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, 16. May 2013

Presentation Outline

- Introduction and current situation
- The Problem
- The Objectives
- Methodology and the ADDIE Model
- Analysis
- Solution
- Developed Hands-On Practical Classes
- Evaluation of the E-learning Course
- Future Research
- Conclusions

Introduction

- Estonian IT College (EITC) focuses on applied higher education with curricula
  - IT System Administration
  - IT Development
  - IT System Analysis
- Curricula development being held with help of universities, private companies, graduates and students

The Main Problem

- The main problem is deficiency of the skilled and security aware system administrators
  - EITC courses do not cover needs of industry on practical security field
  - Many system administrators are self studied and do not have required qualification
  - Amount of practical word is not sufficient to gain security skills for configuring IT infrastructure services

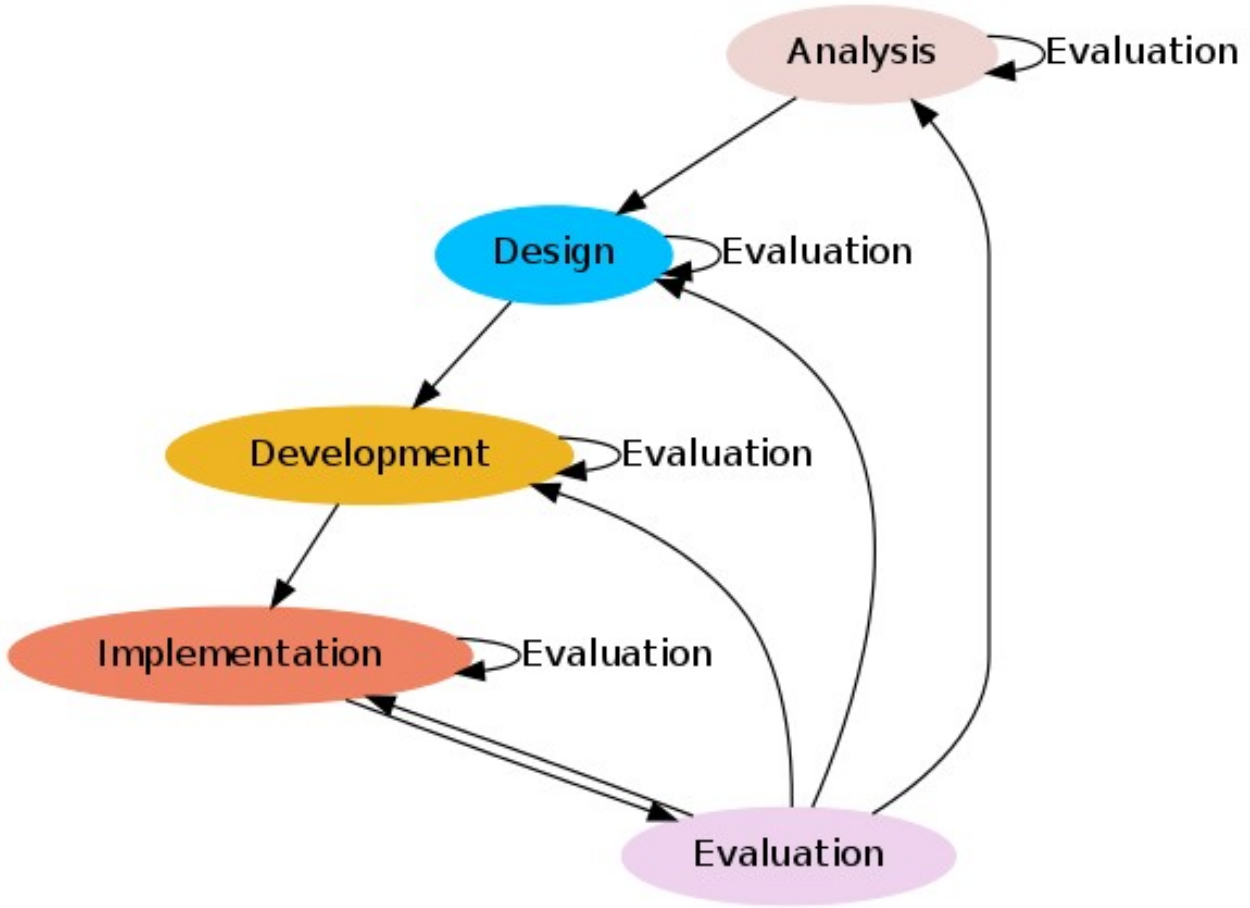
Main Objectives

- Developing new hands-on e-learning course
  - Dedicated to defense of the IT systems
  - Securing services is part of configuring them
  - 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 specialist

