Cybersecurity Outreach for Underrepresented Minority Students

Gonzalo E. Perez | John V. Monaco | Charles C. Tappert | Li-Chiou Chen

Abstract

Growing a cybersecurity workforce begins with generating student interest. One way for community colleges to develop a cybersecurity workforce is by exposing students to active research through academic partnerships with established cybersecurity research institutions. In 2012, Passaic County Community College and Pace University formed a partnership to better attract underrepresented minority community college students into the cybersecurity field of study. The purpose of the partnership was to expose underrepresented minority students to a four-year university in order to promote transfer, to engage the students in various hands-on experiments and activities, and to teach the students how to write a research paper from the results of their experiments. The result has been positive for our students and 82% have transferred to four-year institutions in an information technology or cybersecurity field.

Introduction

Cybersecurity has been identified as one of the most serious economic and national security challenges facing our nation today. Cyber-attacks are becoming more prevalent, and no organization or individual is immune from nefarious hackers. In order to strengthen the nation’s security interests, significant effort is needed to recruit and build a 21st-century cybersecurity workforce. According to the Bureau of Labor and Statistics, the rate of growth for jobs in information security is projected at 37% from 2012-2022, which is higher than the average for all other occupations (Bureau of Labor Statistics, 2014). Hence, the demand for cybersecurity professionals is soaring, and leveraging an emerging underrepresented minority (URM) group of community college students is an ideal strategy to consider. According to a study by Cornell University ILR School, fewer women and minorities are receiving bachelor degrees in STEM disciplines (Griffith, 2010). The percentage of men entering STEM fields was higher than that of woman (33% vs. 14%); asian/pacific islander students expereinced a 47% STEM entrance rate as opposed to other groups (19-23%) (Chen, 2009). Some reasons cited as to the lower entrace rates for these groups include lack of preparation throughout secondary education and a lack of positive role models in the same gender or race. (Griffith, 2010).

One approach to support cybersecurity adoption and retention is through an academic partnership formed between a community college and established cybersecurity research institution. This provides URM community college students a clear pathway into a field that will afford a rewarding career, as well as directly benefit society.

The paper describes the cybersecurity outreach program that resulted from such an academic partnership. Using Passaic County Community College (PCCC) and Pace University as a case study, recommendations are made for other institutions interested in forming similar relationships. A background on behavioral biometrics is provided, including keystroke, mouse motion, and mobile touchscreen behavior, as a prelude to the biometric experiments that were cooperatively conducted between the community college and university students. Additionally, this article defines best practices that were developed to increase the impact on student success. Finally, some conclusions are drawn based on the feedback provided by the students through a reflection paper.

Background

In 2012, Passaic County Community College and Pace University formed a partnership to better attract underrepresented minorities (URM) into the Cybersecurity field of study. Pace has been a designated National Center of Academic Excellence in Information Assurance Education (CAEIAE) by the National Security Agency and the Department of Homeland Security since 2004. PCCC students traveled to Pace throughout the semester and also worked on various hands-on activities in between meetings as part of a cybersecurity outreach program. At the end of the research project, students had an opportunity to present their findings at Pace University's Annual Research Day Conference and publish their joint paper in the official conference Proc. (Farnon, et al., 2013) (Ciaurro, et al., 2014). Student research projects were in the area of behavioral biometrics, exposing the cohort of students to topics of growing interest in cybersecurity. The projects focused on behavioral biometrics, including keystroke, mouse motion, and touchscreen gestures on mobile devices. Additionally, Pace offered a cybersecurity day workshop to an alternative group of PCCC students in order to attract new groups of students to cybersecurity for the following academic year. The workshops introduced additional areas of cybersecurity to students such as web security, mobile forensics, and keystroke biometrics. Information was made available to students regarding the CyberCorps scholarships supported by the National Science Foundation for students interested in pursuing a degree in Cybersecurity at Pace University and working for the federal, state or local government upon graduation.

Program Structure

The PCCC research team consisted of a total of 17 URM students in the spring semesters of 2013 and 2014. Students were made aware of the program by advertising on campus via posters, flyers, email blasts and most importantly, faculty announcements in class. Students were interviewed and were selected by the following criteria:

- Computer Science, Engineering Science, Electrical Engineering Technology or Information Technology Major;
- Grade Level, (at least 3rd semester);
- GPA 2.5 [1];
- Student schedule availability.

Students with a lower GPA were considered; however, motivation and commitment are important factors to consider when selecting students that are struggling academically. Once a cohort is recruited; all of the students meet each other via a kick-off meeting and expectations are made clear to all students.

