Hands-On E-learning Course on Cyber Defence for System Administrators

Praktilise küberkaitse e-kursus süsteemiadministraatoritele

Master's thesis

Author: Margus Ernits
Supervisor: Rain Ottis, Ph.D

Tallinn, June 3rd 2013

Presentation Outline

- Introduction and current situation
- Problem statement
- Considerations
- Methodology and the ADDIE model
- Analysis
- Solution
- Developed hands-on labs
- Evaluation of the e-learning course
- Conclusions
- Future research

Introduction

- Estonian IT College (EITC) focuses on applied higher education with the following curricula: IT System Administration, IT Development, IT System Analysis.
- Author is a lecturer of EITC:
  - Operating System Administration (6ECTS)
  - Linux administration (4ECTS)
  - Scripting languages (Bash, Python) (4ECTS)
  - IT infrastructure services (5ECTS)
  - Instructor of robotics club
  - Digital image processing C++
- Curricula development is held in cooperation with universities, private companies, graduates and students.

Problem Statement

- Insufficient numbers of skilled and security aware system administrators (in Estonia):
  - EITC courses did not cover the needs of industry for practical security field.
  - Many system administrators are self-taught and do not have required qualification.
  - Practical component of studies was not sufficient for configuring IT infrastructure services securely.
- Solution was to develop a practical hands-on e-learning course.