Methodology

- Investigate 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 (more then 100 variants)

Chosen Method – The Addie Model



Analysis

- Goals for course and learning outcomes
  - After completing the students will be able to install, configure and secure IT infrastructure services as (NTP, DNS, DHCP, web servers, firewalls, file servers and authentication services)
  - Student explains common attacks against web applications as well able to explain terms VPN, SAN, NAS, IDS, IPS.
  - The students able to document installed services
- Learner analysis
- Course module list
- How to make course playful?
- What environment is needed?

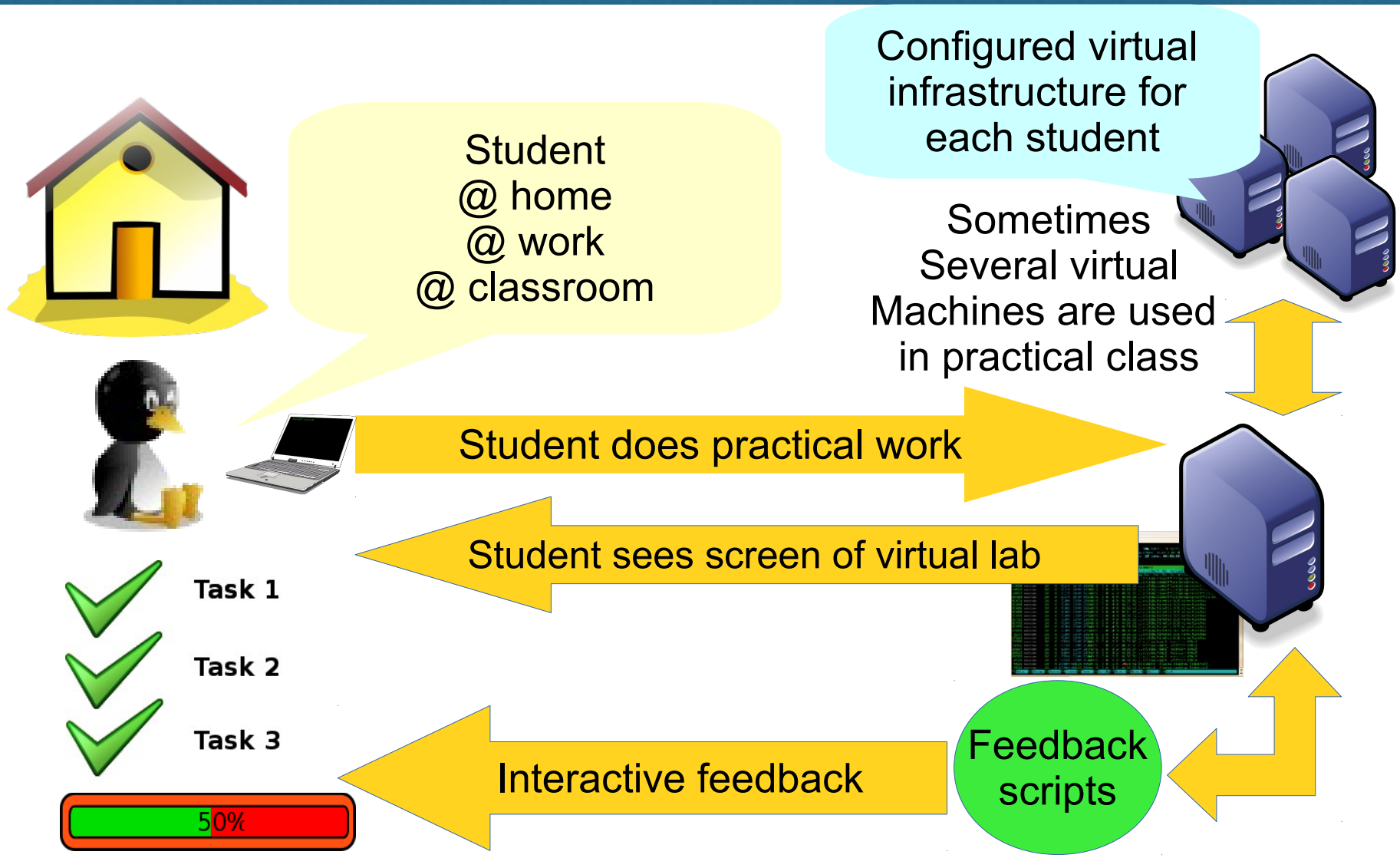
Solution

- To develop courses
  - Learning outcomes
  - Hands-on laboratory materials and learning material
  - Virtual Machine (templates) and interactive scripts for feedback
- To develop virtual environment
  - Existing environment do not cover all expectations
  - Development can take place in summer (Live system in use during semester)