The program was modeled similarly to an agile design approach that is utilized in the Doctor of Professional Studies program at Pace University (Alipui, et al., 2014). Students traveled to Pace from Paterson, NJ, four times during the semester and worked on various problems onsite and in-between sessions that would ultimately result in a research paper submitted to Pace's Annual Research Day Conference. The four sessions are briefly described.

Session 1 included an introduction to Pace's Cybersecurity Program and the CyberCorps: Scholarship for Service Program. Students were exposed to active areas of research in biometrics and an overview of the research conducted at Pace University. Students also participated in data capture exercises to enroll them into a mobile biometric authentication system and later perform a live test of the system. A university tour with an admissions representative including information about transfer and scholarships was also given. Assignments for this session were to perform a literature review on keystroke and mobile biometrics in order to build context and learn best-

[1] GPA requirement was lowered in order to motivate the average students, which helps to increase retention, graduation and ultimately transfer.

practices in writing a research paper. Data Capture exercises were conducted for the students to begin the enrollment phase of the biometric system.

Session 2 consisted of an introduction to data, analysis, and reporting. Elementary data analysis techniques were introduced, such as Euclidean distance and the nearest neighbor classifier. Biometric system analysis was described, including system evaluation in terms of empirical error rate. After this session, students began drafting their research paper and drawing conclusions based on several biometric experiments.

Session 3 prepared students to write a research paper for journal submission. Research methodology, specifically concerning biometrics and cybersecurity was introduced. After this session, students collaborated in order to complete the paper and submitted to the Research Day conference.

Session 4 was the final session where students presented their findings at Pace University's Research Day Conference.

Two or more weeks are needed in order for students to complete the assignments in-between sessions. An advisor on the community college side must manage the program and follow-up with students in order to ensure that work is being completed in a timely manner. Meetings are required at the community college sites in-between sessions where students can further collaborate on their projects and stay on track with their responsibilities. Online collaboration tools such as Google Docs/ Hangouts and Microsoft One Drive were introduced to the students to encourage collaboration outside the classroom.

Student Projects

Students were afforded the opportunity to learn about general biometric topics, keystroke biometrics, mouse motion, and touchscreen gestures on mobile devices all via hands-on experiments. Behavioral biometrics is a growing area of research in cybersecurity, as suggested by recently issued RFPs by DARPA (DARPA, 2013) and the recent designation of the Defense Forensics & Biometrics Agency, established by the Secretary of the Army as an agency dedicated to biometric defense applications (McHugh, 2013). Several market reports indicated that biometrics will be about $20 billion industry by 2020-2024 (TechSciResearch, 2015; Tactica, 2015).

Utilizing hands-on activities at a level that the individual student can understand and appreciate has proven to better engage, motivate and increase student STEM proficiencies (Davis, et al., 2012). A biometrics project is ideal for this scenario as this field is itself extremely multidisciplinary, drawing from other fields such as human-computer interaction, machine learning, and hardware and software design.

Biometrics background

Biometrics is the study of utilizing measurable human characteristics to identify, verify and authenticate an individual. There are two major classes of biometrics: physical and behavioral. Physical biometrics consists of fingerprints, facial features or scanning an individual's iris. Behavioral biometrics includes analyzing a person's behavior, such as the manner in which a person walks (gait), eye movement, or keystroke input. There is not always a clear distinction between the two, as speech is considered both a physical and behavioral biometric since the way a person speaks depends on both physiology and behavior.

Behavioral biometrics, such as those that involve human-computer interaction, have become an increasingly popular solution for certain cybersecurity applications. It is believed that intrusion detection systems based on behavior may offer a robust solution to keeping networks and physical computers secure. Continuous authentication systems are designed to re-authenticate an individual continuously while an application is in use to offer greater security. Identify verification also bodes a solution, as a number of courses are now freely available online through massively open online (MOOC) course providers. Online course provider Coursera has begun offering certificates of course completion by verification of the student through keystroke dynamics, among other factors (Maas, et al., 2014).

A biometrics authentication system is typically evaluated based on empirical error rates from simulated authenticate scenarios. There are two types of errors that can occur during authentication: a false rejection occurs when a genuine user attempts to authenticate and is rejected by the system, and a false acceptance occurs when an imposter successfully authenticates as another user. These correspond to Type I and Type II errors in statistics, respectively.

In simulating many genuine and imposter authentication scenarios, the empirical false reject rate (FRR) and false acceptance rate (FAR) can be determined. There is a direct tradeoff between the FRR and FAR, which is controlled by a system parameter. The receiver operating characteristic (ROC) curve is a summary of the relationship between FRR and FAR, as a function of the system parameter. Typically, the performance of a system is summarized by the equal error rate (EER), the point on the ROC curve at which the FRR and FAR are equal.

