A Comparative Study of Teaching Forensics at a University Degree Level

Martin Mink
University of Mannheim, Germany

IMF 2006, Stuttgart
October 19

UNIVERSITÄT
MANNHEIM

Joint Work

- Laboratory for Dependable Distributed Systems
  - University of Mannheim/RWTH Aachen University
  - Maximillian Dornseif, Felix C. Freiling, Thorsten Holz, Martin Mink
- School of Computing, Engineering and Information Sciences
  - Northumbria University, U.K.
  - Philip Anderson, Alastair Irons, Christopher Laing

Outline

- Introduction and aim
- British case
- German case
- Comparison
- Conclusions

Introduction

- Need to develop specialists in computer forensics
  - determine where cybercrime may have taken place
  - examine the cybertrail
- Skills required
  - computer scientists trained to deal with various hard- and software systems
  - educated in law to assess relevant evidence
  - trained in the principles of forensic science
  - judge their actions in the context of psychological stress and possible own criminal activity

Introduction (2)

- Computer forensics at University degree level
  - programmes and courses
    - only few offered
    - differ
  - has a global aspect
  - national standards in computer forensics education are only of limited value

Aim

- Are international standards in computer forensics education possible?
- Compare University degree computer forensics curricula from two countries
  - Great Britain: full BSc honours programme in Computer Forensics at Northumbria University
  - Germany: area of specialization within a general Computer Science Diploma degree programme at RWTH Aachen University
  - no output in students yet, so compare design of the programmes

The British Case: Motivation

- Popular topic among students at Northumbria
- A number of members of academic staff already centered on computer forensics
  - growing body of knowledge
- Other groups of the School interested in the topic
- Interest by employer groups
- Raise popularity with potential students

Philosophy

- Address the need of law enforcement agencies and organisations for skilled professionals
- Focus on the principles of evidential integrity and the challenges of dealing with digital evidence
- Provide the knowledge to professionally and systematically preserve and extract all relevant digital evidence
- Prepare to use the principles defined by the Association of Chief Police Officers (ACPO)

Curriculum Design

- In collaboration with practitioners
  - to address the skills, techniques and theoretical requirements for graduates to work in the field
  - to ensure that students are immediately useful to their employers
- Analysis of historical cases, hypothetical case studies and cases made publicly available
- Computer forensics introduced in the first year, increasing the coverage until the final year
- Placement year between second and final year

Ethics and Interdisciplinary

- Ethics
  - students are made aware of
    - the potential for misuse of computer forensics tools and techniques and
    - the need for ethical and professional behaviour
- Inter disciplinary considerations
  - input from other Schools of the University
    - forensic science
    - criminal justice systems and criminal motivation
    - legal and evidentiary aspects

Equipment and Industry Relations

- Laboratory Facilities
  - hard- and software specific to comp. forensics
  - to develop practical skills using computer forensics tools
- Employer links
  - police forces and enterprises provide
    - expert knowledge through presentations and case studies and
    - placement and employment opportunities

First Year

120 points*

Sem. 1	Programming 1 (20 points)	Introduction to Computer Forensics and Criminology (20 p.)	Relational Databases (20 p.)	Learning and Skills (10 p.)	SW- and Data Modelling (10 p.)
Sem. 2	Programming 2 (20 points)			Introd. to Internet Technologies (10 p.)	Computer system Fundamentals (10 p.)

*1 unit equiv. to about 15 working hours, ~ 0,5 ECTS

Second Year

120 points

Sem. 1	Dynamic Internet Technologies (20 p.)	Professional Development (10 p.)	Networks and Operating Systems (20 p.)	Data Structures and Algorithms (20 p.)	Principles of Computer Forensics (20 points)
Sem. 2		Further Networks (10 p.)			Computer Forensics Applications (20 points)

Last Year

120 points

Sem. 1	Applied Professionalism and Management (20 p.)	Individual project (30 points)	Advanced Computer Forensics (20 points)	Ethical Hacking for Network Security (20 p.)	Legal and evidentiary aspects (10 p.)
Sem. 2			Computer Security (10 p.)		Forensics Case Project (10 p.)

The German Case: Motivation

- No graduate programmes specialized in computer forensics in continental europe
- Interest in computer forensics by staff members
- Developing a new degree programme specialized in forensics was not possible
  - due to restricted resources
  - instead: “area of specialization” within a traditional Computer Science Diploma programme

Two Semester Curriculum

88 points*

Sem. 1	Applied Computer Security (20 points)	Computer Forensics (12 p.)	Seminar (6 p.)	*Other Courses from Computer Science*
Sem. 2	Web Application Security (10 p.)	Hacking Lab (20 points)	Summer School (20 points)	*Other Courses*

*units have been calculated to the same unit as in the British case

First Semester

- Lecture „Applied Computer Security“
  - classical lecture presenting basics
  - security concepts on UNIX, network security
- Lecture „Computer Forensics“
- Research seminar
  - introducing security related issues
  - students give a presentation

Second Semester

- Lecture „Web Application Security“
  - teach, how insecure web applications can be broken
- Practical „Hacking Lab“
  - attack and defense of networked computers
- Summerschool „Applied IT Security“
  - advanced exploitation techniques

Computer Forensics

- Classic: gathering, interpretation and presentation of evidence found on computers
- But:
  - dependent on the legal system
  - literature and experiences only from countries with a different legal system
- Our definition: tool to understand security
  - ⇨ analysis of security incidents to improve security in the future

Computer Forensics (2)

- Students learn how to extract and interpret evidence and to evaluate the validity of that information
  - focus on file systems
  - analysis with only basic tools
  - should be able to develop their own tools
- Practical exercises:
  - give students the opportunity to experience different forensic techniques themselves
  - e.g. analysis of pre-used hard disks

Honeypots

- Honeypot
  - system without a task in the network
  - every interaction is a possible malicious action
- Can be used to provide real-world cases of computer incidents
  - analyse
    - data collected by honeypots
    - compromised system
  - honeynet.org: Scan of the month

Comparison: British

- More mature and better–developed (considering industrial needs)
  - higher amount of financial and personal resources
  - close cooperation with industry and law enforcement agencies
- Much more focussed on computer forensics
  - specialized BSc degree
- Strong inter disciplinary involvement
- Strongly motivated from best practices and rules of professional bodies

Comparison: German

- Part of a general computer science diploma degree
  - large freedom of choice for students
- Almost entirely focussed on computer science
- Motivated by questioning standard approaches and aiming for scientific discovery
- Educate computer scientists that can perform research in computer forensics and security

Conclusions and Outlook

- Two complementing and orthogonal aspects
  - rigorous practical skills and
  - competence for fundamental research
- Prototypical for the differences in the aim and scope of the two implementing Universities
- Future: conduct an empirical study of each of the two programmes on the skills and success of the students who successfully earned a degree