SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World* [†]

Deliverable D3.3: Common Curriculum

Abstract: In this deliverable, we discuss the way the consortium designed and implemented the SysSec common curriculum and the reasons for doing so. The common curriculum is currently operational and finds increasing use among the system security community, well beyond the consortium itself.

Contractual Date of Delivery	February 2013
Actual Date of Delivery	April 2013
Deliverable Dissemination Level	Public
Editors	Andrei Bacs & Herbert Bos
Contributors	All *SysSec* partners
Quality Assurance	Vladimir Dimitrov, Ali Rezaki

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

[†] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

Contents

List of Figures

1 Introduction

The EU/FP7 Syssec project has the main goal of creating a Network of Excellence in the field of Systems Security in Europe. One of the core activities of this network is the promotion of cyber security education which would form the next generations of researchers as well as industry workforce. A key component of the activity is the development of a common curriculum that will benefit instructors both from within the consortium and from the broader community.

1.1 Approach and motivation

At the outset, the consortium did not have a very clear idea of what would constitute the common curriculum. For instance, we have explored the development of a reference curriculum (e.g., for a master degree), a compilation of courses used in a program in systems security taught at any of the participating universities, and an infrastructure which facilitates participating universities to both use and contribute course material.

When presenting our ideas to the Industrial Advisory Board, the Board unequivocally advised against a reference curriculum or a compilation of courses. The reason was that the IAB members had experience with other attempts in these directions and they had all failed. Also, they argued it is not practical: instructors interested in adding system security material to his course, are not well served with full-length programs. Because of the interdependencies of material in a full course, it is complex to extract exactly the topics in which the instructors are interested.

Instead, the IAB suggested to make material available in the smallest chunk size possible. So, rather than full courses, make available focused and more or less self-contained presentations, exam questions and assignments, such that instructors can very easily adopt them. As the common curriculum would be defined as a set of lectures with their own structure

and topics, participating universities can very easily restructure the curriculum and group the topics in the appropriate courses.

The consortium thought that this was a very good suggestion and we started developing an infrastructure to accommodate this approach. The requirements we set for this infrastructure were: maximum flexibility and minimum complexity. Specifically, we should allow any and all course material to be uploaded and require virtually no prior knowledge to do so.

The infrastructure, described in detail in this deliverable is now available to all consortium members and all associated partners as an on line learning environment which contains lectures, exam questions and general background knowledge.

1.2 Outline

The components of the common curriculum are described in the following chapters. In Chapter 2, we explain our view on a computer science degree with a strong system security component. In Chapter 3, we discuss the infrastructure for the common curriculum. In Chapter 4, we give preliminary information about the curriculum's adoption.

2 Adopting a common curriculum

As pointed out by the Industrial Advisory Board, it is difficult to define a common curriculum in system security and expect it to be adopted widely. Requirements differ for different universities and different programs, and a one-size fits all solution does not work. At best, we could define topics that are important for a curriculum with an emphasis on systems security, but in the end, each degree program will make its own choices about what to include.

In addition, we would be faced with the complex task of deciding what program(s) and degree(s) to aim for. Should we define a curriculum for a master in pure system security? Or a master in computer security with system security components? Or a broader computer science master with a track in security? And should it be a one year master, or a two year master? Or should we aim for a bachelor program? Or a post graduate degree?

Moreover, keeping a complete curriculum up to date and consistent over a longer time is challenging.

Still, the SysSec consortium does want to provide some guidance for higher education organizations to help them set up their curriculums. Rather than defining a SysSec curriculum, we compile an overview of the curriculum in the area of system security a number of top universities, as well as the ACM reference curriculum.

The main thrust of the SysSec common curriculum, however, is our collection of focused lectures that we compile and make available via the infrastructure. The collection serves as a repository for instructors; they can browse and pick out exactly the material they are looking for. In contrast to a complete degree program, this is very easy to do. If one wants to start a course on Application Security, say, one can simply make use of material such as the presentation about buffer overflows, forensics, taint analysis, etc. And when one wants to teach about malware, one can select the material about reverse engineering, IDA, static and dynamic analysis, the un-

derground economy, etc. And one could throw in some of the assignments also.