Keystroke biometrics project

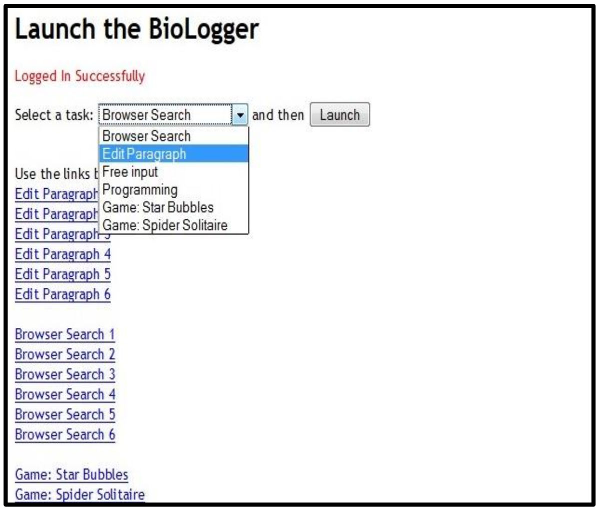
In the spring of 2013, the students embarked on a keystroke biometric research project. The project focused on authentication of an individual user based on his/her various behavioral patterns on a desktop computer, such as typing and mouse movement.

The project was executed in four phases: first, the students collected data to simulate enrollment in a keystroke and mouse biometric authentication system. Next, students contemplated various behavioral traits that would be indicative of a user's identity. This was done with the help of experts from Pace, and ultimately a set of features were developed to capture user behavior. Experiments were then designed and carried out to simulate many genuine and imposter authentication scenarios. Finally, students reported their findings in a research paper.

Data collection

The enrollment phase included performing three tasks: editing text, navigating a web browser, and online gaming. The text and browser tasks consisted of six different scenarios each while the online gaming task consisted of two scenarios that were repeated six times each. For all three tasks, participants were asked to complete two scenarios for practice one time, and then complete all scenarios in each task one time. The students began collecting data during the sessions held at Pace and completed data collection independently as necessary.

During each task, all the user's interactions with the computer were recorded. The information obtained includes the timestamps of keys pressed and released on the keyboard, mouse pointer coordinates, and clicking and scrolling actions performed with the mouse. Events were logged by a cross-platform Java application developed at Pace University that utilizes the jnativehook library to register system-wide hooks (kwhat, n.d.). The data was transmitted by the logger to central server for processing. Figure 1 shows the web interface students used to launch the logger (via Java Web Start) and begin each task.



Launch the BioLogger

Logged In Successfully

Select a task: Browser Search and then Launch

Use the links t

Edit Paragraph

Edit Paragraph

Edit Paragraph

Edit Paragraph 4

Edit Paragraph 5

Edit Paragraph 6

Browser Search 1

Browser Search 2

Browser Search 3

Browser Search 4

Browser Search 5

Browser Search 6

Game: Star Bubbles

Game: Spider Solitaire

Figure 1. BioLogger Task Selection Interface

Edit tasks

Edit tasks are typical of activities performed by computer users. The tasks for this study were designed to induce a significant cognitive load and require hand-eye coordination and manipulation of the mouse and/or the keyboard. Six edit scenarios were prepared. Students were presented with a portion of text that they had to edit to match another non-editable portion of text on the screen. A typical sample edit scenario is listed below. The **given** text is what the student had to modify to make it match the **accepted** text, and the **edit** text highlights the changes that had to be made for the student to complete the task. In the edit text, insertions are underlined, and deletions are denoted by a strike through.

> **Given** Koobface is a computer worm that spreads through social networking sites. Its name is an anagram for Facebook. The worm aims at web users...
>
> **Edit** Koobface is a multi-platform computer worm that spreads primarily through social networking sites. Its name is an anagram for Facebook. The worm ~~aims~~ targets ~~at w~~Web users...
>
> **Accepted** Koobface is a multi-platform computer worm that spreads primarily through social networking sites. Its name is an anagram of Facebook. The worm targets Web users...

Each of the six edit tasks were designed to require either *minor edits* that do not alter the meaning of the text, such as the correction of typos, or *moderate edits*, such as structural reorganizations and word substitutions.

Browser tasks

Browsing tasks were designed to induce a typical web browsing session. There were six web-browsing scenarios, each containing instructions similar to those below.

