J Comput Virol (2007) 3:149–161
DOI 10.1007/s11416-007-0054-0

EICAR 2007 BEST ACADEMIC PAPERS

Bologna process revisited: educating information security and malware experts

Urs E. Gattiker

Received: 12 January 2007 / Revised: 10 February 2007 / Accepted: 29 March 2007 / Published online: 26 May 2007

Abstract The Bologna process has resulted in the restructuring of undergraduate and graduate education across Europe. This paper outlines what these changes mean for acquiring degrees in information security and how various universities have tried to respond to these demands. What is unclear at this stage is how the offering of continuous master degrees at Polytechnic and Applied Science Universities will affect the content and curriculum being taught in computer science and information security in particular. This question must be addressed since polytechnics are more industry focused and less research oriented than their university-counterparts. What seems to be clear at this stage is that continuous type master programs in computer science demand a greater level of mathematical knowledge than specialized masters. Moreover, due to the amount of credits that must be acquired, graduates of these types of programs will bring a deeper knowledge about the specialization such as, information security or malware, they acquired at university. This movement toward greater convergence in post secondary education may not have made things easier for recruiters, who are trying to hire graduates in information security or anti-virus experts. In fact, as this paper shows while the Bologna process may have eliminated the obvious differences, countless intricate and not so obvious differences have been added making it sometimes obscure for a bystander.

Urs E. Gattiker, Ph.D. is founder and chief technology officer of CyTRAP Labs (http://blog.cytrap.eu/?page_id=115) and runs the CASEScontact.org early warning system.

U. E. Gattiker (✉)
CyTRAP Labs, Roentgenstrasse 49, 8005 Zurich, Switzerland
e-mail: research@CyTRAP.eu

1 Introduction

A fundamental fact in computer, information and network security is the impossibility of 100% assurance that a computer system is trusted.[1] How education can help in achieving the required level of trust considering various stakeholders (e.g., society, consumers, shareholders and suppliers) is open to discussion. Some have suggested that certification is the answer, others support the notion that information assurance[2] programs can fill the gap. Europe is further trying to standardize its education efforts with the help of the Bologna process[3] in the hopes to improve educational transparency as well as encourage convergence of programs.

In the latter case, advocates also hope that this will provide nations with the professionals required to reduce risks for possible disasters, while improving security of critical infrastructure and information assets.

This paper focuses on undergraduate and graduate education efforts in the area of computer security in Europe. Specifically, we try to address three issues:

[1] By trusted we mean to say that the system always operates as expected by design and policy.

[2] Because the term information assurance is not widely used across Europe we rarely if ever use this term here. Instead, we have chosen to use information security in our terminology. Our rational for this choice is explained further into this paper.

[3] The term Bologna process—the follow-up to the Bologna Declaration of 1999 [9]—is to establish a European Higher Education Area by 2010 in which students and staff can move with ease and have fair recognition of their qualifications. The main action lines of the Bologna Declaration therefore aim at the:

– adoption of a system of degrees essentially based on two cycles (i.e., undergraduate and graduate);
– co-operation in quality assurance and recognition; and
– promotion of mobility.

1. How the Bologna Declaration is influencing education in information security across Europe,
2. What focus programs on information security currently have and
3. How this increasing convergence could help or stifle our efforts in better protecting information and critical infrastructure.

Due to space limitations our discussion will be incomplete and sometimes even sketchy. All the same, we have made an effort to provide references to additional resources to allow further in depth study of the matter by the reader if desired (see also the Appendix).

The paper is organized as follows. First, some of the recent developments in post-secondary education set in motion by the Bologna Declaration of 1999 [9] will be outlined. Next, the development of the educational programs in information security fitting this new framework are presented and then discussed. Finally, we summarize key findings and where these efforts might lead us regarding education and training and highlight practical implications regarding better protection against future threats and malware.

2 Undergraduate and graduate education: convergence in educational programs

With the help of the Bologna process, European universities have started to standarize their program offerings. The Bologna Declaration (1999) aimed to ease the transfer of credit units to other institutions and, thereby enable students to move easily from one institution to another to complete their work. At the heart of this effort is work that tries to compare curricula as well as student workload across institutions (Student workload, teaching method and learning outcomes, 2003). More details about the Bologna program can be found in the Appendix to this paper.

2.1 The Bologna program: getting a bachelor in information security

Of interest here is, however, how these efforts will help in achieving further convergence in undergraduate and graduate education regarding information security. The scientific discipline of computer science is sometimes also called informatics in Europe. In Europe, rarely if ever can one find a program called information assurance although courses dealing with this topic or malware are offered across the university landscape.

For meeting all graduation requirements for a bachelor degree in information security as part of the Bologna system the student must have acquired 180 ECTS[4] credit points and in some countries this might be 240 ECTS. These are obtained over a 3–4 year or 4 year period using the semester system (i.e., 30 units according to the European Credit Transfer System or ECTS each semester). Compared to a North American undergraduate degree, the first year with its general distribution requirements is not part of the university education in Europe if 180 ECTS are required for graduation. In fact, students have taken and successfully passed these types of courses during their high school program (see also Tables 1, 2 below).

Table 1 Information security—pre-requisites for graduation

Pre-requisites or focus of undergraduate studies	Undergraduate (ECTS)
Foundation courses in computer science	70
Foundation courses in mathematics and statistics	20
Specialization courses	40
Undergraduate thesis (minimum or higher)	10
Total number of ECTS in computing science or related fields (could be higher) out of 180 ECTS credits required to attain a bachelor diploma	140

In short the following points are noteworthy:

1. A bachelor-level degree is earned at an institution of higher education and requires between 3-and-4 years of full-time study, or 180–240 ECTS credits.
2. The degree can be fulfilled at both traditional universities and at non-university institutions of higher education.

As Table 1 above illustrates in some computer science programs, 70 ECTS are the foundation courses in computer science as well as further 20 ECTS credits must be taken in the area of mathematics and statistics.[5] These are the minimum requirements, however it is left to the various institutions on how what these requirements may contain (see also Entrance Requirements in the Appendix).

