Teaching Secure Coding in Introductory Programming Classes

Siddharth Kaza
Blair Taylor
Towson University

http://www.towson.edu/securityinjections

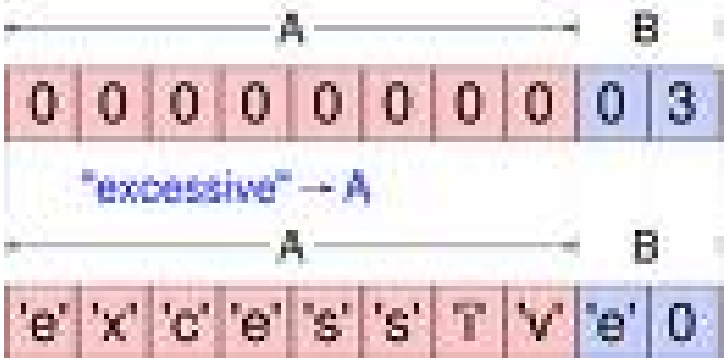
Software Vulnerabilities

- Vulnerability – weakness in the software
- Estimated 1 to 7 defects per thousand lines of code
- For large system with millions of lines of code
  - => thousands of vulnerabilities

Big Three

- Buffer overflow
- Integer overflow
- Input validation

Three programming errors are responsible for 85% of vulnerabilities (SANS, 2006)



Software Security begins with Education

It is our job to teach secure coding

"I think the most critically important part of delivering secure systems is raising awareness through security education."

Bill Gates, Microsoft

"The ability to write secure code should be as fundamental to a university computer science undergraduate as basic literacy."

Matt Bishop, UC Davis

"The first and foremost strategy for reducing securing related coding flaws is to educate developers how to avoid creating vulnerable code."

Robert C. Seacord, CERT

The current state of undergraduate security education…

Too little, too late

- Security tracks
- Security classes
- Reaches only a subset of students
- Courses occur late in curriculum
- After students have learned fundamental coding and design