- Open a browser and go to Yahoo: http://www.yahoo.com/
- Click on Sports (left menu) MLB (top menu) Teams (top sub-menu) Boston Red Sox Team Report for the Boston Red Sox
- Go back two pages
- ...
- Exit tab or browser

Gaming tasks

The students were required to complete 12 game-playing sessions, six sessions for each of two games: Spider Solitaire and Star Bubbles. The games were selected to require heavy interaction with the computer, in comparison with the edit and browse tasks. Both games are operated primarily by the mouse, with little or no keystroke information recorded during these sessions. They are both web-based and run in a typical browser. After launching the logger, students were directed to read the rules for each game before the first session of that game. For each sessions, they were instructed to play one hand (Solitaire) or one round (Star Bubbles), attempting to finish the game.

Dataset summary

The average number of events per sample for each type of event is shown in Table 1.

Table 1: Average number of events per sample for each task

	Number Events			
Task	Motion	Click	Scroll	Keyst.
Edit	4.5k	28	1	233
Browse	4.6k	33	108	107
Solitaire	12.6k	86	29	15
Star Bubbles	8.3k	110	46	5

Feature extraction

As part of the second phase of the project, students worked with researchers from Pace to develop a set of features that capture user behavior. This involved introducing students to previous research in keystroke dynamics, which includes a well-established set of features (Tappert, et al., 2010).

Keystroke dynamics

Keystroke biometrics has developed around the concept that each individual possesses distinctive, measurable typing characteristics and that any variation is improbable to duplicate by an imposter. Although keystroke biometrics has been one of the least studied behavioral biometrics, it is gaining in popularity due its low-cost and ubiquity. A keystroke event is generated when a key on the keyboard is pressed and released. The events occur in a sequence ordered by the timestamp of the press action, and each keystroke event contains the name of the key, the press time, and the release time.

The set of features used in this experiment were adapted from (McHugh, 2013). A total of 218 keystroke features are used, consisting of means and standard deviations of keystroke duration and latency times. The duration is the time that a key is held down for. There are four different types of latencies, and only two are used here: a release-press (RP) latency is the time from the release of a key to the time of the press of the next key. A press-press (PP) latency is the time between the presses of successive keystrokes. While a RP latency can be negative when the second key is pressed before the first one is released, and PP latency is always positive since the press timestamps in the sequence of keystrokes is monotonically increasing. The first 218 keystroke features in Appendix A of (McHugh, 2013) are used to obtain experimental results for the students.

Subsequent data pre-processing includes outlier removal and normalization as described in (McHugh, 2013). Since some tasks are dominated by interaction via the mouse and not the keyboard, a mechanism for dealing with missing data is needed. A linguistic fallback hierarchy, also described in (McHugh, 2013) is used to account for missing keystrokes. This ensures that keystroke features will not contain null values. Infrequently occurring keys are augmented with observations from other keys before computing the feature value.

Mouse Motion Biometrics

The mouse input device is widely used today, and it is believed that mouse movement or touchpad behavior is unique to an individual and can be utilized as a method of authentication. While keystroke biometrics has seen an increase in research recently, mouse dynamics research remains largely untested (Betances, et al., 2014).

As part of the project, students worked with researchers from Pace to define a set of features to capture mouse behavior. The set of features includes measurements of motion, clicking, and scrolling.

Motion events are captured when a user moves the mouse. Each motion event contains a timestamp and the screen coordinates of the pointer. The distributions of three point-to-point measurements are considered: velocity, direction, and angular velocity.

Click events are generated when the user presses the left or right mouse buttons. Along with the button and the press and release timestamps, the event record contains the pointer coordinates at both the press and the release of the button. The event records in the sequence of click events from a sample are first labeled according to the “type of click” the user intended to perform. The three types of clicking actions that may occur are single clicks, double clicks, and drag-and-drops, corresponding to the three commonly occurring mouse-button interactions. Double clicks are characterized by the elapsed time between the press timestamps of consecutive click events. The default timing threshold between click events on Windows is 500ms (Microsoft, 2015), and click events which occur within 500ms of each other generate a double-click system event. Similar to keystroke, there are four different transition times that can occur between successive click events and only the RP and PP latencies are considered here.

Scroll events are generated when a user spins the wheel of a mouse in either direction to navigate quickly to off-screen elements in an application. Each scroll event contains a timestamp, the direction and amount of rotation, and the location of the pointer on the screen.

For a complete set of mouse features, see (Betances, et al., 2014).

Experiment design

After the data was collected and preprocessed, the authentication scenarios were simulated. The preprocessing and simulations were performed by Pace, on behalf of the PCCC students using an authentication system developed at Pace over several years (Monaco, et al., 2013).

To obtain authentication results, a leave-one-out cross-validation (LOOCV) procedure was used. LOOCV has low bias and high variance and is often used with small amounts of data as in this project. It simulates an authentication between every sample and enrolled user.