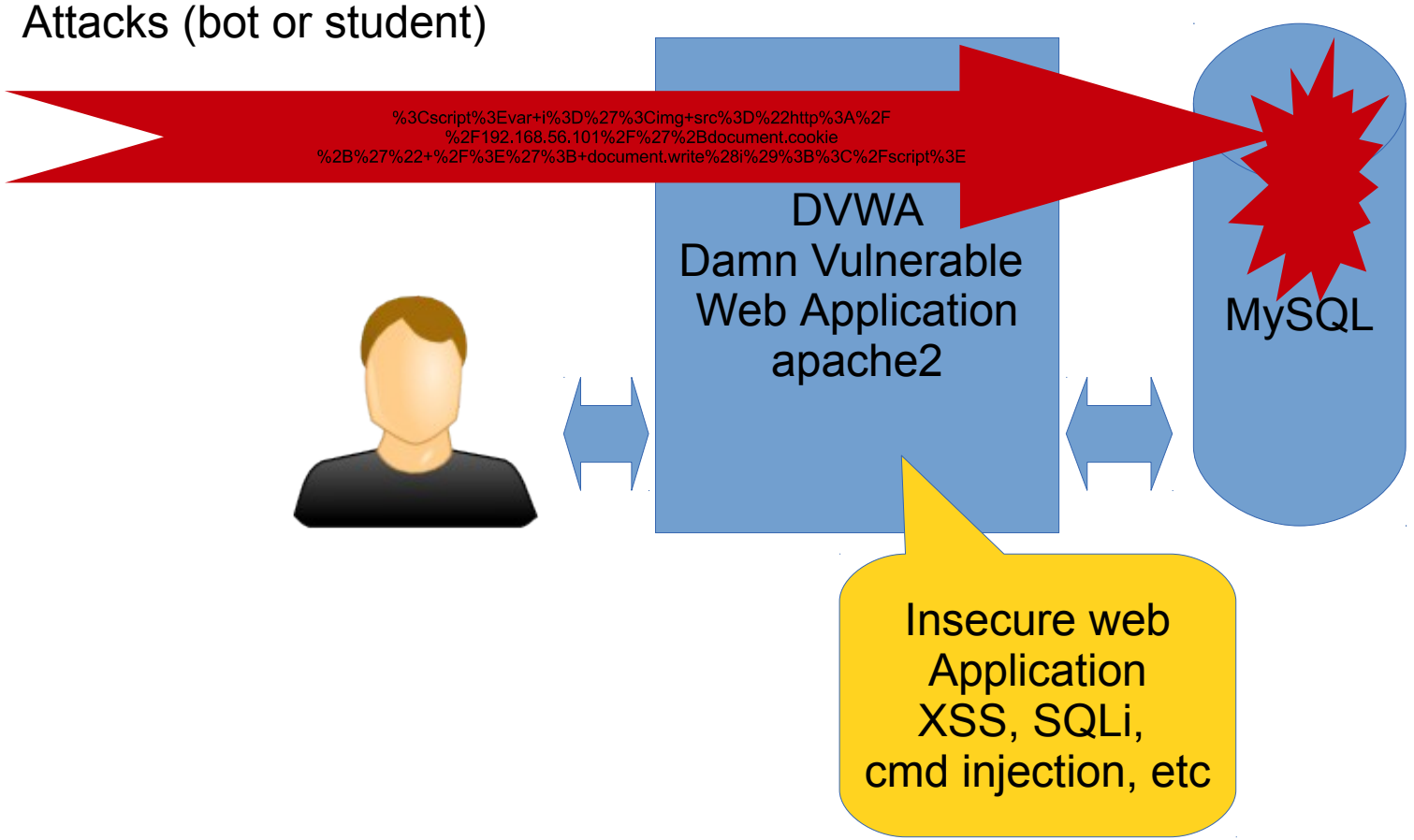
Developed Hands-On Practical Classes

- Pre requirement course (GNU/Linux, Bash, Python and PowerSehell scripting)
- Hands-on labs and materials
  - NTP/DNS/DHCP
  - Securing web application
    - Caching – varninsh
    - Application firewalls
      - Hardening web server installation
      - SQL firewall (GreenSQL)
      - Mod Security firewall
      - Offload HTTPS using nginx
    - Coming shortly (Kerberos/LDAP Samba4, logging, firewalling)