We only mention the system security topics from within the general area of security and do not deal with the complementary courses which may vary considerably based on the level at which the security programme is taught (bachelor, masters, etc.). Moreover the structure of the curriculum which is implemented at a university may be different from other universities. Even if the universities choose to teach the same topics, they may include them in different courses.

3 The common curriculum infrastructure

In this chapter, we first explain what environment we selected for the infrastructure and why. Next, we explain the set up of the common curriculum infrastructure for SysSec.

3.1 Selecting an environment

The requirements we set for the infrastructure were that we should make it easy for any instructor to download and upload any course material. On the other hand, it should not be possible for students to access assignments, exams, and hints. Moreover, we want an infrastructure that allows for more advanced features such as a subversion repository, mailing lists and discussion groups in the longer run.

The consortium surveyed several online learning environments such as Blackboard and Moodle, and several SCM and project management systems such as Trac, and Gforge. The feeling of the consortium was that both of the online learning environments were too heavy-weight and not sufficiently simple. Moreover, we anticipated that we might require advanced features such as a source code repository in the future, and did not see a way to integrate this easily with either of the two environments.

On the other hand, the consortium was quite taken with the wiki-based environment in Trac. Wikis are very common, require very little training to modify, and no training to use. Since Gforge also contains a wiki environment, has even more features than Trac and is already in active use at the WorkPackage leader's university, the consortium decided to use Gforge.

A full description of the Gforge webserver can be found here: [2].

3.2 The common curriculum on Gforge

The common curriculum course material is hosted at a web based Gforge server[1] which is available to the consortium partners, as well as the associate members of Syssec[2].

All course material is currently kept in a wiki[3] based environment which is both flexible and easy to use. Other features such as mailing lists, discussion boards, tracking and versioning systems are available and augment the possibilities of the learning environment. Figure 3.1 shows a screenshot of the main screen of the common curriculum environment.

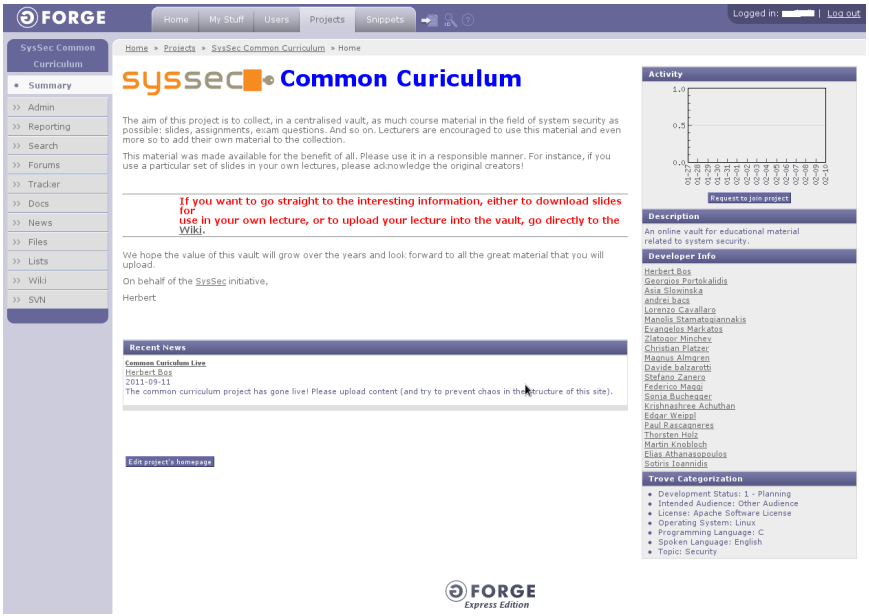

Figure 3.1: The Common Curriculum Environment main page

We see that the menu on the left allows convenient access to mailing lists, forums, news, information about users etc. The menu also gives immediate access to the section that is currently most active: the Wiki.