The third year is taken up for specialization by taking courses as part of one's major (about 40 ECTS), as well as getting credit for doing an undergraduate thesis that again is focusing on a topic relevant to one's major (for instance about 10 ECTS or higher). Hence, after the student having acquired all the basics in computer science and mathematics,

[4] *European Credit Transfer System* (ECTS) guarantees academic recognition of studies abroad by providing a way of measuring and comparing the student's learning achievements, and transferring them from one institution to another.

[5] For instance, as described by the University of Aarhus' degree requirements for a Bachelor in Computer Science here http://www.nat.au.dk/default.asp?id=9213&la=DK. Accessed: 25 May, 2006.

thereafter specialization in information security,[6] cryptography[7] may occur. Naturally, specialization options do, at least in part, depend upon the expertise and focus of the particular program (e.g., focusing on secure programming versus more focus on risk assessment) and its staff and their particular research interests. Everybody who attended a graduate program remembers that while a course title and description are helpful, the instructor's research interests also influence the content and focus of a course. The research interests will automatically flow into the content of the courses taught by a particular instructor. Generally, this helps making the content better and bringing the latest research findings to the students' attention.

Regarding the undergraduate curriculum, these programs often entail a practical component that students must complete. The practical component of a study program may be satisfied in part by having to successfully complete laboratory-type exercises. These may contain but not be limited to the student having to carry out the functions and tasks of a system administrator for server. In turn, fellow students' partial task may be to test if that server has been hardened well enough to meet best practice while being a dependable and reliable system withstanding these attacks. Moreover, the program may also require an internship at a local company for a few months to further enable the student to transfer classroom knowledge to the workplace.

2.2 Obtaining a graduate degree

So what does the Bologna Declaration do for education at the university-level in computer science and information security specifically? The Bologna Declaration defines the Bachelor's degree as containing the following:

1. A bachelor-level degree is earned at an institution of higher education and requires between 3-and-4 years of full-time study, or 180–240 ECTS credits.
2. The degree can be fulfilled at both traditional universities and at non-university institutions of higher education.
3. The details (profile) of each degree program and its learning outcomes should be noted in their title and included in the diploma supplement issued to the student.
4. Bachelor-type study programs must prepare students for further study. Most important is that they should be freestanding and, therefore, not be regarded as part of a longer curriculum. This allows students to change disciplines and/or pursue graduate studies at another institution. Admission to second-cycle (graduate) degree programs requires successful completion of first-cycle (undergraduate) degrees.

Of interest in this paper is, however, how the above requirements are being met across universities in Europe when it comes to training security and malware experts and engineers. This will be discussed in more detail below.

Continuous versus Specialized Master Degrees in Information Security To accommodate point 4 above, the **Bologna system allows for two broad types of Master programs** being offered, namely:

– *Consecutive master programs* offering a direct continuation to a corresponding Bachelor program (i.e., where one has specialized in computer science). Students have the option to choose specialization streams, whereby a major and minor focus can be attained.
  90 ECTS credit points are required of which about 30 ECTS are taken by a thesis project of about 6 months duration. In total the study program should take 3 semesters or 18 months, whereby sometimes more in-depth projects delay the student at the end so graduation requirements may be met after 24 months.
– *Specialized master programs* where studies could be interdisciplinary and the student has not taken an undergraduate degree in exactly the same area.
  120 ECTS credit points are required of which about 30 ECTS are taken up by a thesis project of about 6 months duration. Usually, these programs take four semesters and are of about 24 months duration.

Table 2 suggests that a student may specialize in eight different types of programs of study leading to a Master in Information Security degree. Naturally, within each type there are nuances and differences in the curriculum that affect the skills and knowledge the student will acquire. However, these go beyond the scope of this paper.

Table 2 outlines some of the possible variations in programs. Needless to say that all other things being considered equal, a consecutive type Master program provides students with more in-depth knowledge and understanding of the subject than a specialized Master. Partially, this is simply due to having had training of 180 ECTS during undergraduate studies as well as and additional 120 ECTS for doing graduate work in information security.

Specialized master degrees compared to diploma of advanced studies or diploma programs A lesser known type of program is a so-called diploma of advanced studies (some countries call them *Nachdiplomstudium*) such

[6] The description is one for computer science students who are interested in taking an undergraduate major in information security at an Institute of Technology see here http://www.maturanden.inf.ethz.ch/studium/aufbau_struktur. (Access: 15 May, 2006).

[7] This description is for a 3 year bachelor degree in informatics with a focus on cryptographic issues http://www.cs.kuleuven.be/cs/info_studenten/nieuwe_studenten/informatica/opleiding/overzichtBa/. (Access: 29 November, 2006).

Table 2 Information security studies—pre-requisites for a graduate degree

Pre-requisites or focus of undergraduate studies	Consecutive	Specialized[a]
1) Bachelor of Science degree is in the **same field**, such as computer science, with a major in computer/information security. Master studies requires student to do advanced level work in computing security (i.e., concentration courses and master thesis address computer security issues)	X 90 or 120 ECTS	
2) Bachelor of Science degree is in the same field, such as computer science with a major in **software engineering**. Master education offer student advanced work in computing security (i.e., concentration courses and master thesis address computer security issues)	X 90 or 120 ECTS	
3) Undergraduate studies may not have been in computer science but what is considered a **related discipline** (e.g., also natural sciences such a mathematics or physics) giving the student the skills and knowledge considered a pre-requisite for admission (e.g., mathematics and programming). Master studies will be done in computer science with a concentration on information security (i.e., concentration courses and master thesis address computer security issues)	X 120 ECTS	X 90 or 120 ECTS
4) Undergraduate studies may neither have been in computer science nor a related discipline. However, student may be able to meet pre-requisites (e.g., having attended and successfully completed several types of courses during her undergraduate studies or passing a test demonstrating these skills before being fully admitted) or else attend and successfully pass pre-requisite courses before being fully admitted to the program(e.g., mathematics and computing). Master studies will be done in computer science with a concentration on information security (i.e., concentration courses and master thesis address computer security issues)	X 120 ECTS	X 120 ECTS
5) Student has **successfully completed a BachelorB**. Undergraduate studies may neither have been in computer science nor a related discipline. However, student may be able to meet **pre-requisites** (e.g., having attended and successfully completed several types of courses during her undergraduate studies or else attend these courses before being fully admitted to the program(e.g., mathematics and computing). Master studies will be done in computer science with a concentration on information security (i.e., concentration courses & master thesis address security issues		X 120 ECTS
6) Student may have completed undergraduate studies in any subject.		X 120 ECTS