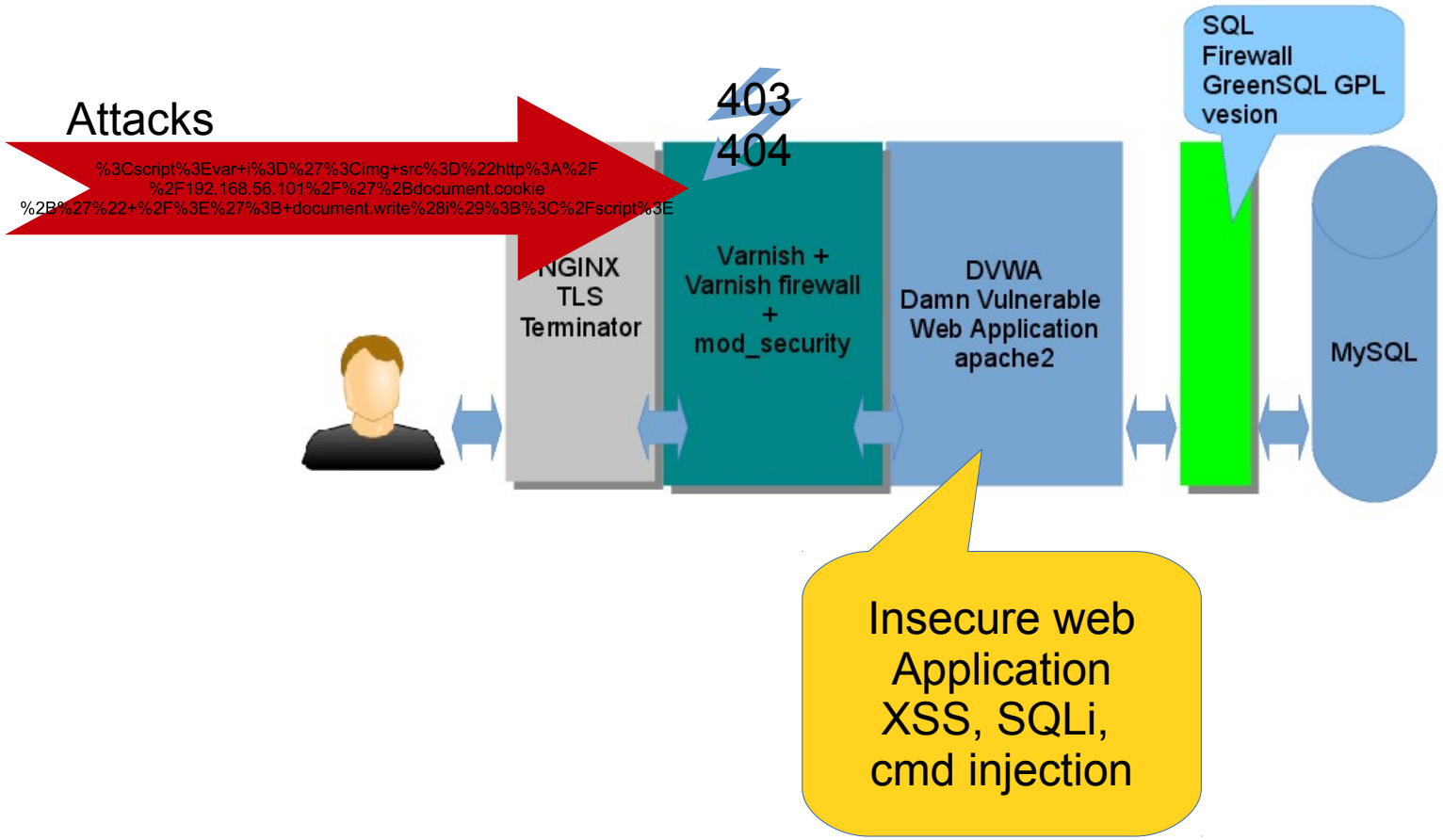
The Distance Laboratory used for Hands-on Practical Classes