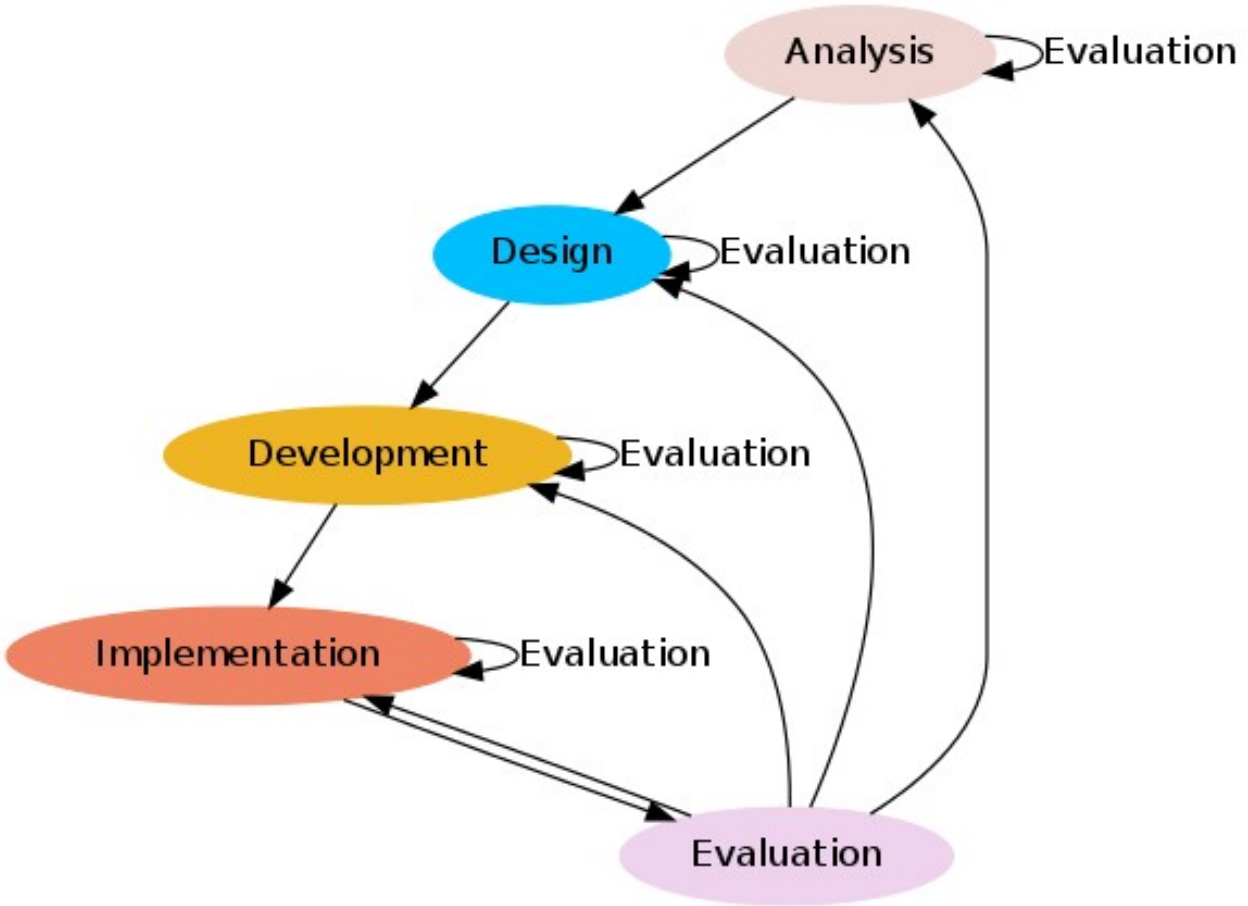
Considerations

- Developing the new hands-on e-learning course:
  - focused on defence of the IT systems;
  - securing services is part of configuring the services;
  - lab intensive, *command dojo* (follow the master);
  - playful, motivating (badges, competition);
  - suitable for students and for continuous education.
- Not for teaching offense or cyber security specialists!
  - The target audience is system administrators and students.

Methodology

- Investigating the problem and similar research (Kasak, HyneSim, defensive and offensive courses/trainings/exercises).
- Instructional design models:
  - behaviorist, suitable for trainings;
  - cognitivist, suitable for exploring, group-works;
  - prescriptive models:
    - ADDIE model – used in Estonia.

Chosen Method – The ADDIE Model



Analysis

- Instructional goals
- Learner analysis
- Learning outcomes
- Course module list
- How to make the course playful?
- Which technical environment is needed?

