School of Computer and Information Science

Engaging Students through Reflective Practice Assessment within a Software Security Lifecycle

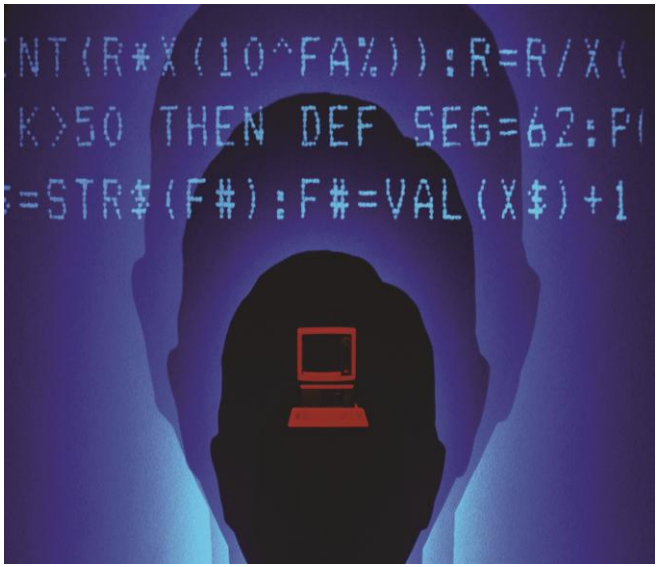
Elena Sitnikova

PhD, BE(Hons), CSSLP

elena.sitnikova@unisa.edu.au

Outline

- Background
- Why Reflective Practice?
- Designing and Implementing a RP Assessment
  - Goals and Objectives
  - Target Students
  - Intensive week:
    balancing theory and practicals



- Characteristics of success and challenges
- Questions and discussions

Background

- Significant challenges to protect information assets and customers' sensitive information from cyber-attacks
- In 2010 2.28 M of info security professionals worldwide; by 2015 ~4.2 M (14.2% US ; 11.9% in Asia- Pacific)
- 20 % of information security professionals reported involvement in software development.
- A clear gap in skills needed to protect organisation's systems and data, also its reputation, end-users and customers *)

*) Frost & Sullivan, 2011

Background

- Top security threat concerns: application vulnerabilities, mobile devices; and viruses and worms.
  - 75% of respondents rated **application vulnerabilities** most important.
  - Greatest proportion of application vulnerabilities - result of insecure software development and coding practices *)
- Cultural issues – communication gap between specialists with engineering skills and network security specialists with IT background.

Frost & Sullivan, 2011

Education in software security

- Critical need for cyber security education - software security in particular.
- In Australia most educational programs and information security courses focus on network security .
- Focus on theoretical aspects of software security.

Reflective Practice - Definition

- "… reflection is about maximising deep and minimising surface approaches to learning."

  Hinett, K (2002), Developing Reflective Practice in Legal Education, UK Centre for Legal Education.

- "A reflection in a mirror is an exact replica of what is in front of it. Reflection in professional practice, however, gives us back, not what is, but what might be, an improvement on the original."

  Biggs, J. (1999), *Teaching for Quality Learning at University*, Buckingham: Open University Press

Pedagogy

– Reflective practice (RP) used in legal science, health and medicine - relatively new to engineering; not known in computer science

– RP approach process : enables students to:

1) understand what they already know;
2) identify what they need to know in order to advance understanding of the subject;
3) make sense of new information and feedback in the context of their own experience and
4) guide choices for further learning.

Master of Science (Cyber Security and Forensic Computing)

I. Forensic Computing Stream:

- Electronic Evidence 1 – Forensic Computing
- Electronic Evidence 2 – Network and Internet Forensics
- Electronic Evidence Analysis and Presentation
- e-Crime, e-Discovery and Forensic Readiness

II. Cyber Security Stream:

- Intrusion Analysis and Response
- Critical Infrastructure and Control Systems Security
- Information Assurance and Security
- Software Security Lifecycle

III Minor Thesis 1&2 – Research Project

SSLC course aims and objectives

- Provide deep understanding; and
- Ability to implement and manage security throughout the software development lifecycle.
  - Secure Software Requirements; Secure Software Design; Secure Software Implementation / Coding; Secure Software Testing; Software Acceptance; Software Deployment; Software Operations, Maintenance and Disposal.