Sample lab - Securing Insecure Web Application the Beginning



Sample lab – end
Securing Insecure Web Application



•Evaluation of the E-learning Course

- Feedback from students (feedback from Study Information System)
  - Grade for course (4.858 – distance learners, 4.6 – students, max is 5)
  - Grade for lecturer (4.88 – distance learners, 4.8 - students)
- Feedback from continuous education students
  - Grade for course (2.9 max is 3)
  - Grade for lecturer (2.9 max is 3)
- Feedback from lecturers
  - Too intensive to so limited time
  - Too much work (preparing for lab needs work before every course)

Future research

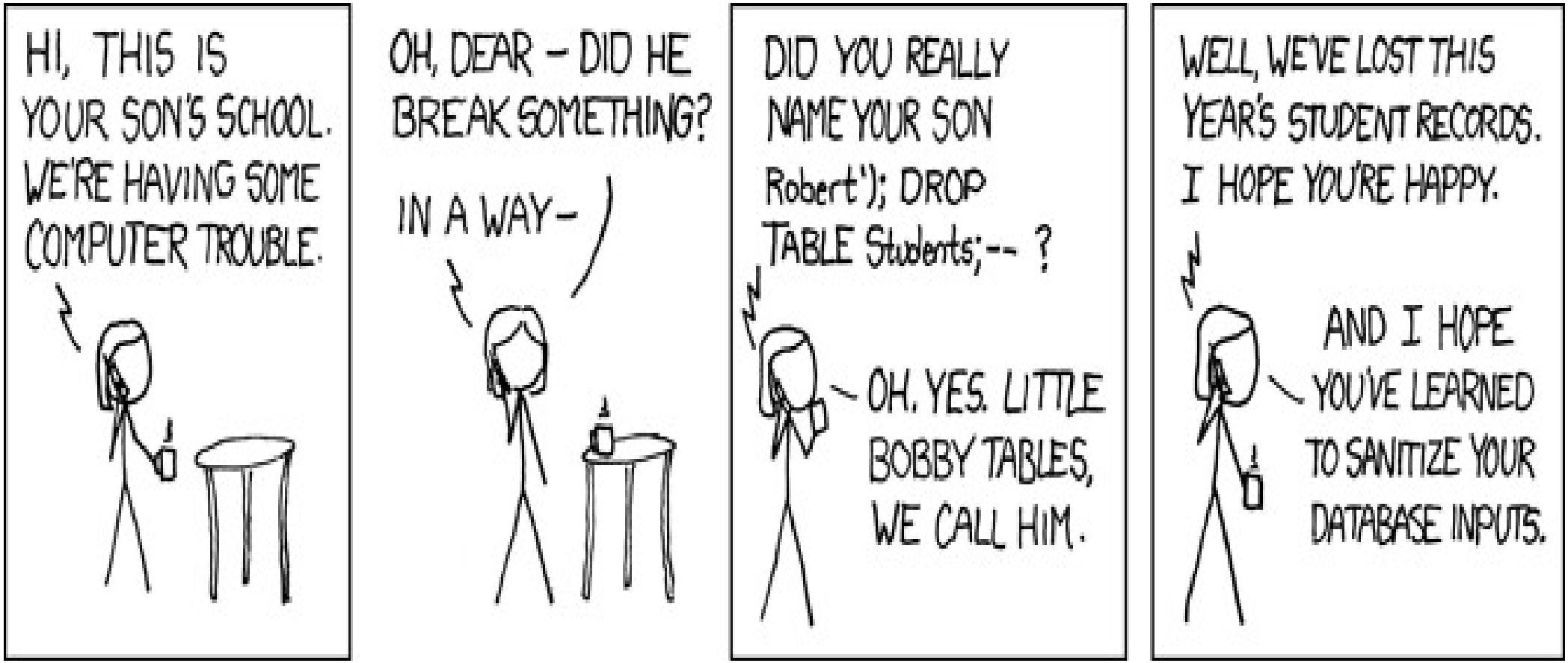
- Evaluate new course and get more feedback
- Design interactive module (expert system) to give real-time feedback to the student (suggest what went wrong etc)
- Develop distance laboratory system to support new methodology (rewarding, badges, instant feedback and different network setups)
- Redesign some learning materials to follow new text material standards (For DNS/DHCP/NTP)
- Integrate and test new learning materials and lab scenarios (logging, fire-walling, central management)

Conclusions

- The quality of studies will improve (improved) due to increased amount of practical hands-on classes
- System administrators are more security aware due continuous education
  - More then 70 attendees on courses during 2012-2013
- The new E-learning course Protecting IT Infrastructure is developed and piloted

Thank You

Exploits of a Mom...can be stopped



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