In total, there were 16 students who provided 6 samples from each task. This includes data collected from the PCCC students and several graduate students at Pace University. Thus, there are $1536 = n \times n \times m$ authentications, where n is the number of users and m is the number of samples per user. Out of these, there are $n \times m$ genuine authentications and $n \times (n - 1) \times m$ imposter authentications. The number of false rejects and false acceptances are tallied to obtain the FRR and FAR in deriving the ROC curve. For more detail of the authentication system, see (Monaco, et al., 2013).

Using the classification system developed at Pace (Monaco, et al., 2013), experimental authentication results were obtained for each task and each modality, as well as combined modalities. The results are shown in Table 2, where task 1=edit, 2=browse, 3=Solitaire, and 4=Star Bubbles. It is clear that performance varies drastically between each task and modality, although it generally increases when various modalities are combined. This demonstrated to the PCCC students the importance of multi-factor authentication and multimodal biometric systems.

Table 2. Keystroke and mouse experimental results.

Task	Motion	Click	Scroll	Keyst	Multi
1	8.3	22.3	50.0	10.1	4.2
2	9.4	34.5	26.5	21.4	6.3
3	4.2	22.9	8.3	22.2	4.2
4	5.2	21.8	11.2	33.3	5.5
Avg	6.8	25.4	24.0	21.8	5.0

Mobile device biometrics

In spring of 2014, PCCC students participated in a similar joint project with Pace University utilizing mobile touchscreen behavior. Based on the success of the project from previous year’s students, the mobile project was structured similar to the keystroke and mouse biometrics project. The mobile biometrics project focused on user identification, instead of authentication.

Mobile Biometrics background

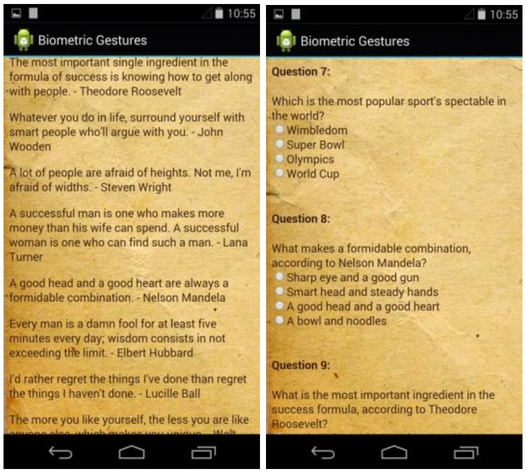
Mobile or handheld devices are becoming increasingly important in our society as users are adopting the technology both for recreational and business purposes. According to a report by MobiForge in May 2014, there are nearly 7 billion mobile subscriptions worldwide. That translates into 95.5% of the global population (Mobithinking, 2014). Moreover, mobile phone sales worldwide have increased 8% since 2013, and tablets have experienced a whopping 79% increase in sales. Conversely, PC/laptop sales have experienced a precipitous decline over the past three years. Since 2013, worldwide sales of PC/Laptop sales have decreased by 11% (Rivera & Goasduff, 2014). The explosive growth and adoption of mobile and tablet devices warrants the need for a new biometric to emerge in order to better authenticate users across this growing medium. Very few studies have been conducted in this domain, one notable research effort occurred in 2012 in Hong Kong (Meng, et al., 2012). The researchers analyzed various gestures that are commonly used on a mobile device and derived a low EER rate of 3%.

Mobile biometrics applications generally consist of three major components. The first component is the touchscreen that is now widely considered the most adopted interactive panel for mobile devices. The second component that will assist in developing a mobile biometric system is the gesture recognition capability of the device. With regards to Android-based devices, the following are the core gestures supported as listed in the Android Developers Documentation (Google Inc., 2014): touch, long press, swipe or drag, long press drag, double touch, double touch drag, pinch open, pinch close.

The third component for a mobile biometric system consists of the device sensors. Sensors are typically grouped into three categories: motion sensors, position sensors, and environmental sensors. Motion sensors are used to measure acceleration and rotational forces along the axes (Google, 2014). Position sensors are used for capturing data about the physical position of the device (Google, 2014). Environmental sensors are used to measure environmental considerations.

Data collection

During two sessions held at Pace, the PCCC students collected data on LG Nexus 5 devices using an application developed by Pace graduate students. The application prompted students to answer a series of questions that required navigating a web page, reading text, and studying an image. During this time, the application sampled the screen and various sensors at a rate of about 1 kHz. An example of the data capture interface is shown in Figure 2. Each student recorded approximately 15,000 samples during each session, where a single sample consists of the touchscreen and device sensors values at an instant in time.