- Structure assessment to demonstrate what students learn by using **reflective processes.**

Who are these students?

Main motivation - to gain a post-graduate qualification and become better positioned for employment in the industry

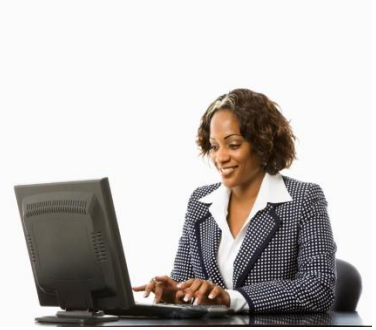
Student characteristics

- Part-time mature aged students from different government and industry organisations with:
  - a Bachelor degree in IT or
  - a Bachelor degree in engineering (electrical and electronic) ; and
  - technicians with more than 6 years' experience in the area
- Two diametrically opposed backgrounds
  - process control engineers - mature professionals with depth of experience in operation /maintenance of SCADA systems.
  - IT network specialists -earlier stages of their careers, networking background and good understanding of the security and reliability issues
- Small number of final year under-grad students -SSLC as an elective unit

Delivery Options

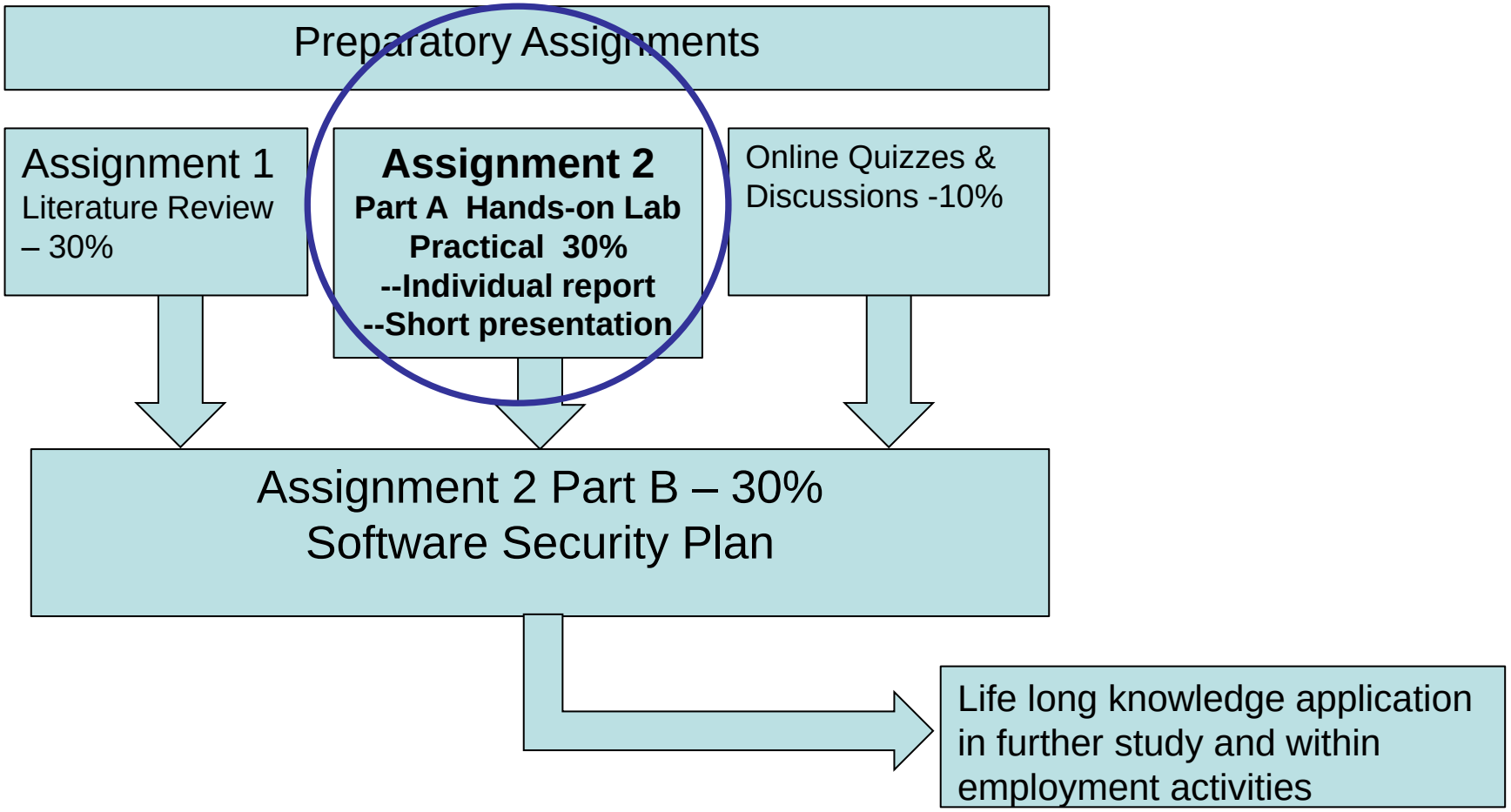
- F-to-F study mode (internal class)
  - 2h F-to-F class per course per week
    over 12 weeks