Secure coding education in a perfect world …

Create a Security Mindset

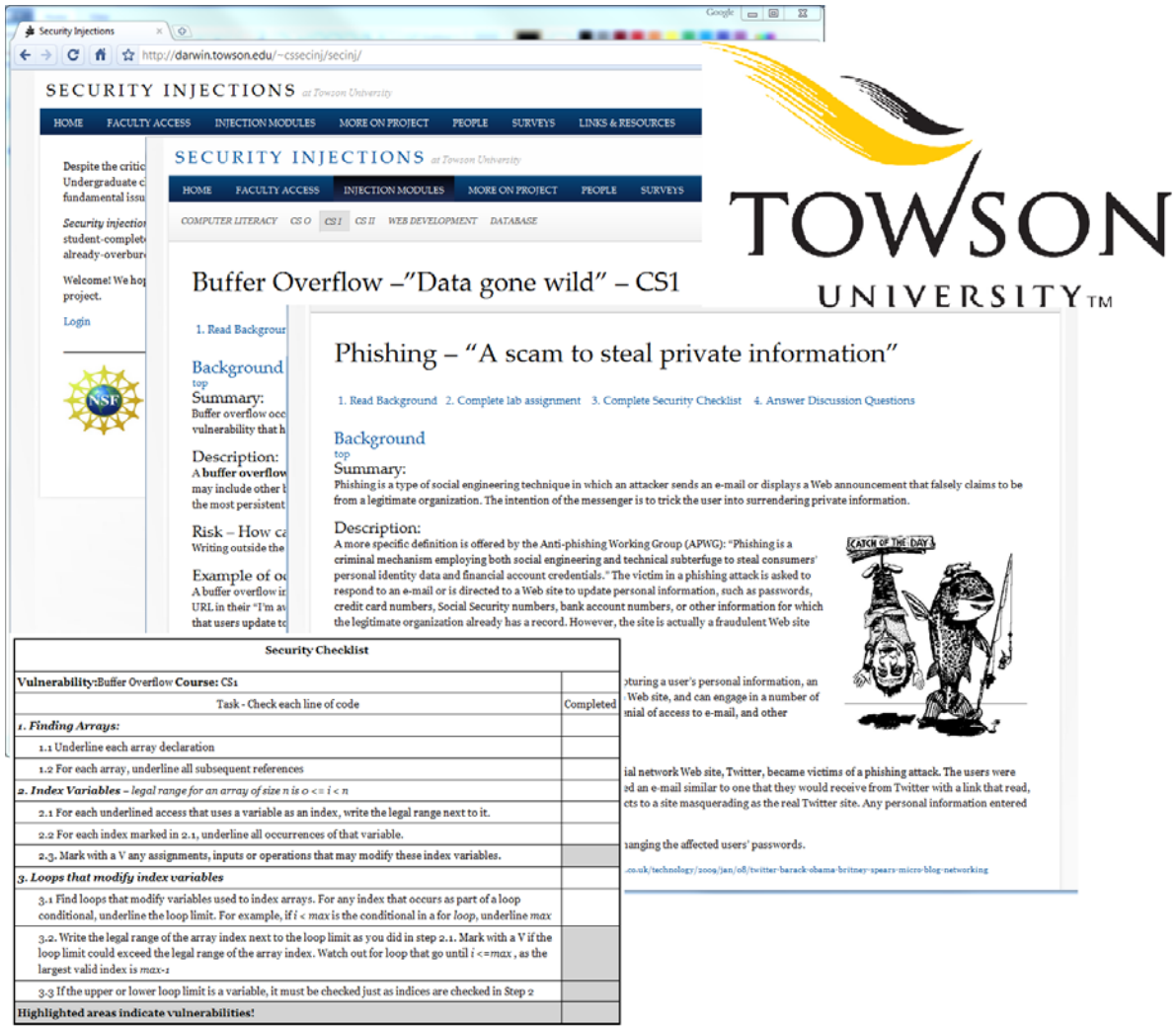
Early and Often

Importance of Curricular Guidelines

- ACM/IEEE Computer Science 2013 Curriculum
  - In CS2013, the Information Assurance and Security (IAS) Knowledge Area (KA) is added to the body of knowledge
- NSA CAE Accreditation
  - The guidelines include mapping to new knowledge units (KUs)

Security Injections @Towson

- 26 Modules
- CS0, CS1, CS2
  - Buffer Overflow
  - Integer Error
  - Input Validation
- Computer Literacy
  - Phishing
  - Cryptography
  - Passwords
- Minimally invasive
- Security Checklists