The most important single ingredient in the formula of success is knowing how to get along with people. - Theodore Roosevelt

Whatever you do in life, surround yourself with smart people who'll argue with you. - John Wooden

A lot of people are afraid of heights. Not me, I'm afraid of widths. - Steven Wright

A successful man is one who makes more money than his wife can spend. A successful woman is one who can find such a man. - Lana Turner

A good head and a good heart are always a formidable combination. - Nelson Mandela

Every man is a damn fool for at least five minutes every day; wisdom consists in not exceeding the limit. - Elbert Hubbard

I'd rather regret the things I've done than regret the things I haven't done. - Lucille Ball

The more you like yourself, the less you are like

Question 7:

Which is the most popular sport's spectable in the world?

○ Wimbledom
○ Super Bowl
○ Olympics
○ World Cup

Question 8:

What makes a formidable combination, according to Nelson Mandela?

○ Sharp eye and a good gun
○ Smart head and steady hands
○ A good head and a good heart
○ A bowl and noodles

Question 9:

What is the most important ingredient in the success formula, according to Theodore Roosevelt?

Figure 2. Mobile data capture interface

The touchscreen data that was collected includes the location of each pointer (finger) on the screen, the pressure applied by each pointer, and major and minor axes of an ellipse approximating the pointer size. An example of the screen coordinates from a series of gestures from two users is shown in Figure 3.

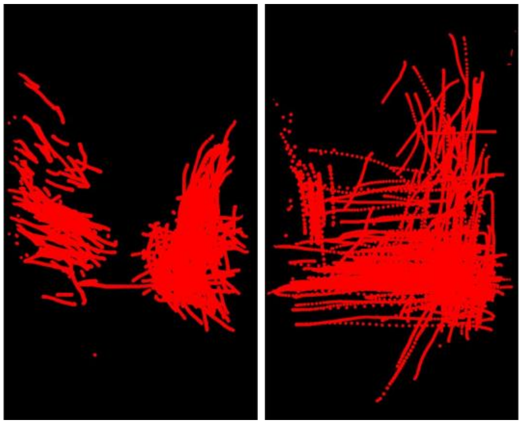


Figure 3. Touchscreen gestures recorded.

In addition to touchscreen data, sensor-based data was recorded from the following device sensors.

Gyroscope: measures the rate or rotation around the device's axes and is used to maintain orientation of the device.

Accelerometer: measures the acceleration applied to the device, including the gravity force.

Linear Accelerometer: provides a three-dimensional vector representing acceleration along each device axis, excluding gravity.

Orientation: allows monitoring the position of a device relative to the earth's frame of reference, i.e. portrait vs. landscape orientation.

A feature vector was formed from the touchscreen and sensor values in each sample. For more details on feature extraction and data preprocessing, see (Alotaibi, et al., 2014).

Experiment design

Experimental results were obtained by Pace University graduate students and presented to PCCC in session three of the project. PCCC students were then able to include the results in their paper submitted to Pace's Research Day conference.

Results were obtained using a decision tree classifier generated by the C4.5 in Weka using a

10-fold cross-validation. Using data from both sessions yielded an identification accuracy of 98.4%, which is on par with other studies containing a similar amounts of data. Since the data was collected in two different sessions, results were also obtained using the data from the first session as the training set and the second session as the testing set. In this case, identification accuracy dropped to 25%. This demonstrated to the PCCC students the problem of template aging, an issue that continues to arise in various biometric applications.

Outcome

Overall, 25 URM students participated in the partnership throughout 2013-2014. 17 students participated in the research project, and 8 participated in the outreach workshops. Out of the 25 students that participated, 22 (82%) graduated PCCC and are enrolled in a four-year STEM program. A few of the students in the cohort have not completed their degrees due to their part-time student status. It should be noted that a few students expressed interest in participating in the project during the recruitment phase; however, due to conflicts with their work schedules, they were unable to participate. Full-time employment can be a hindrance for students trying to achieve their degree in a timely fashion. According to the Chronicle of Higher Education, 71% of part-time students had not completed their associates within three years (Supiano, 2010). Many of these students must work a full-time job in order to support themselves and pay tuition. In order to help address this issue, PCCC applied for and was awarded a $4.1M Title V STEM grant from the Department of Education, and a $1.5M Bridges to Baccalaureate grant from the National Science Foundation, which provides stipends to students participating in research projects and supports other STEM activities. These grants provide the student with some financial assistance and support resources which allows students to focus more on their studies as opposed to work obligations and leverage resources to ensure STEM student success.