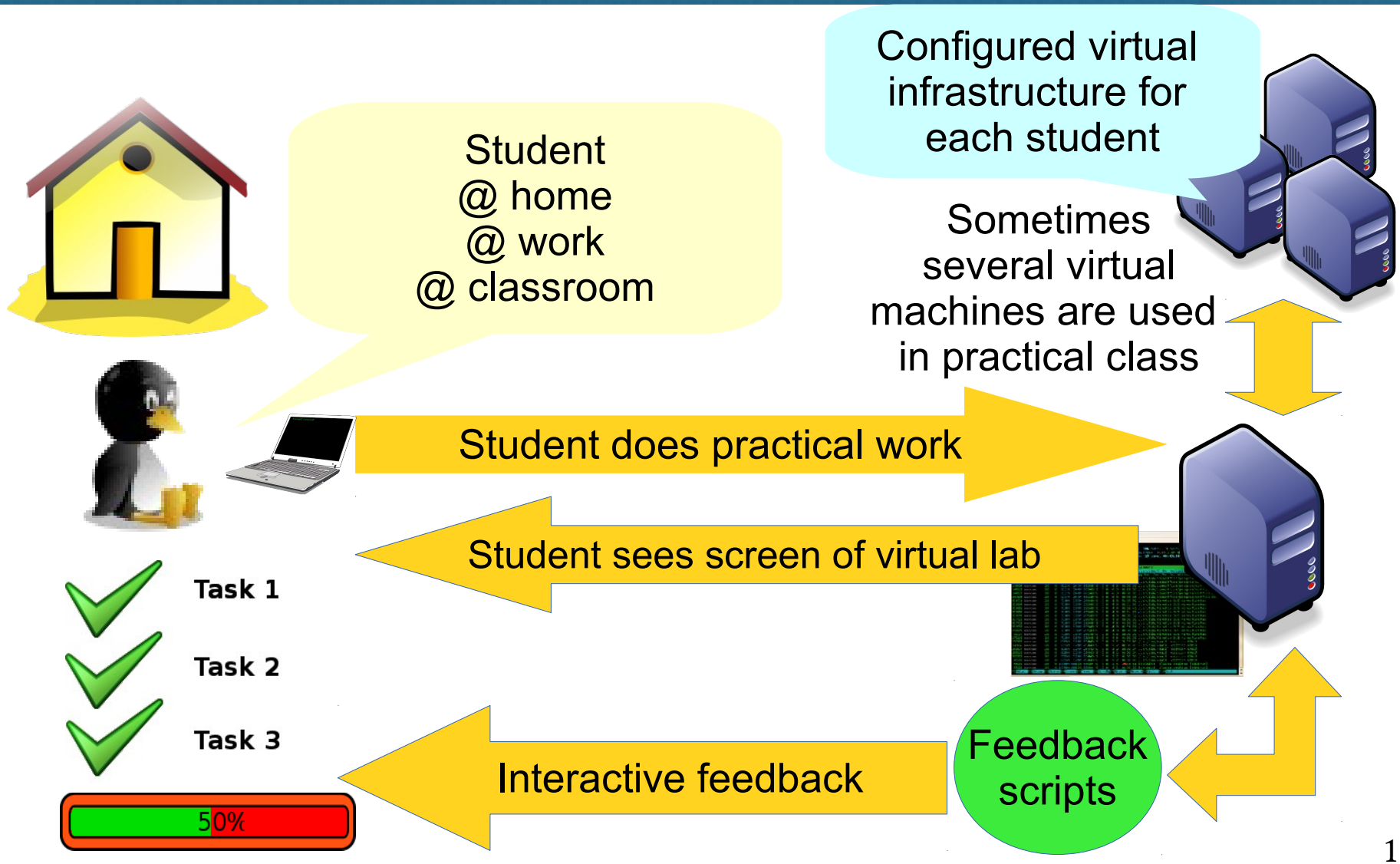
Solution

- Developing labs:
  - learning objectives;
  - hands-on laboratory materials and learning material;
  - virtual machine (templates) and interactive scripts for feedback.
- Developing virtual environment:
  - the existing environment does not meet all expectations;
  - development can be done during summer.