[a] A student in a specialized program may already have a Master from a consecutive type program. A well-known example is a civil engineer that may have an undergraduate and graduate degree in engineering and then decides to acquire a Master of Business Administration (MBA) degree to improve managerial skills. Generally, specialized programs are offered to satisfy continuous education needs and may be attended part-time. Ever more likely, such a program will be funded by fees paid by students attending the program. MSc programs in business using the consecutive structure are being offered throughout Europe (e.g., Aarhus School of Business http://asb.dk/programmes/master.aspx)

as in information security or cryptography. These programs require 30 ECTS credit points including course work and possibly a final thesis. Duration is usually 1 year. Students taking such programs of study attend courses in blocs such as 1 or 2 weeks and/or during evenings and on weekends (e.g., thursday night through saturday morning – in residence). The design of such programs permits students to remain employed full-time while attending.

Diploma programs are another type of program under the Bologna system that are the shortest kind accepted under this system. They require 10 ECTS and are usually attended part-time (see also Table 5 in the Appendix).

Certification programs While certification programs are not part of the Bologna system, however, in the global marketplace they are becoming ever more prevalent. For instance, some of the best-known certifications we know are those required to become a chartered account (also called public accountant), passing the bar to become a lawyer and so on. These designations may differ across countries or even regions for that matter, however, the requirements to be met for having the right to audit financial accounts or defending an accused in court have to be agreed upon by various parties (e.g., association of the professionals, legislators, regulators, etc.).

Table 3 Computer science and information security—science and practice

Science-based education (basic and applied research) (university)	Professional education (polytechnics and universities of applied sciences)
Concepts	Practice—how to
Fundamental recurrences and patterns—generalize	Skilled performance of tasks
Discovery and presentation of ideas	Invention, new products and services
Analysis of the problem	Synthesis of the issues or opportunities
Dissection of the issues and questions	Construction
Theory and models	Principles-based standards ⇒ prescriptive or inherent rules of the trade

The above represents a rudimentary comparison between what could and is most likely taught in a science program at university compared to more professionally focused schools or what others call the art of information security (see also [4] and [7])

The field of information security has various designations as well. However, these designations are not as well established nor have they evolved over decades if not centuries as is the case with a public accountant designation in most countries. For starters, certification in the information security field is less likely a local matter but instead may be an international one instead and often driven by North American interests. For instance, ISACA's Certified Information Systems Auditor (CISA) program that originated in the US is now also widely accepted in Europe. It focuses on preparing professionals to provide IS auditing, control and security services meeting best practice standards.[8] There is neither theory nor science involved in getting this type of designation. Instead, acquiring skills and knowledge regarding best practices and standards is what such training provides (see Table 3).

Moreover, ISACA's Information Systems Control Journal offers with every issue CPE (Continuous Professional Education) credit for CISA designation that includes 15-20 True/False questions (3-5 for each article) with a passing score of 75% earning 1 h of CISA continuing professional education credit. The test is clearly a memory-type one that requires recall and regurgitation but neither critical nor integrative thinking.

2.3 Convergence Quo Vadis

So how does convergence across programs in computer science and information security manifest itself. For starters and as outlined in Point 4 above and similar to North America, with the Bologna program having been implemented the **student can fulfil entrance requirements for a graduate program in information security by having acquired an unrelated undergraduate degree** (see far right column in Table 2). It also points out that the institution can, however, demand proof of proficiency in certain areas. And this is happening across Europe at better known universities, especially, regarding continuous master type of programs. This proficiency could be demonstrated by having attended and attained ECTS credits in certain courses (e.g., mathematics) and, as well, passing an exam before being allowed to register in the graduate program (for more details see the Appendix).

Table 2 illustrates that while the Bologna Declaration puts forward the requirement that a bachelor program should be freestanding from a master degree program and, therefore, not be regarded as part of a longer curriculum, the reality is different. In fact, quite a few of the better known computer science programs expect a related undergraduate program to be able to attend a continuous program. In fact, if the student comes from another university, an entrance examination may even be required. Needless to say that a student having passed a continuous master program will have acquired more in depth knowledge about the subject matter information security, information security engineering or cryptography than his or her counterpart having acquired this know-how in either a bachelor level program or a specialized master program only (cf. Table 2).

Educational focus: science and practice Master and undergraduate programs may also differ in what it teaches a student. For instance, Table 3 below shows that a science focus in a program for information security or engineering has different activities at center stage compared to a program focusing more on practice and what some have labelled the art of a discipline. The latter does not refer to drawings or sculptures but to the useful practices of a field instead, such as information security. As Table 3's right-hand column indicates, professional type schools are likely to teach more applied skills and knowledge regarding information security that could be grouped under the art of useful practices that help one succeed in one's profession. However, as Fig. 1 below also shows, neither a science-based education nor a professional program leading to a bachelor degree can succeed by just focusing on either alone. Instead, a mixture is quite likely.

Until now, Polytechnics or Universities of Applied Sciences taught the more application-oriented curricula. This made sense, because in some countries students had attended

[8] A short description is provided here http://www.isaca-canberra.org.au/certification. Accessed: 30 June, 2006.