http://www.towson.edu/securityinjections

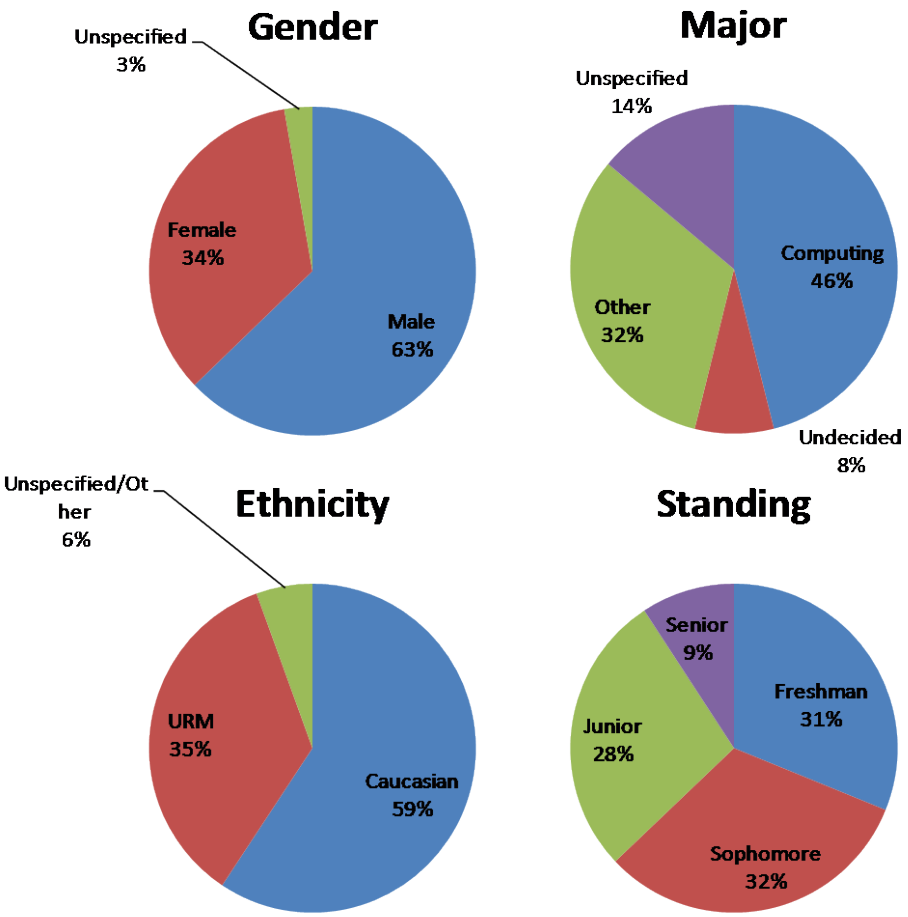
Assessment Design and Results

- Four primary goals to assess
  1. increasing the number of security-aware students
  2. increasing students' security awareness
  3. improving students' ability to apply security principles
  4. increasing faculty security awareness

- Instruments
  - student and faculty surveys
  - random sampling of assignments
  - qualitative inputs from faculty
  - controlled experiments in classrooms
  - institutional quantitative data