- Online distance study mode
  (external class)
  - 1h virtual online class per course per week
    over 12 weeks



+ **one week half day intensive study in-class (15 hours)**
  - Hands-on practicals
  - Industry guest lectures presentations
  - Networking opportunities

Scaffolded Assignments



RP Implementation to SSLC assessment task

RP	Where?	What?	Activity	Assessment and feedback
1) understand what students already know	W1-2 seminars	Backgrounds and work experience M1-3 materials	Online discussion Quiz	Online weekly Quiz auto marking
2) identify what they need to know	Plan intensive wk	Survey skills Balance of theoretical lectures and lab practicals	Plan and preparation	Plan test materials
3) make sense of new information and feedback in the context of their own experience	**Week 4 Intensive workshop**	**Day1-Day4 Lectures/practicals Day5 Presentations Individual reports submissions**	**Active participation in group discussions, presentations Written report**	**- Informal feedback from fellow students and instructors - Report marked - Comments simulate and prepare learners for a new step in their learning curve**
4) guide choices for further learning	Week 5-13	M1-13 materials All quizzes Work on Software Security Plan (SSP)	Written assignment component - Software Security Plan (SSP)	Reflection on comments and suggestions provided in week 4 in their major Assignment

Lab hands-on practicals:

- Application level attacks as defined by OWASP.
  - script errors, authentication flaws, injection flaws, cross-site scripting, and exploitation of numerous vulnerabilities in web service coding systems. Use was made of WebGoat and WebScarab.
- As root-level (administrator) access
- Fuzzing
  - Backtrack5 three tools
  - students gain experience by ulitising very limited probes to web sites known as weak in security.
- OS vulnerabilities

  Metasploit open-source suite- variety of exploit codes -test vulnerabilities in OS components, databases, compilers and others.

Limitations and future implementations

- Intensive week on week 4. Lecture on SW implementation and testing in wk 6 & 9
  - some concepts of software development, software testing in before hands-on practicals,
  - but some deeper insight into these topics is needed prior to the intensive week.
- Oral presentations informally assessed by educators and fellow students.
  - It would be better to include this activity for a formal submission with the weighting associated.

Students say

"The subject matter covered throughout the course was generally directly relevant to the industry I work in. The assignments were very helpful and relevant. Data collected during the first assignment and the report generated as part of the second assignment was able to link directly with issue within my own enterprise and been able to submit internally within the enterprise for further action"

Anonymous survey

Conclusions

- Assessment very much **a work-in-progress**
- First run shows virtually **every aspect** of students' learning and understanding is enhanced by RP approach
- Challenges and future development:
  - Continue relationship between two universities, the University of South Australia and the University of Canterbury
  - Reflect rapid changes in the field via regular updates
    - hands-on exercises reflecting new technologies ;
    - ISC2 , OWASP resources
    - Online education and joint virtual classes
    - Active research in the area and collaboration with security advisors

Thank You!