Conclusions

Students were asked to submit a reflection paper after the research project that summed up their experience with the project. We will summarize the key points mentioned by the students in this section to provide readers an idea of the key value gained from the experience. Many students mentioned how the biometrics research project expanded their current knowledge of technology. Students recognized the importance of security as they have read about the many data breaches that have occurred in the private and public sector. Many were not aware of biometrics as a study and career option, nor the high demand and growth potential for cybersecurity professionals. The project has increased their awareness and many are considering a career in cybersecurity. PCCC offers a networking option under the Information Technology degree that includes a computer forensics course. The cybersecurity research project will help expand the program and act as a recruiting tool with the goal of enrolling more students, offering more cybersecurity courses and ultimately an A.S. degree.

Pace University has emerged as a highly attractive option for transfer by offering bachelor and master's degrees in cybersecurity. Information regarding transfer is made available throughout the research program and outreach workshops. Students particularly enjoyed the college tour offered by Pace during the project as well as the staff available to assist in the transfer process.

Students also noted the program design and development, mentioning in their reflection papers how they now have a better understanding of the agile project management process. The program coordinators introduced the method before the start of the program, provided examples throughout the sessions and utilized the process during the development of the final paper.

Students found the final paper to be a rewarding experience due to the distributed nature of the assignment. The students enjoyed working collaboratively while using various online tools to complete the task before the deadline. Many students planned to use this newly acquired distributed model concept for future team projects.

Lastly, all of the students particularly enjoyed presenting their findings at Pace Research Day. The event afforded students an opportunity to meet Pace faculty and students focused on similar research areas. PCCC students had the opportunity also to learn about other research projects in biometrics as well as the emerging field of telehealth. They were extremely excited about taking home a copy of the official conference Proc. which included their paper in the publication. The research experience was highly successful and motivating for our students. Many of the students used this experience as a launchpad which would keep them working hard towards their goal and pursue their dreams. As one student best put it, "I am now aware of what is expected in order to complete a dissertation; I will now strive to complete my Ph.D."

References Cited

Alipui, G., Asamoah, C., & Barilla, R. (2014). An Agile Approach to Doctoral Research Dissertation. *Proceedings of Student-Faculty Research Day, CSIS, Pace University* (pp. D2.1 -D2.8). White Plains: Pace University.

Alotaibi, N., Barilla, ,. R., Betances, F., Chohan, A., Garcia, A., Gazarov, A., . . . Monaco, J. V. (2014). Biometric System Design for Handheld Devices. *Student-Faculty Research Day.* Pace University.

Betances, F., Pine, A., Thompson, G., Zandikarimi, H., & Monaco, J. V. (2014). Mouse Biometric Authentication. *Proceedings of Student-Faculty Research Day, CSIS, Pace University, May 2nd, 2014*, (pp. B5.1-B5.8). White Plains.

Bureau of Labor Statistics. (2014, January 8). *Occupational Outlook Handbook*. Retrieved from Information Security Analysts: http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Chen, X. (2009). *Students Who Study Science, Technology, Engineering and Mathematics (STEM) in Postsecondary Education.* Washington DC: National Center for Educatioal Statistics.

Ciaurro, W., & et al. (2014). Touch- Screen Mobile Device Data Collection for Biometric Studies. *Proceedings of Student-Faculty Research Day* (pp. B10.1-B10.3). White Plains: Pace University.

DARPA. (2013, February 11). Active Authentication (AA) Phase 2. *Broad Agency Announcement*. Arlington, VA, USA: Defense Advanced Research Projects Agency.

Davis, C. E., Yeary, M. B., & Sluss, J. J. (2012). Reversing the Trend of Engineering Enrollment Declines With Innovative Outreach, Recruiting and Retention Programs. *IEEE Transactions on Education*, 157-163.

Farnon, E. et al. (2013). A Keystroke Biometric Experiment on Edited Text. *Proceedings of Student/Faculty Research Day, CSIS, Pace University* (pp. B7.1-B7.6). White Plains: Pace University.

Google. (2014, March). *Sensors Overview*. Retrieved from Google Inc.: http://developer.android.com/guide/topics/sensors/sensors_overview.html

Google Inc. (2014, March). *Android Gestures*. Retrieved from Android API Guides : http://developer.android.com/design/patterns/gestures.html

Griffith, A. L. (2010). Persistence of women and minorities in STEM field majors: Is it the school that matters? *Economics of Education Review*, 911-922.