Results – increase number of security-aware students

- 1,630 survey responses

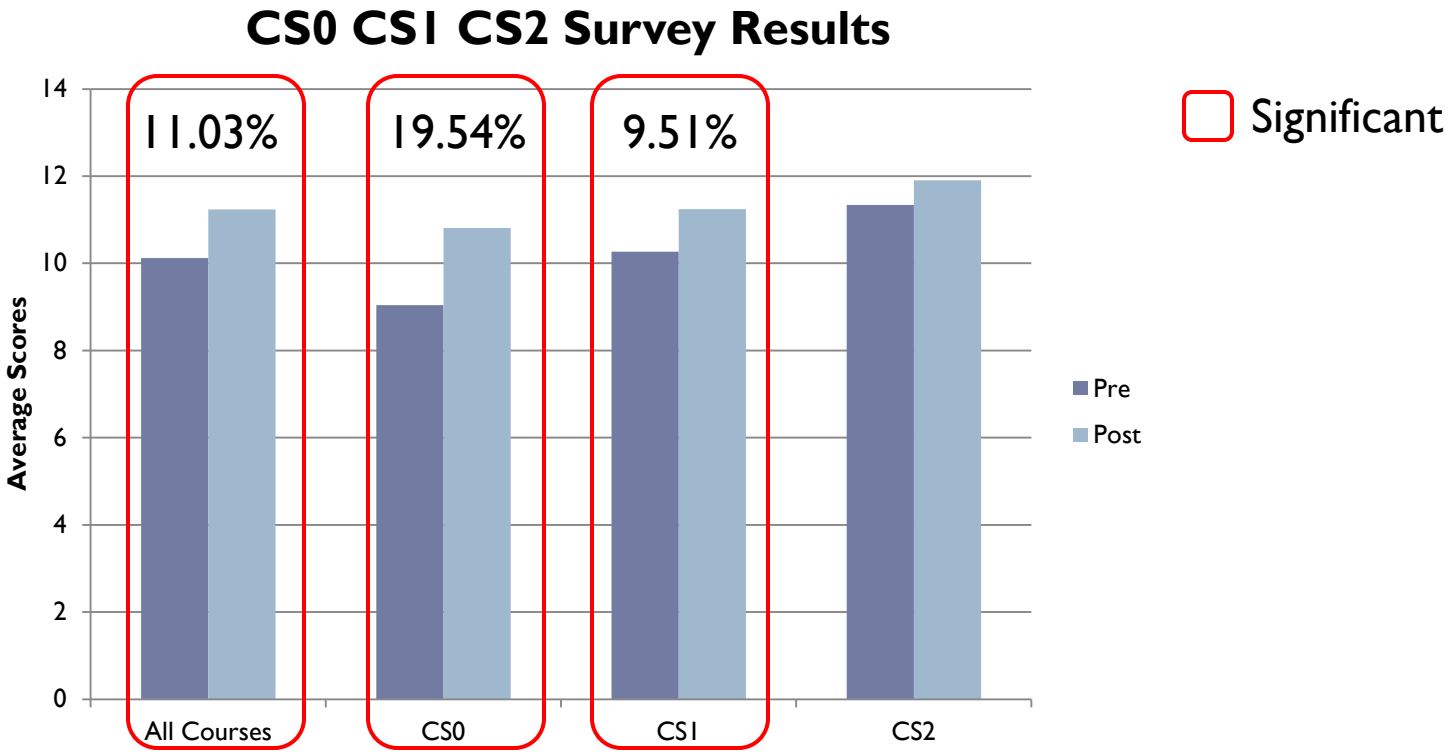


Increase in Student Awareness – Assessment Design

- Two strategies need to be evaluated
  - Test security awareness at the end of foundational courses
  - Test security awareness due to repeated exposure

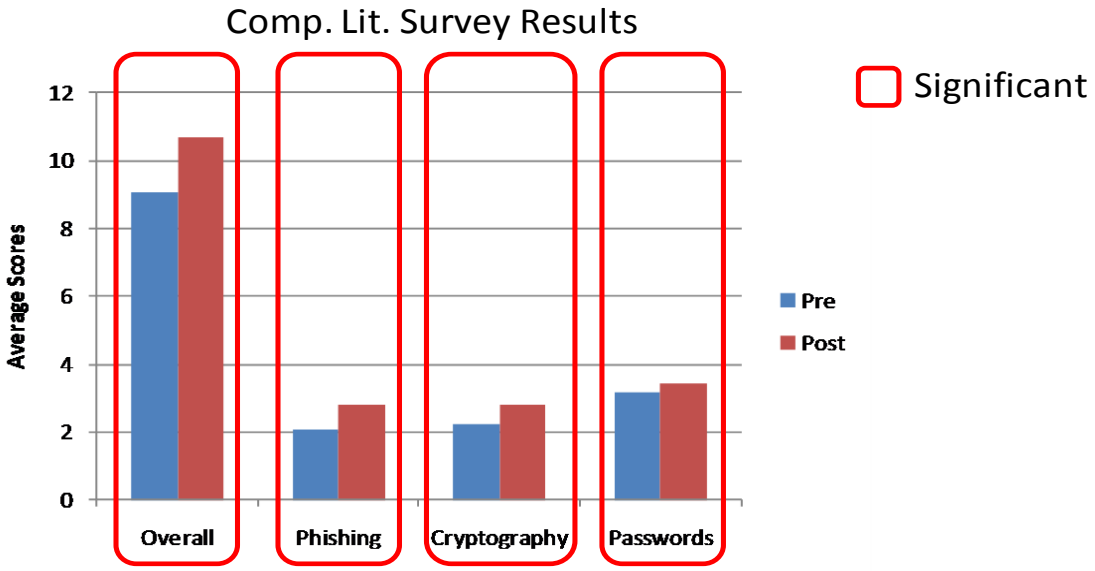
- All classes were administered a pre-survey and a post-survey
  - Each survey has
    - demographic information
    - general security awareness questions, and
    - questions targeted at the injections (secure coding for CS0,1,2)

Results – Student Awareness



- 1,026 survey responses, 40+ sections, 5 institutions
- Significant increase ($p<0.01$) in across core courses, CS0, and CS1
  - but not in CS2 (topic fatigue in CS2?)
- These results persisted across majors