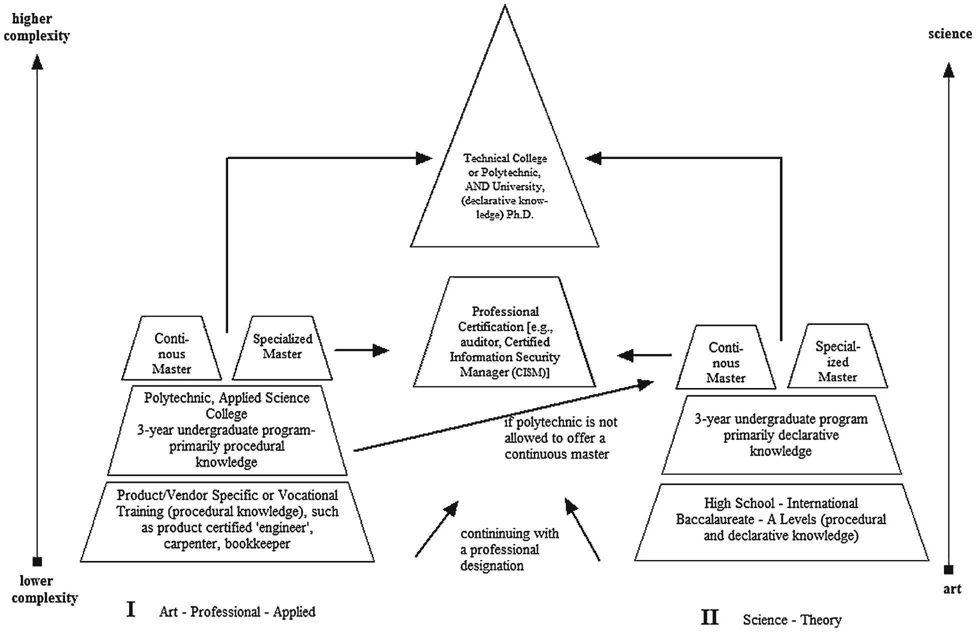
higher complexity
lower complexity
science
art
Technical College or Polytechnic, AND University, (declarative knowledge) Ph.D.
Professional Certification [e.g., auditor, Certified Information Security Manager (CISM)]
Conti-nous Master
Specialized Master
Polytechnic, Applied Science College 3-year undergraduate program-primarily procedural knowledge
Product/Vendor Specific or Vocational Training (procedural knowledge), such as product certified 'engineer', carpenter, bookkeeper
if polytechnic is not allowed to offer a continuous master
contininuing with a professional designation
Conti-nous Master
Special-ized Master
3-year undergraduate program primarily declarative knowledge
High School - International Baccalaureate - A Levels (procedural and declarative knowledge)
I Art - Professional - Applied
II Science - Theory

Fig. 1 Information security education under Bologna process

9 years of formal schooling and thereafter an apprenticeship of 3- or 4-years duration. Apprenticeship programs are offered throughout Europe in different forms. Some require attending school for 2–3 days a week (or doing it in blocs of weeks) while the rest of the time the apprentice works in an organization in the field of the trade under close supervision. In turn, the individual will acquire a “journeyman” certificate that qualifies her to attend a university of applied sciences to study for an undergraduate degree.[9]

Figure 1 shows the two approaches that could lead to a Ph.D. degree using the more practical (see Table 3 left column) applied route versus the more theoretical one at the university. Hence, it is possible that a student doing an apprenticeship in informatics will attend a University of Applied Sciences thereafter to get a bachelor degree. After successful completion, this student may then fulfill requirements for a continuous master in informatics and thereafter begin with his or her Ph.D. studies.

Some countries allow Polytechnics to offer all the programs needed to fulfil the requirements for a research-based Ph.D. Nevertheless, some countries such as the Netherlands have decided that Hogeschools (Polytechnics) will not offer education leading to a Continuous Master degree. Here, the student switches from a university of applied sciences (Polytechnic) to a university for getting a continuous master. Neither do Hogeschools (University of Applied Sciences) offer Ph.D. study programs in the Netherlands. Hogeschools are allowed to offer specialized master studies. In other countries, Polytechnics are free to offer both, Continuous Master as well as Specialized Master program.

Figure 1 also shows that professional designations can be attained after having entered a profession at different levels and stages and these are also different in what they require to receive the designation (e.g., see passing the bar to become a trial lawyer).

Summary Based on Fig. 1 and Table 3 below one has to conclude the following:

1. an applied university’s education will remain more applied than the traditional university program, a natural thing since these universities are supposed to have close relationship with business and industry as part of their mandate;
2. environmental realities have resulted in both, universities and polytechnics or applied universities to offer some instruction about useful practices (see also Table 3 above), and
3. regardless of entering stream I or II (see Fig. 1), the student is able to study for a Ph.D. degree, however, the previous education may have prepared him or her differently regarding theory and doing scientific research and, finally,
4. professional certification may require certain education but this depends upon profession and formal education may be offset to some degree through on-the-job experience.

How the above developments will affect the quality of education at universities and Polytechnics remains to be seen. For instance, doing a Ph.D. at a Polytechnic institution will,

[9] For instance in Switzerland, attaining the journeyman certificate as electrician will enable the person to attend an undergraduate degree program in electrical engineering. If he or she wants to do this at a university, however, an entrance examination has to be passed first.

Table 4 Checklist for the recruiting process of IT officers

Pre-requisites or focus of undergraduate studies	Undergraduate program	Graduate program
Length of program (number of semesters required) Pre-requisites required for entering program (e.g., demonstrated mathematical skills by having attended and passed special courses or passing a subject-based entry exam before being admitted to a program)	Total ECTS acquired Course work and other requirements	Total ECTS acquired Undergraduate course work required and other pre-requisites
Specialization taken whilst studying computer science, such as information security, information assurance, etc. i.e., total number of ECTS credits taken in information security	Which specialization and depth attained	Bachelor program and high school
Thesis topic (ECTS credits obtained—other things considered equal—the more the greater the scientific and research component included)	ECTs credits	Depth and quality (science vs. regurgitation)

all else considered equal, be more applied than if it were done at a university. If this affects the quality of students getting a Ph.D. remains to be seen.