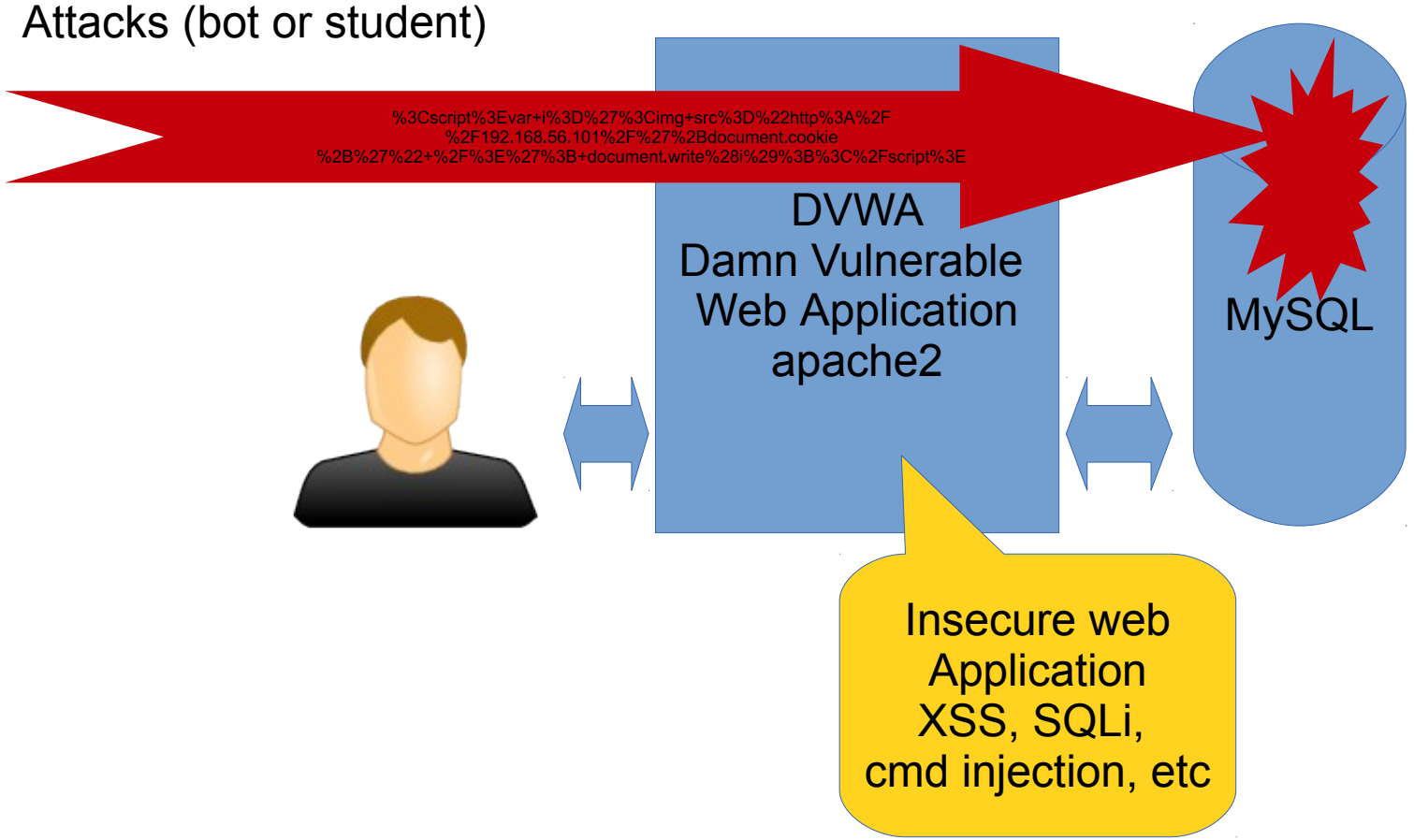
Developed Hands-On Practical Classes

- Preliminary courses (GNU/Linux, Bash, Python and PowerShell scripting).
- Hands-on labs and materials (**6 ECTS**, tested with 56 students):
  - NTP/DNS/DHCP;
  - Securing web application:
    - Caching – varnish;
    - Application firewalls:
      - Hardening web server installation;
      - SQL firewall (GreenSQL);
      - Mod Security firewall;
      - Offload HTTPS using nginx.