Results – Student Awareness

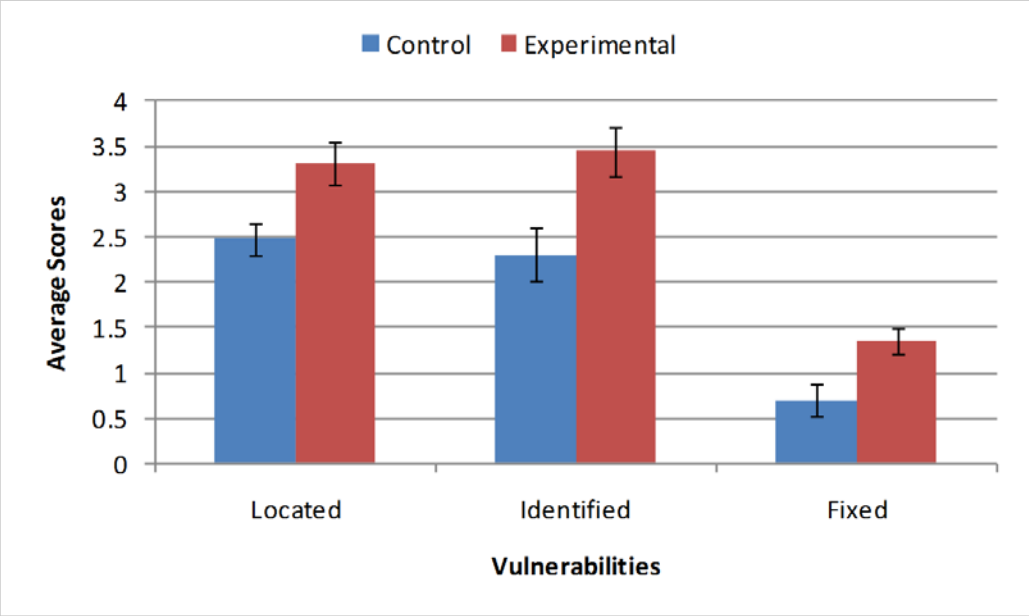


- 384 survey responses, 4 institutions
- Significant increase in all modules in computer literacy
- These results persisted across gender and ethnicity

Increase in Student Ability to Apply - Split Sections

- Another quasi-experimental strategy was to have one integrated section and one control section under the same instructor.
- Pre-surveys and post-surveys were administered in both the sections.
- In addition, a more stringent 'code-check' was given at the end

Results – Split Section



- CS0 and CS1 students (four sections) using the modules are significantly better at Locating, Identifying, and Fixing vulnerabilities

Outreach

- Build-a-Lab Program
  - Requests proposals to design lab modules on security topics
  - Three semesters
    - 1 – Design
    - 2 – Pilot & Revise
    - 3 – Assess

- Security Ambassadors Program
  - Identifies faculty from workshops who can acquire a leadership role in teaching with and disseminating the injection modules
    - Year 1 – hold a secure coding workshop in their home institution
    - Year 2 – hold a secure coding workshop/present paper at regional conference (with travel support)
    - Continue to work on cybersecurity education

www.towson.edu/splash

Secure Programming Logic Aimed at Seniors in High School

Background

- Need for software developers, need for IA professionals
- Colleges and universities
  - Low numbers of underrepresented populations (UP)
  - High drop out rates
    - underprepared and/or feel that they are underprepared
- High Schools
  - CS AP exam
    - 7% of all AP tests taken
    - 5% of public high schools offer CS AP (2,100 out of 42,000)
  - Lack of instructors
  - CS not required part of the curriculum
  - Situation is worse for Ups: females, African Americans, Hispanics, and urban and rural students
  - Pipeline issue
- ***Meeting the workforce needs depends on reaching all UP***

SPLASH goals:

- Increase the interest and participation of students from underrepresented populations in computing and IA majors.
- Prepare students from underrepresented populations for college majors such as computer science, information science, information assurance, and engineering.
- Create a sustainable model for introducing students from underrepresented populations to secure programming.