Kaminsky, M. E., & Anderson, E. (2008). *Identifying Game Players with Biometrics*. Retrieved from University of Seattle: http://homes.cs.washington.edu/~miro/docs/mouse_ID.pdf

kwhat. (n.d.). *jnativehook: Global keyboard and mouse listeners for Java.* Retrieved 2013, from Github: https://github.com/kwhat/jnativehook

Maas, A., Heather, C., Do, C., Brandman, R., Koller, D., & Ng, A. (2014). Offering Verified Credentials in Massive Open Online Courses: MOOCs and technology to advance learning and learning research. *Ubiquity symposium.* ACM.

McHugh, J. M. (2013). *Redesignation and Transfer of the Biometrics Identiy Management Agency as the Defense Forensics and Biometrics Agency.* Washington, DC, USA: Department of the Army.

Meng, Y., Wong, S. D., Schlegel, R., & Kwok, L. F. (2012). Touch gestures based biometric authentication scheme for touchscreen mobile phones. *Proceedings of the 8th China International Conference on Information Security and Cryptology.* Hong Kong.

Microsoft. (2015). *Microsoft Development Center*. Retrieved from Set Double Click Time Function: https://msdn.microsoft.com/en-us/library/windows/desktop/ms646263%28v=vs.85%29.aspx

Mobithinking. (2014, June 13). *MobiForge*. Retrieved from Global mobile statistics 2014 Home: all the latest stats on mobile Web, apps, marketing, advertising, subscribers, and trends...: http://mobiforge.com/research-analysis/global-mobile-statistics-2014-home-all-latest-stats-mobile-web-apps-marketing-advertising-subscriber

Monaco, J. V., Bakelman, N., Cha, S., & Tappert, C. C. (2013). Recent Advances in the Development of a Long-Text-Input Keystroke Biometric Authentication System for Arbitrary Text Input. *European Intelligence and Security Informatics Conference (EISIC).* IEEE.

Moodle bioauth plugin. (n.d.). Retrieved 2014

Rivera, J., & Goasduff, L. (2014). *Gartner Says Worldwide Traditional PC, Tablet, Ultramobile and Mobile Phone Shipments Are On Pace to Grow 6.9 Percent in 2014.* Egham: Gartner.

Supiano, B. (2010, December 1). *Half of All First-Time Students Earn Credentials Within 6 Years*. Retrieved from The Chronicle Of Higher Education: http://chronicle.com/article/Half-of-All-First-Time/125585/

Tactica. (2015, May). *Biometrics Market Forecasts*. Retrieved May 19, 2015, from Tactica: https://www.tractica.com/research/biometrics-market-forecasts/

Tappert, C. C., Cha, S., Villani, M., & Zack, R. S. (2010). A Keystroke Biometric System for Long-Text Input. *Int. J. Info. Security and Privacy (IJISP)*, 32-60.

TechSciResearch. (2015, March). *Global Biometrics Market Forecast and Opportunities, 2020*. Retrieved May 19, 2015, from TechSciResearch: http://www.techsciresearch.com/3234

Authors

Gonzalo Perez (gperez@pccc.edu) is the Executive Assistant to the President/ Assistant Dean for Academic Affairs and a Computer Science Adjunct Professor at Passaic County Community College. His role was to help develop the model for the cybersecurity research project, recruit the students, coordinate the activities and help students collaborate on the final paper. He also held student meetings in-between sessions in order to support the tasks that students were completing and finally conducted a closing meeting in order to reflect on the project outcome and assess student impact.

John V. Monaco (jmonaco@pace.edu) is an Adjunct Professor at Pace University, where he is also pursuing a Ph.D. in Computer Science under the supervision of Dr. Charles Tappert. In 2013, John was named one of Westchester's "Top Professionals under 30" for research in keystroke biometrics at Pace University. He has authored or coauthored over a dozen publications as a Ph.D. student and placed 1st in an international competition on identifying users based on eye movements. John currently attends school under a full scholarship provided by the Department of Defense. His role was to develop the applications used for data collection and obtain experimental results.

Charles C. Tappert (ctappert@pace.edu) has a Ph.D. in Electrical Engineering from Cornell University and was a Fulbright Scholar. He worked on speech and handwriting recognition at IBM for 26 years, taught at the U.S. Military Academy at West Point for seven years, and has been a professor of computer science at Pace University since 2000. He has over 100 publications and his research interests include pattern recognition, biometrics, handwriting recognition/pen computing, speech recognition/voice applications, human-computer interaction, artificial intelligence, and Big Data.

Li-Chiou Chen (lchen@pace.edu) is a Professor at Pace University. She has a Ph.D. in Engineering and Public Policy from Carnegie Mellon University. Her publications and research interests have been focused on computational models for Internet-based attacks, user authentication, security usability and computer security risk perception. She is the principal investigator of Pace's CyberCorps: Scholarship for Service program, supported by the National Science Foundation.