3 Teaching information security: what can we expect from graduates?

Globalization has resulted in a convergence of standards[10] and the Bologna Declaration is one of the many results thereof. However, when looking at post secondary education and information security, convergence should not result in a shift from principles-based standards to prescriptive rules.[11] The same must apply for education. Hence, doing a good job in information security must surely be more than checking answers off a multiple-choice list.[12] In a recent study across Europe [2], the authors pointed out that information security skills and know-how represent a moving target. Moreover, the study concluded that while training at university or technical colleges focuses on more general-type issues, the work in the certification and skills area is clearly addressing vendor and industry specific concerns.

Table 4 provides a rudimentary checklist for managers and human resource experts to assess differences amongst job candidates coming with various educational backgrounds applying for an IT security and risk management opening.

As Table 4 shows, all else considered being equal, the more courses in mathematics were taken in order to meet graduation requirements, the more likely will our graduate be able to handle technical issues. Also, the more ECTS credits are taken in a sub-discipline such as security engineering, the greater the in-depth understanding of this area that our graduate should bring to her new job.

Not every activity in a university-type education must have practical effects that are quantifiable, such as passing a multiple choice test with 250 questions to be able to know anything about information security (see the CISSP exam—a professional designation). We also would like to point out that if universities go too much along with providing training that suits vendors, industry and government, they may err too much on the side of providing students with piecemeal skills that soon become absolute. Rapid change in information and wireless technology poses new challenges. Our moving toward ubiquitous computing in a nanotechnology environment, moreover, requires educated professionals that are curious and able to do some unorthodox thinking.

Neither does the certification mania catching on in Europe help in making the above differences easier to discover nor explain how to apply them in the hiring process. An applicant applying with a CISSP or CISM designation brings some additional education that enabled one to answer multiple-choice questions successfully. Having answered a certain percentage correctly qualifies one to be given this designation. In order to keep the designation, continuous education credits are needed. These may be attained by attending a conference or workshop as well as reading a magazine and answering a set of true-false type of questions successfully. Unfortunately, such training does not foster integrative and reflective learning or what some may prefer to call out of the box thinking. Nonetheless, in an ever faster changing technology and threat environment out of the box thinking is required to

[10] For more information about this term see here: http://cytrap.org/RiskIT/mod/glossary/view.php?id=2&mode=entry&hook=391 (click Login as a guest for free access).

[11] For more information about this term see here: http://cytrap.org/RiskIT/mod/glossary/view.php?id=2&mode=entry&hook=390.

[12] CISSP stands for Certification for Information System Security Professional. For an explanation of the CISSP designation see here: http://cytrap.org/RiskIT/mod/glossary/view.php?id=2&mode=entry&hook=401. Accessed: May 28, 2006.

improve protection of information assets. Additionally, using innovative process management will help to dwarf malware threats. In fact, we fear that some professional designations being offered on the market add little to the quality of one's work, or enable one to innovate organizational processes to better protect and leverage information assets.

This does not mean that continuous education is not a thing required for skills and knowledge updating that helps one succeed in any profession. However, convergence in standards has also resulted in an increasing number of prescriptive standards whereby checklists are used to protect one in a litigious society. This is in contrast to principle-based standards that follow common sense rules, whereby the regulator may outline what should be done and the enterprise has different choice to do so but, most importantly, must be able to explain why it did things in a certain way.

In contrast, prescriptive standards make it appear, at least at first, easier to satisfy the rules because they outline what is wrong and what is right and can, in turn, be used to take another party to court. Else they also allow a regulator to impose a hefty fine if need be.

As Table 4 suggests, for recruiters and human resource specialists it is not necessarily becoming easier thanks to the Bologna model. At first glance, a degree in computer science with a specialization in information security or assurance from two universities may appear similar. However, the art of cooking is not just having the right ingredients but, instead, it also requires a bit of art and science to get there. Without the proper mixture, the chef is unlikely to succeed in her efforts for getting awarded a star in the Michelin Guide. The same applies to information security experts and engineers. The right mixture of science and art must be attained to succeed where many others have failed.

3.1 Teaching information security: understanding the principles of malware

The question could be raised how the convergence of programs in computer science both at the undergraduate and graduate levels have affected training and preparation of students for information security. For starters, many people might state that malware is not a scientific discipline but represents work by technicians. And while we do not want to get down this road, if malware is a scientific discipline it requires a precise definition similar to what a mathematician understands under the term "root" compared to a botanist. The definition of root for both is quite distinct and misunderstandings are unlikely. While we may be able to define malware to some extent one will hardly be able to claim that this is a unified definition shared by many as exhibited by mature scientific disciplines (cf. [6]). The uniqueness of the meaning of words is characteristic of the scientific method and results in a shared vocabulary as well as a shared paradigm describing the discipline (see also [8]).

Teaching malware Teaching students about malware at university level can cause a stir in some circles. In fact some people may state that knowing about malware is neither useful for becoming a security expert nor will it help students in acquiring the skills needed for programming more secure applications. Of course, the totally opposite opinion is also found amongst anti-virus vendors.

As we pointed out previously, undergraduate and graduate education focus on helping students learn and understand concepts, theories and foundations of disciplines. So as part of *security assurance* or information security, malware epidemics are a clear example that not all may be up to standard regarding the correctness, consistency, or completeness of the requirements and implementation of those mechanisms. The use of code path analysis will surely help in reducing the number of vulnerabilities that will be used by zero-day exploits.

But training students regarding concepts and theories about malware means that instead of just focusing on "how to do things right" university education also addresses "how to avoid doing things wrong" or what can happen if one does things wrong. To illustrate this challenge further we provide two examples below.