SPLASH plan:

- Develop a *SPLASH Learning Environment*
  - pilot-tested learning environment that supports anytime-anywhere learning
  - College credit
  - programming logic course
  - laboratory modules that introduces critical secure coding concepts.
- Build a *SPLASH Community*
  - Includes educators and students
  - Tools
  - facilitate recruitment, mentoring, and outreach to ensure a sustainable and successful program
- Create a *SPLASH Endurance* Component
  - build a sustainable model that will increase interest and preparedness among high school students lacking access to CS curricula.

SPLASH details

- Piloted Fall 2012, In progress Fall 2013
- Dr. Alfreda Dudley and Dr. Blair Taylor
- COSC175: General Computer Science
- Programming Logic Course
- 4 credits: 3 hours lecture/1 hour lab
- C++
- Software Security/Secure Coding
- http://pages.towson.edu/btaylor/cosc175/syllabus/syll_175fa13.htm

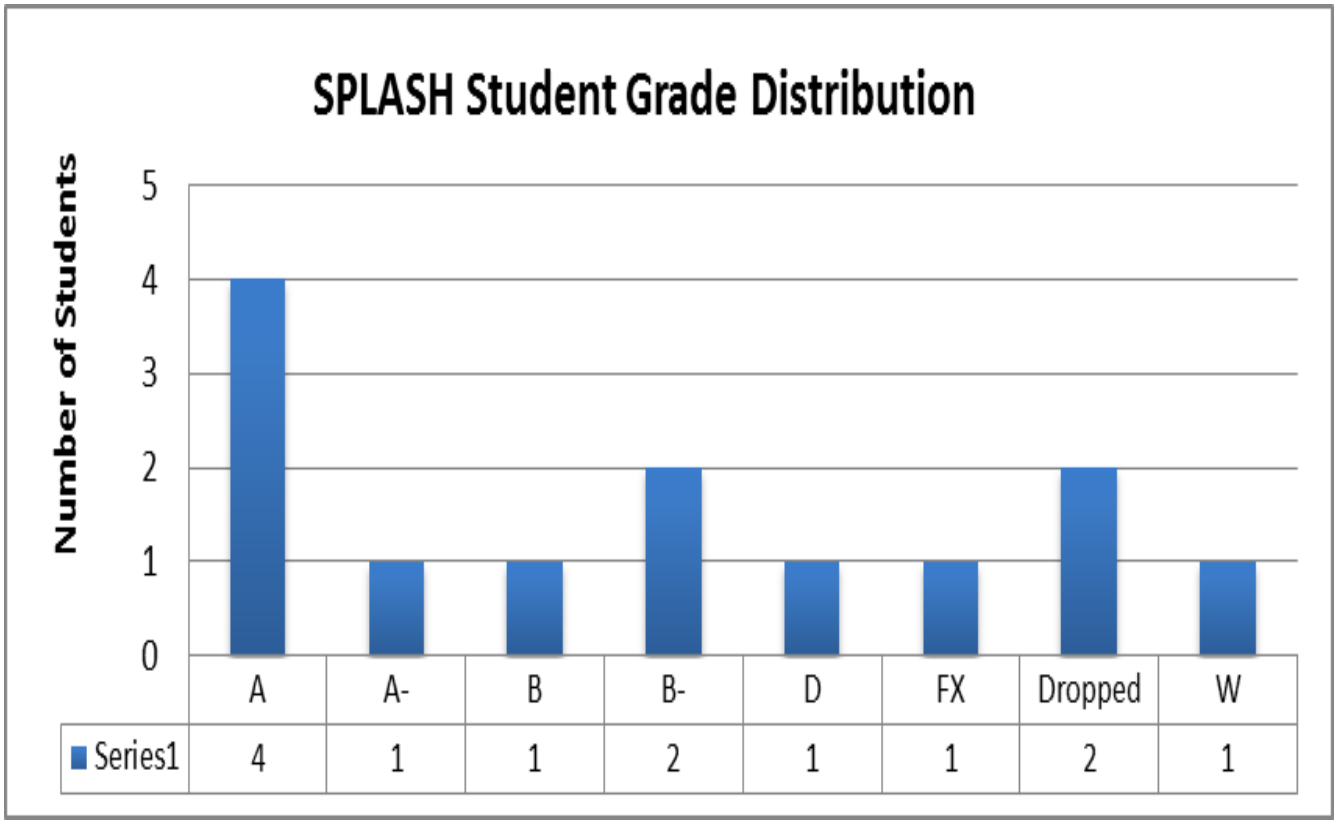
Tools

- Videotaped classes
- Onsite support:
  - Coordinators at each high school
  - responsibilities included: proctor tests and exams, help with scheduling, consultation, grading, logistical issues, and communication with the SPLASH professor
- A private social networking support group for the SPLASH students (Facebook)
- Near-peer mentors: Two female undergraduate computing students mentors from Towson University
- Email, Skype, Google Hangout, Telephone

Results

- The majority of SPLASH students earned a grade of "B-" or higher.
- Three of the SPLASH students finished in the top 10% of all the students.
- Two of the top three grades in the course were earned by the SPLASH students.
- Some of the most creative projects submitted were by the SPLASH girls.
- Four SPLASH students did not successfully complete the course.

Results


SPLASH Student Grade Distribution
Number of Students
5
4
3
2
1
0
A
A-
B
B-
D
FX
Dropped
W
Series1
4
1
1
2
1
1
2
1

Challenges

- Videotaping and uploading lectures was technically and logistically difficult.
  - The hardware and software used for the pilot did not meet the needs of the project.
- Student workload.
  - For some girls, the course work and time commitment was more challenging than anticipated.
- Time consuming enrollment process.
  - The amount of time spent enrolling SPLASH students in the course was very involved and not anticipated.
- Providing additional student support.
  - In a few cases, students needed more help than their high school coordinator could provide. Students' diverse schedules and geographic locations resulted in frequent one-on-one interventions by the instructor, which is impractical as the course and program scales.
- Particular challenges at the targeted urban female high school included
  - Communication: sometimes the students did not reply to the instructor or high school coordinator.