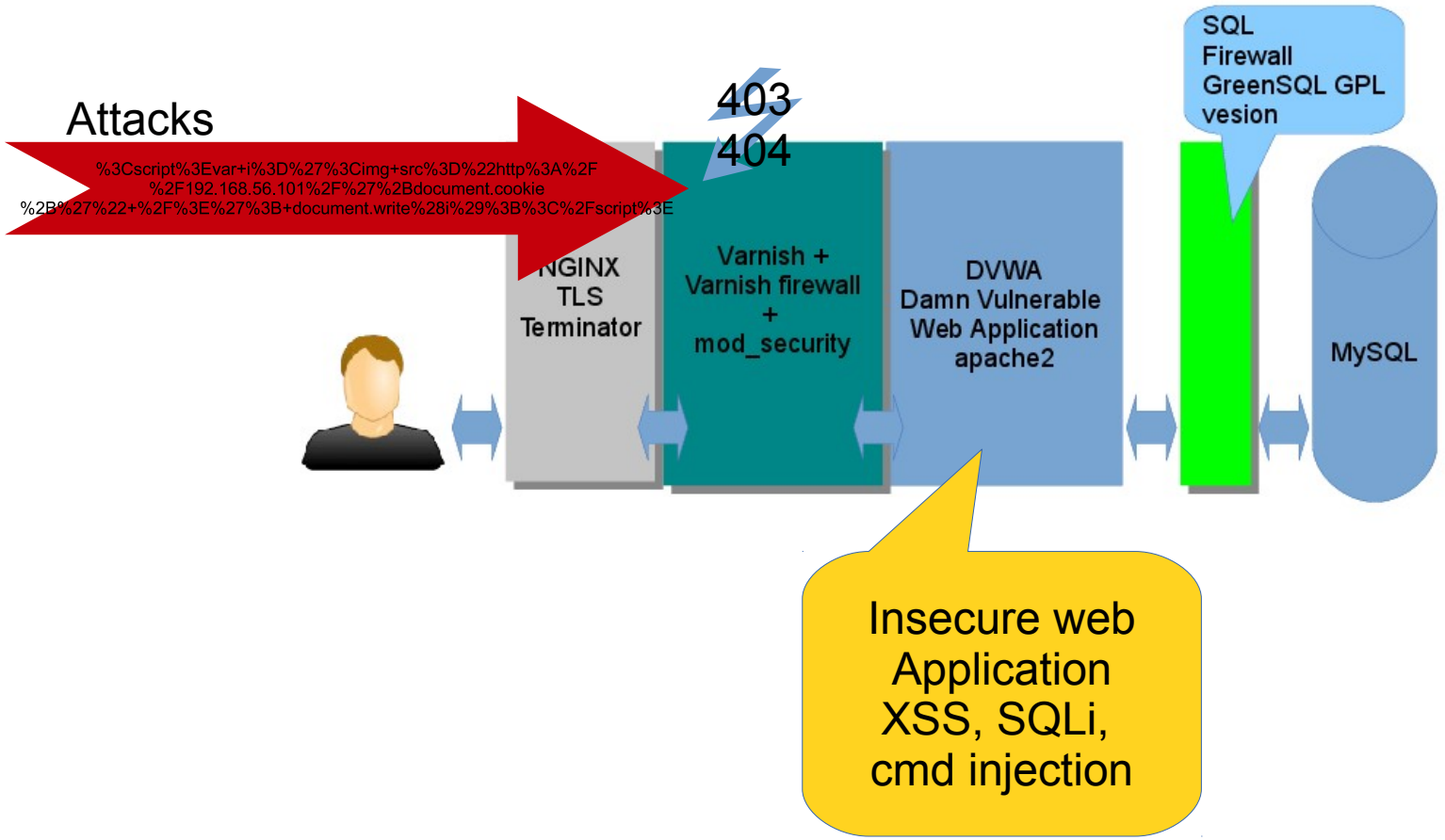
The Distance Laboratory used for Hands-on Practical Classes



Sample lab - Securing Insecure Web Application the Beginning



Sample lab – end
Securing Insecure Web Application



Evaluation of the E-learning Course

- Feedback from 17 students (collected via Study Information System):
  - average grade for course - 4.9 from distance learners and 4.6 from students (on 5-point scale);
  - the lecturer (the author of the thesis) was graded with 4.9 on 5-point scale.
- Feedback from continuous education students (50 system administrators):
  - the course was graded with 2.9 and the lecturer with 2.9 points, both on 3-point scale.
- Feedback from two lecturers:
  - too intensive for so limited time;
  - too much work (preparing for lab needs work prior to every course).