Canada In North America malware has entered the curriculum of computer science programs in various ways. Most famous was the recent example by the University of Calgary (U of C). Here, fourth year computing science majors meeting certain course pre-requisites may apply to be accepted for registration into a course addressing malware issues.[13] The U of C announcement in summer 2003 created a stir in anti-virus vendor circles at the time. Several vendors chose to misquote material and get excited about nothing spectacular. In fact, the teaching objectives in this course are very much in line, with what one would expect from an advanced undergraduate course for computer science majors in information security [1].

In reality, theory and practice are symbiotic. Hence, business practices in the commercial world led to the development of several security policy models such as the Clark-Wilson model. These models in turn help designers of

[13] CPSC 527—Computer Viruses and Malware (was CPSC 599.48) see here: http://pages.cpsc.ucalgary.ca/ aycock/virus-info.html and the U of C described the course in Summer 2003 (first being taught during Fall semester 2003) as: "Once again, the University of Calgary's department of computer science explores new territory as it becomes the first institution in Canada to offer a course in computer viruses and malware as part of its undergraduate program. This course is unique—along with covering legal, ethical and computer security issues, it will focus on developing malicious software, such as computer viruses, worms and Trojan horses, that are known to wreak havoc to the tune of billions of dollars worldwide on an annual basis."

Table 5 Work load and grading for the different university programs being offered under the Bologna program

Work load at a glance	What it means
1 credit point means	25–30 h of work for the academic year
60 credit points are given per academic year	requires full time study
180 credit points are required to attain a Bachelor degree	3 year full-time study
Post graduate programs	
90–120 credit points for a master degree (see Table 2 for discussion of continuous versus specialized master programs)	Three or four semester of full-time study
30 credit points for a diploma of advanced studies	Two semesters part-time
10 credit points for a diploma	One or two semesters part-time
Grading scheme	
The Bologna program does also try to standardize grading scales being used	A best 10% of students, B next 25%
This grading scheme suggests a forced distribution	35% of attending students receive a B or A
Grade inflation means that rarely if ever do 65% of students receive a C or lower and it might be the other way around. In reality then, 65% or more receive a B or A.	C next 30%, D next 25%, E next 10%

security policies to better understand and evaluate the mechanisms and procedures required to secure their sites. Courses at university level teaching virology in computer science focus on building virus-resistant systems that might help reduce the risk for a new type of malware or a variant string of a well-known virus from spreading quickly between vulnerable systems.

France The above U of C example describing an anti-virus course indicates that some vendors want universities to specify their curriculum according to what they think is appropriate. Naturally, for the betterment of society, universities should resist these attempts.[14] The stir caused by the anti-virus course at the University of Calgary came a bit as a surprise to many researchers in Europe. Teaching about virology is apparently a more common practice in Europe than in Canada or the USA. Partially, this can be explained by a different educational focus. For instance, most French computing science programs have either a course that includes a virology component and/or the programs require attending students to successfully complete such a course [5].

Naturally, such type of courses at French universities or other ones across Europe are taught within the strict limit of the law. Neither do these courses propagate virus writing nor do they allow students to spread viruses. Instead, course materials and exercises try to apply scientific principles to these situations. In turn, students are being enabled to learn engineer systems that could be less vulnerable to these types of menace. Additionally, such teaching and research also helps students and scientists discover if accepted practices in engineering can be changed to improve security levels. The latter may foster better efforts for safeguarding systems, data and information against future attacks and new forms of malware.

4 Conclusion

This paper tried to address three issues:

1. outline how the Bologna Declaration is influencing education in information security across Europe,
2. what content or training such programs provide across the educational landscape and
3. what the effects of these efforts are upon the quality output produced regarding our graduates level of scientific knowledge, understanding and skills needed to perform in their work careers.

Below we try to outline the implications of our discussions for educators, policy makers and software vendors.

4.1 Implications for educators

In France, pre-requisite for most programs in this area is having passed education and exams reaching a certain level of mathematics (e.g., http://www.supelec.fr/cgi-bin/reframeFc?http://www.supelec. fr/fc/ms/QDR.htm or http://www.cryptis.unilim.fr/). The student must have passed a specified set of courses in mathematics during high school to enter an undergraduate program in computing science or information security. Moreover, additional courses in mathematics must be completed successfully during undergraduate education to

[14] During Fall 2005 the U of C also began teaching a course entitled CPSC 528—Spam and Spyware (was CPSC 599.63) http://pages.cpsc.ucalgary.ca/ aycock/spam-info.html.

meet the pre-requisites for a Continuous Master type of education in computing science (see also Table 5).

Denmark, Switzerland and Germany, to mention a few more examples and as discussed in this paper, all have similar requirements regarding mathematics to be qualified and accepted into a master program that leads to a continuous level type of degree (i.e., building upon one's undergraduate degree, see Tables 1 and 2) in information security, cryptography or computer science.

In fact, we hope that in Europe and elsewhere universities and their teaching staff in particular continue to strive to teach students higher-order learning. Moreover, advancing science, theory and practice is a must while worrying about day-to-day issues that concern security software vendors is something to be kept to a minimum.

4.2 Implications public policy decision-makers

Here we narrow down our reflections regarding public policy to issue about information security and malware in particular. If malware will ever become an independent academic discipline and at this point we dare to state that it will not likely become such in the European university setting, there must be room for work at different levels of intellectual rigor for the betterment of society.

The pre-occupation with using benchmarks for comparing programs across institutions, regions, countries and continents appears very appealing in light of the ever greater demands for accountability and transparency by taxpayers and students alike. In the process, however, we will create a lot of paper work and have to cope with administrators who are busy developing another survey, assessment tools and more. Unfortunately, educational institutions and educators will do what humans have always done, work the system by making sure they perform according whatever ineffective criteria is being used (see Appendix, section on tuition where we outlined the problem with accreditation agencies who enjoy a booming business thanks to the Bologna process).

Unless we remain vigilant regarding excellence and focus on learning about science instead of some ephemeral skills and techniques, our educational efforts will produce graduates who will fail to be able to improve information security and protect our infrastructure.