  - Help-Seeking Behavior: the students from the urban high schools did not seek assistance with any problems they had in the course.
  - Tenacity: Students stopped attending and dropped the course; not one female African-American student enrolled in this course passed and/or completed this course.

Results from Fall 2012 Semester

- Projects
- Comments:
  - I enjoyed this class much more than I initially thought I would and it really opened the doors to programming for me.
  - I feel much more comfortable about taking future computer science classes.
  - This experience has been very exciting for me. I loved being able to tell people I was taking a class at Towson as a junior! Many of my friends were interested in it so if you continue with this program I'm sure you'd have a lot of girls signing up!
  - I've never taken an online class before and you honestly made it so manageable! Having all of the information on the syllabus was a life-saver. I found the recordings very easy to understand and being able to pause and rewind was definitely a bonus.
  - I showed my parents the programs we did in lab each week; they were really interested in everything I learned how to do.
  - I found the class to be very bearable -- even on top of my regular high school work. It got stressful at times but I don't think any of the work was unreasonable. Your lessons were easy to comprehend and all of the tests and quizzes were straight-forward! I'm very grateful that my first college class was so well organized.
  - I came into the class expecting to learn about C++ as well as programming and left with a greater understanding of computers in general and a lot about memory and other software applications.

References – Security Injections

1. Turner, C., Taylor, B., Kaza, S. 2011. Security in Computer Literacy- A Model for Design, Dissemination, and Assessment, Proceedings of the 41st SIGCSE technical symposium on Computer science education, Dallas, TX 2011.
2. Taylor, B., Kaza, S. 2011. Security Injections: Modules to Help Students Remember, Understand, and Apply Secure Coding Techniques, Proceedings of the 16th Annual Conference on Innovation and Technology in Computer Science Education (ITICSE 2011), Darmstadt, Germany.
3. Kaza, S., Taylor, B., Hochheiser, H., Azadegan, S., O'Leary, M. and Turner, C. 2010. Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design. USA. Proceedings of the 14th Colloquium for Information Systems Security Education, Baltimore, MD 2010.
4. Taylor, B., Hochheiser, H., O'Leary, M. & Azadegan, S., Cross-site Security Integration: Preliminary Experiences across Curricula and Institutions, Proceedings of the 13th Colloquium for Information Systems Security Education. Seattle, WA 2009.

