mark Stevens



Partial support for this work was provided by the National Science Foundation's Federal Cyber Service Scholarship for Service (CFSS) program under Award No. 1241655. Any views, findings, 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.

CPU v.s. GPU



The **Central Processing Unit (CPU)**, more commonly known as simply the **processor**, handles all arithmetic and logical operations. The CPU essentially performs as the brain of the computer, synchronizing and performing tasks and instructions. The average CPU will have 4-8 cores, and generally a greater number of cores increases the amount of instructions that can be executed simultaneously.

Computers equipped with a **Graphics Card** can take advantage of a **Graphics Processing Unit (GPU)**, a processor optimized specifically for rendering images to the screen. A GPU can contain hundreds of times more cores than a CPU, allowing a GPU to handle much larger volumes of arithmetic functions in parallel. **oclHashcat** takes advantage of this increased throughput to process large numbers of password hashes very quickly. **oclHashcat**: <http://hashcat.net/oclhashcat/>



Intel i7 CPU

NVIDIA Quadro 2000

Password Complexities

Some examples of how many passwords can be created with some simple parameters

	Combinations	Possible Passwords
6 digits	10 x 10 x 10 x 10 x 10 x 10	10 ⁶ = 1,000,000
6 symbols	35 x 35 x 35 x 35 x 35 x 35	35 ⁶ = 1,838,265,625
6 lowercase	26 x 26 x 26 x 26 x 26 x 26	26 ⁶ = 1,073,741,824
6 characters	97 x 97 x 97 x 97 x 97 x 97	97 ⁶ = 689,869,781,056

Hashing Algorithms

A **password hash** is the product of inputting a password into a **hashing algorithm**. The resulting **hash** is a seemingly random collection of numbers and letters that represent your encrypted password, disguising it from an attacker. A hashing algorithm cannot be reversed, and the stronger the hashing method, the longer it takes to produce a hash.

Due to the fact that hashing algorithms cannot be reversed, the algorithm itself isn't what we are cracking. In fact, many popular hashing algorithms are available to the public. In order to crack a password, thousands of trial passwords must be generated, hashed, and compared to the original hash. If a match is found, you have successfully cracked the password.

```
dccff28314d9ae4ed262cfc6f35e5153
c4d4d037d70a05e8f526d18aa25fb5e
01545fa976c8367b4f0d59169ac4e66c
08d25bf279e353686a974b7b14ae7d81
119cb63b48c9a18f31f417f09655efbd
a4fc15313ef2a516bfbf83ce44281535
ca2531b8cd79ea5b778ede3a524779b9
3aa14ca13d52df070870d39306f4a4eb
b31731ea6cdebbe1d02f8193db420886
```

Attacks

Some example attacks and their performance in terms of kHashes/sec

	MD5	SHA1	SHA256	SHA512
Straight	25,761.2	9581.3	10591.4	7016.3
Combination	20,200.3	10,800.2	68326.3	20194.5
Brute Force	38,300.2	10391.4	79693.4	20798.8
Hybrid	20,900.7	10,800.3	67726.1	20217.9

Components Used In Attacks:

Large.dict	869,232 lines
common_passwords.dict	3,557 lines
?a?a?a?a	8,587,340,257 combinations
?l?l?l?l?l	11,881,376 combinations

Attacks:

Straight:	Large.dict
Combination:	Large.dict x common_passwords.dict
Brute Force:	?a?a?a?a
Hybrid:	Large.dict x ?l?l?l?l?l

Tips for safe passwords

- Short **randomized** phrases are easy to remember, but still very secure
- Don't follow patterns that are commonly used
- Don't use the same password for multiple sites or accounts
- Always use two factor authentication if given the option
- Use a variety of symbols and numbers

Cracking Test Passwords

Hash	Salt	Password
4c08307c2808c0897f010844373b084570872c5177235		Password
f4ea3ec716086e5861039363926e2b88e43887	95ee460b	apple123
48034e27e08a70d70a449080e0795144336cf	a982c8ba	yes
0902c6e06f7c0e01b3242097f04e680919e3a	4880789e	31631992
32c5a7241836909802bb09a7766a478332076c	6587d1ed	0
0530e49119d7312100711c000e440a019205e	4f80e06c	quinnsekid
00179b18dc09e586e1f6ac5b0866e14e45d6a3b	40f2059	gower1stuh
09f0b34041120107780c19374b088052b6800	3507f83b	hard
08a3750808ac760c6ea0798a4194c0e2e657	02578e55	typpatrac1
040cab7790598a18087c0925e781290f831d	610e097c	harcicarmio
02005520800e405808f71298276400f6f8d	40202223	harveyanny
0101d06710910e0915d03080e0e0f7fc381	4e001971	olthargic00
09f5089072a008c1519518a293088417e09402	cd5d0007	gauratrygt
0772e06f0e1d1080081324c099880b70e0	0000070c	tharg1e1
1127c56470276523c3973a845312c65336a0	0ba3c0aa	qemanderfym
0212e05027ac15c0c04f6344670b708306	ff10c	fc0798ca
5a9800e18270a720950487f6e34303a10416	09c13e0	quintaibue
00713aaa1b0423855a049507f090e0818019	0e315c1f	qust1bus1ec
00453707f08ca0971e0f7f998400f08077	01307c03	newsp0r1bus
000e250c170e1905c050e00f44c7db1d3978e2	27019736	just1bus789
009a80b04072080f7c40c383509e09927744	0b31f102	password22
300e4e0013171e011990e50b5324c7c0519	c0d0000e	laker
000c5084505811015089308011085312d7f4	00f00005	quinnasez83

The test started with 16 students creating 3 passwords of varying strength: easy, medium, and strong. 52 more passwords were then randomly generated using numbers and dictionary words to end with a total of 100. The passwords were then hashed and given to us to try to crack using the different attacks available with **oclHashcat**.

- Given the limited resources available to us in the project, simpler, more efficient attacks had to be used.
- Some of the passwords were just too long and random to crack given these restrictions.
- We were able to crack 59% of the password hashes we were given.

Cracked Examples

qwerty	simply cracked with a dictionary attack
Password	cracked with a hybrid attack: ?u large.dict
apple123	cracked with a hybrid attack: large.dict ?d?d?d

Not Cracked Examples

32WaterFISH7239	Both 15 characters long and has a mix of lowercase, uppercase, and digits
10gwr2dv3	Random enough to need a mask of 9 characters
23571113171923293137	Password seems simple, but it could take 10 ²⁰ combinations to find