4.3 Implications for software and anti-virus vendors

Vendors want to hire graduates that possess the tools as well as the scientific knowledge that will enable them to develop models and response technologies that help better protect the reliability and dependability of large and small systems including home PCs and smartphones. Pervasive computing implies an environment in which the dominant communications device is a descendant of today's smartphone, Like the current generation of broadband-connected desktops, the pervasive computing device will always be turned on; always hooked in to cyberspace. This will bring new threats to users while the spreading and prevalence of malware may be far greater than we can imagine today. Moreover, home networks linking the fridge, stove, home entertainment system, smartphone and/or any other communication device are all linked thanks to IPv6. For the home user worst is that these network enabled white goods and household devices and can be accessed from the Internet by an attacker.

This requires employees that are ready to consider these threats in a systematic and scientific way. If necessary, staff must be able to think out of the box to find solutions that better protect users' rights, confidentiality of data and privacy. Future work of security experts can be understood by describing three distinct job descriptions or groups of staff:

1. Repository keepers or archivists act like librarians and try to make sure that company's data are captured, maintained, secured and accessible in cases of need. An example would be e-discovery (e.g., sent mails to produced as evidence to the judge) or fiscal requirements were archived information must be found and provided quickly to the judge or the tax authorities.
2. Optimizers or consolidators focus on deploying technology as efficiently as possible (e.g., anti-virus software updates, installing patches) for squeezing more out of technology, making better use and streamlining systems (e.g., making use of fewer systems rather than more to minimize maintenance and security assurance costs).
3. Innovators will be employees who are charged with looking beyond immediate business needs to find new opportunities and processes or applying technology more effectively while assuring that compliance and satisfactory data confidentiality and security is achieved.

The above indicates that there is plenty of room for more applied programs (e.g., optimizers) as well as mort theoretical ones (e.g., innovators) since all these vastly different skill sets are needed to succeed. If certification adds much beyond what polytechnics and universities can add to acquire the set of skills needed for taking advantage of changes that will affect security of data and information remains to be seen. Nonetheless, multiple-choice and true/false questions will not produce the type of security officers we need, in order to cope with ever more sophisticated malware. Neither will it give the skill set most helpful in developing processes that reduce risk exposure regarding new type of malware.

Hence, while Bologna has helped standardize the educational landscape somewhat, much remains to be done and quality assurance regarding information security is a never ending challenge.

Acknowledgments The author would like to thank Eric Filiol (Ecole Supérieure et d'Application des Transmissions, France) for his important suggestions and comments made on an earlier draft of this paper. All omissions and mistakes are my own.

A Thoughts about Bologna from a bystander

Europe has embarked on a journey of convergence regarding undergraduate and graduate education, since the Bologna Declaration was signed in 1999 [9].

A.1 The facts

In short, it focuses on four issues, namely:

1. Developing a framework that helps increase mobility for learning and teaching while strengthening collaboration across Europe,
2. Acceptance and accreditation of degrees and training across national borders,
3. Structure tertiary education using two levels based on undergraduate and graduate programs whose completion results in Bachelor and Master degrees,
4. Introduction of the European Credit Transfer System (ECTS) that allows students to transfer credits to another institution in another country (e.g., see point 1 above).

In practicality the Bologna Declaration has resulted in the Bologna-type of system distinguishing between graduate and undergraduate courses, thereby facilitating the comparison and mutual acceptance of degrees and certification across national boundaries.

The agreement was launched by European countries and does, therefore also include states that are not members of the European Union, such as Switzerland and Norway.

By the end of 2006, 45 countries had signed up to the Bologna accord. And while the Bologna accord should be implemented by 2010, it is unlikely that this deadline will be met. Some have suggested that having more countries and systems sign up to the accord such as Asian and Pacific Rim countries, is more important than meeting the 2010 deadline.

A.2 Admission requirements

Much has changed but more remains the same. So while in theory Bologna allows a student to enter a program, high-quality programs may impose specific admission requirements. For instance, member institutions of the IDEA consortium (Swiss, German and Dutch institutions) require specific pre-requisites regarding math courses for both, undergraduate and graduate programs. In fact, admission requirements can be such that the student must pass an entrance examination if the applicant does not appear to have the required knowledge (see http://www.theidealeague.org/about_us/index.html, Accessed: 16 May, 2006).

In France, pre-requisite for most programs in computer science is having passed education and exams reaching a certain level of mathematics (e.g., http://www.supelec.fr/cgi-bin/reframeFc?http://www.supelec. fr/fc/ms/QDR.htm or http://www.cryptis.unilim.fr/). The student must have passed a specified set of courses in mathematics during high school to enter an undergraduate program in computing science or information security. Moreover, additional courses in mathematics must be completed successfully during undergraduate education to meet the pre-requisites for a continuous master type of education in computing science (see also Table 5 below).

A.3 Work load

The Bologna system proposes about 30 h of work per unit of credit. Considering 30 units are given per semester, using the ECTS system adds up to 900 h a semester (30 credit points × 30 h) and over 16 weeks per semester would mean the student has to work about 55 h a week on average. Considering that many work part-time ranging from as little as 5 h up to 20 h a week, the work and study week would be long and intense. As well, students submitting to such rigor and time demands will represent a relatively small group of the total undergraduate and graduate student populations.

A.4 Tuition

Most European countries try to make post-secondary education as affordable as possible by limiting tuition and other fees. In turn, the vast majority of university programs and institutions are government funded. In some cases, private support from alumni, endowments and third-party research funds can be considerable. For students, this means that tuition and fees may be a couple of hundred euros a semester for a local resident or EU citizen attending a public institution in Denmark. Attending the same program at a publicly funded institution in the UK may result in several thousand euros in fees and tuition each semester.

With the Bologna Declaration, publicly funded institutions have launched graduate programs that are supposed to be self-financing which, in practice, means tuition and fees are needed to finance these privately funded programs. Here, a 2-year master program may come with a price tag of up 15,000 euros or more in tuition and fees excluding living expenses and health insurance.