Other publications can be found at:
http://cis1.towson.edu/~cssecinj/about/publications/

References - SPLASH

[1] Askarov, A. and Sabelfeld, A. 2009. *Catch me if you can*. ACM Press.
[2] Border, C. 2007. The development and deployment of a multi-user, remote access virtualization system for networking, security, and system administration classes.*ACM SIGCSE Bulletin*. 39, 1 (Mar. 2007), 576.
[3] BytheNumbers09.pdf: *http://www.ncwit.org/sites/default/files/legacy/pdf/Bythe Numbers09.pdf*. Accessed: 2013-09-04.
[4] CS Education Statistics «_Exploring Computer Science: *http://www.exploringcs.org/resources/cs-statistics*. Accessed: 2013-09-04.
[5] desJardins, M. and Martin, S. 2013. CE21--Maryland. *Proceeding of the 44th ACM technical symposium on Computer science education - SIGCSE '13*
[6] Hill, C. et al. 2009. Why So Few? Women in Science, Technology, Engineering, and Mathematics. *American Association of University Women*. (Nov. 2009).
[7] Kaza, S. et al. 2010. Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design. *(CISSE)* (2010).
[8] Kinnunen, P. and Simon, B. 2011. CS majors' selfefficacy perceptions in CS1. *Proceedings of the seventh international workshop on Computing education research - ICER '11*
[9] Klopfenstein, K. 2004. The Advanced Placement Expansion of the 1990s: How did traditionally underserved students fare? *Education Policy Analysis Archives*. 12, 68 (2004), 1–15.
[10] PREPARE AND INSPIRE:- pcast-stemed-report.pdf: *http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-stemed-report.pdf*. Accessed: 2013-09-04.
[11] Program Summary Report_2012_revised 9-11.xls - program_summary_report_2012.pdf: *http://media.collegeboard.com/digitalServices/pdf/research/program_summary_report_2012.pdf*. Accessed: 2013-09-04.
[12] Routledge Student Engagement in Higher Education:Theoretical Perspectives and Practical Approaches for Diverse Populations (Hardback) - Routledge. Routledge.
[13] Sheehy, K. 2012. High Schools Not Meeting STEM Demand. *US News and World Report*.
[14] Single-sex education, particularly for girls, allows students to thrive - Baltimore Sun: *http://articles.baltimoresun.com/2012-01-23/news/bs-edsingle-sex-20120123_1_school-graduates-girls-schoolscoed-schools*.
[15] Software Developers_: Occupational Outlook Handbook_:U.S. Bureau of Labor Statistics: *http://www.bls.gov/ooh/computer-and-informationtechnology/software-developers.htm*.
[16] Summers, W.C. and Martin, C. 2005. Using a virtual lab to teach an online information assurance program. *Proceedings of the 2nd annual conference onInformation security curriculum development - InfoSecCD '05* (New York, New York, USA, Sep.2005), 84.
[17] Taylor, B. and Azadegan, S. 2008. Moving beyond security tracks: integrating security in cs0 and cs1. *Proceedings of the 39th SIGCSE technical ….* (2008).
[18] Taylor, B. and Azadegan, S. 2007. Teaching Security through Active Learning. *Security*. (2007).
[19] Taylor, B. and Kaza, S. 2011. Security injections. *Proceedings of the 16th annual joint conference on Innovation and technology in computer science education - ITiCSE '11*
[20] The Comprehensive National Cybersecurity Initiative |The White House: *http://www.whitehouse.gov/issues/foreignpolicy/cybersecurity/national-initiative*.
[21] Yardi, S. and Bruckman, A. 2007. What is computing? *Proceedings of the third international workshop on Computing education research - ICER '07*
[22] Zhao, C.-M. et al. 2004. Searching for the Peach Blossom Shangri-La: Student Engagement of Men and Women SMET Majors. *Review of Higher Education*. 28, 4 (Nov. 2004), 503–525.