Conclusions

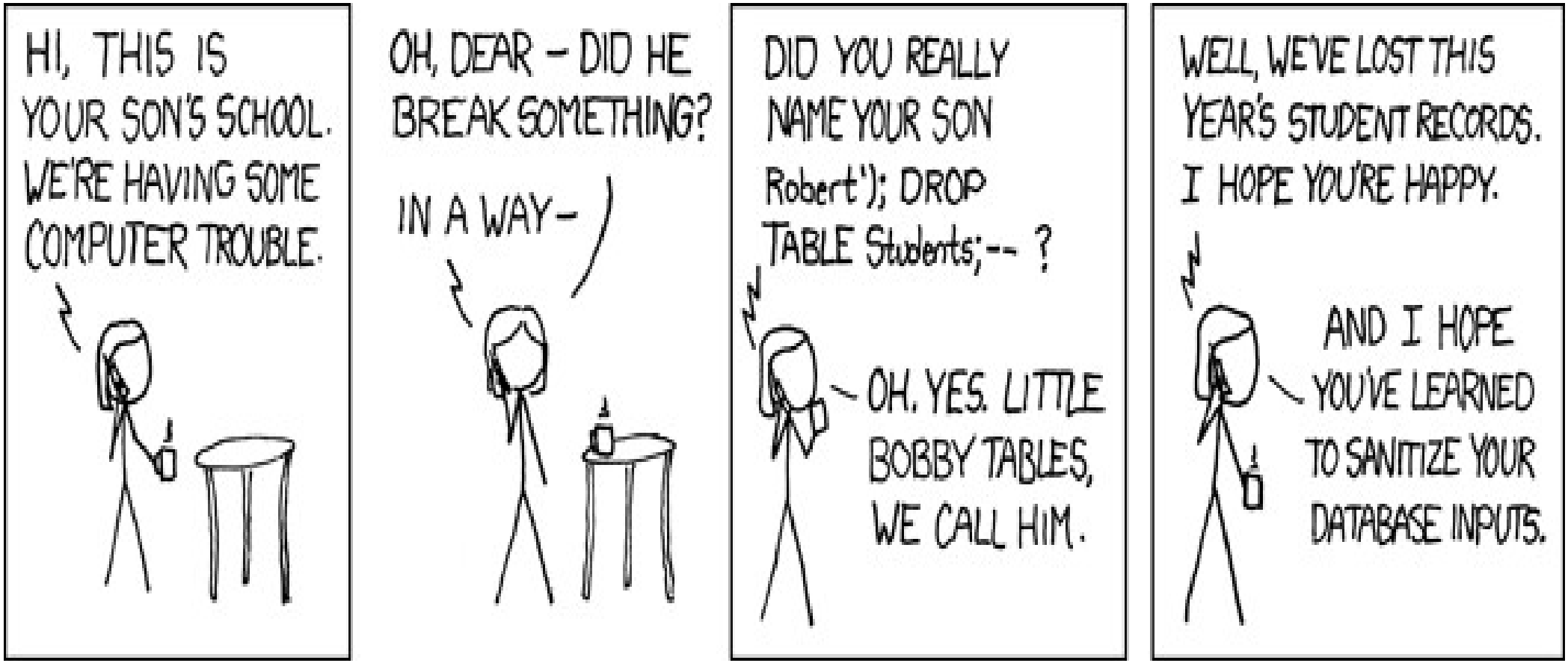
- The quality of studies will improve (improved) due to increased amount of practical hands-on classes
  - (piloted 2012/2013 – 56 students).
- System administrators are more security aware due to continuous education
  - more than 80 attendees in courses during 2012-2013.
- The new E-learning course Protecting IT Infrastructure has been developed and piloted.

Future research

- Evaluate new course and gather more feedback.
- Design a new, interactive module (expert system) for distance study system to provide real-time feedback to the student (interactive suggestions what went wrong etc).
- Develop distance laboratory system to support new methodology (rewarding, badges, instant feedback and different network setups).
- Integrate and test new learning materials and lab scenarios (logging, fire-walling, central management).

Thank You

Exploits of a Mom...can be stopped



Source: Exploits of a Mom http://xkcd.com/327/