Additionally, most students attending post graduate programs work part-time sometimes up to 20 h or more a week to make ends meet. This has also put pressure on the workload. A situation is developing whereby only a few prestigious institutions will be able to attract students that pass strict admission requirements for high level tuition programs. As well, few programs will be able to demand the work load per credit unit as described in the Bologna program (16 week semester—55 h per week) (see also section on admission requirements above).

A.5 Change in academic and educational focus may not be desirable

It is clear the Bologna program tries to move post secondary educational programs toward greater convergence. At first glance this is happening rapidly. However, differences remain such as self-funding programs possibly being more lenient toward applicants regarding meeting pre-requisite course requirements and work load demands put upon students to pass courses.

Students being used not having to pay much for attending university are naturally highly suspicious for having to pay what the might perceive as exorbitant tuition fees. Once a student submits to such fees, in turn, she will challenge the program concerning services and teaching quality. In fact, similar to executive programs, independent learning may no longer be the primary focus.

Unfortunately, supplying students with presentation slides and as some say "chewing out the material for them" could become the key for getting above average teaching evaluations from students. Moreover, students want good grades to land the jobs they might feel they deserve. In such a constellation of circumstances, grade inflation is just around the corner (see also Table 5). As a result, nobody wants to get a grade that indicates average performance but, instead, receiving top grades is 'expected'. In turn, a job applicants' grade-point-average is becoming more difficult to interpret because market pressures may in part result in grade inflation at many institutions of higher education across Europe (cf. Table 5).

A.6 Benchmarking programs reinforces developments

Similar to other countries, benchmarking everything has become desirable if not the norm. In turn, university teachers are benchmarked against department, faculty or university colleagues as well as across institutions. As a customer, students demand service that meets their needs especially in high-tuition programs. Similar to grade inflation pressure, professors experience teaching evaluation and external funding pressure. Hence, satisfied students as reflected by wonderful evaluations are becoming a condition for continuous employment as teacher. The challenge for the latter is to be able to make students appreciate that thoughtful work advancing one's own thinking and level of understanding of the information security issues one's studies and learns about requires concentration, time and hard work. Wouldn't it be nicer to listen to one's favorite show through one's iPod instead?

Considering the above mania for benchmarking it comes as no surprise that the Bologna program requires national governments having their university programs accredited. This was done in the hope that it would result in intellectually stricter criteria for universities. But hoping for A while rewarding B may be the result. For instance, universities have already shown their swift adaptability to the new realities by choosing the accreditation agency in a country that suits their needs best. Accordingly, a university may choose one accreditation agency over another for quite rational reasons. For instance, the International School of New Media—University of Luebeck (www.ISNM.de) chose ZEvA over ASIIN for accrediting its MSc.

ASIIN is the only German accreditation agency specializing in accrediting degree programs from the fields of engineering, informatics/computer science, the natural sciences and mathematics (http://www.asiin.de/english/newdesign/index_ex5.html). ZEva (Germany's first such agency) was launched by the universities of the state of Lower Saxony, with a particular focus in evaluating and accrediting programs with an international focus.

To illustrate these differences between agencies further and how universities are forced to play this game, ASIIN requires a higher mathematical and science component in the programs it evaluates than ZEvA does. This requirement applies regardless if a continuous or a specialized master is being assessed for possible accreditation by the agency (see Table 2). Hence, depending upon the national accreditation agency's emphasis, programs it certifies may be similar in name but definitely not in content. Fact is that different levels of mathematics being required as a pre-requisite do change the focus of a master program in information security quite a bit.

Choosing an evaluation agency carefully is a must because the evaluators will benchmark the program they evaluate against other programs the agency has accredited. Moreover, regular evaluation exercises are needed to demonstrate that what is termed 'satisfactory quality' by the accreditation agency is being maintained by the institution.

A.7 Conclusion

The above might seem that we are against the Bologna program. Far from it we think it is a wonderful idea but the devil lies in the details. Also, if we continue to be focusing too much upon trying to benchmark and measure learning with simple scales and questions that may fall short of providing us with a better understanding about the complex process of learning (e.g., was the professor prepared for her classes), we may achieve A whilst hoping for B.

References

1. Aycock, J., Barker, K.: Viruses 101. ACM SIGCSE Bull. **37**(1), 152–155 (2005)
2. CEPIS and authors Weiss, P., Dolan, D., Stucky, W., Bumann, P.: ICT-skills certification in Europe. (2005) http://www.cepis.org/download/ICT- Skills_Certification_final_report_cedefop_v14_rev_bs_fgr_30_03_05.pdf. Accessed: 17 May, 2006. (see Table 1 in the above report on p. 32 for an overview of certification programs assessed—lowest credibility for industry offered programs such as Company X security engineer, etc.)
3. CRUS (not dated): Was ist ECTS (What is ECTS). (Last modified: 10 January, 2007), (http://www.ects.ch/) (Last access: 1 March, 2007)
4. Denning, P.J.: Is computer science science. Comm. ACM **48**(4), 27–31 (2005)
5. Gattiker, U.E.: Virology—preparing our students for the future. Available online: http://cytrap.eu/blog/?p=130 Last access: 4 January, 2007
6. Gattiker, U.E.: Malware—the jargon glossary. Available online: http://cytrap.org/RiskIT/mod/glossary/view.php?id=2&mode=entry&hook=317. Last access: 1 March, 2007
7. Gattiker, U.E.: W21-2005-Bookreview—introduction to computer security in **EU IST News** (http://casescontact.org/euist_view.php?newsID=3650). Accessed: 16 May, 2006
8. Kuhn, T.S.: Structure of scientific revolutions. University of Chicago Press, Chicago (1972)
9. The Bologna Declaration of 19 June 1999. Joint declaration of the European Ministers of Education (http://www.bologna-bergen2005.no/Docs/00- Main_doc/990719BOLOGNA_DECLARATION.PDF) (Accessed: 16 May, 2006)