The main page also draws the users attention to the Wiki with a message in red and a direct link to the content. The Wiki is convenient environment for reading, adding and modifying content. Figure 3.2 displays a screenshot of the wiki main page with a link to the tutorial which explains how to add or modify content.

The presentations are grouped per category. For example, Figure 3.3 shows the memory corruption group of presentations made of Introductory

[1] https://gforge.cs.vu.nl/gf/project/syssec_edu/
[2] http://www.syssec-project.eu/community/
[3] http://en.wikipedia.org/wiki/Wiki

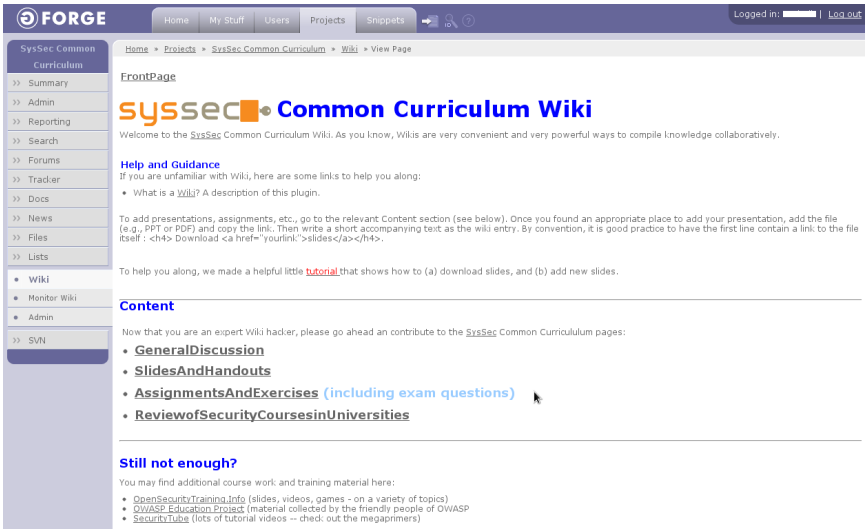

Figure 3.2: The Common Curriculum wiki main page

material, Advanced material, and Dynamic Taint Analysis. Each presentation details a different aspect of memory errors which an instructor may chose to include or omit from her/his course.

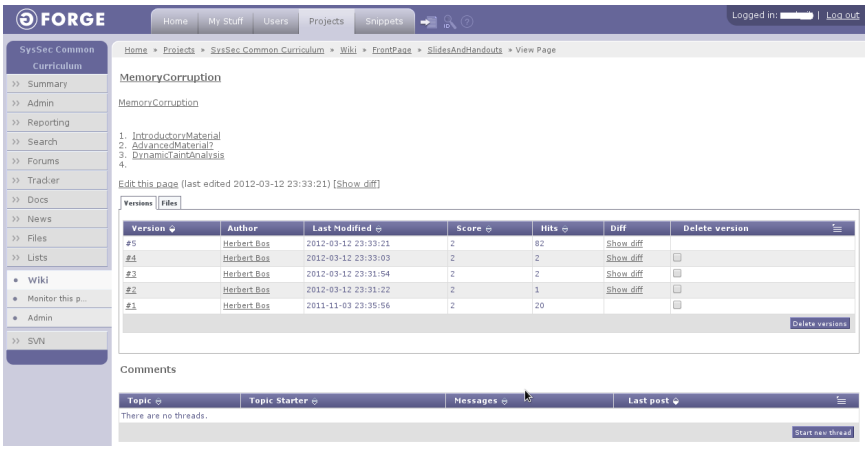

Figure 3.3: The memory corruption group of presentations

Each presentation from a group has a description together with the slides. For example choosing the Introductory material presentation from the memory corruption group mentioned above opens the page presented in Figure 3.4. An instructor can quickly read the description and decide if the presentation is relevant for the course.

The common curriculum also provides a section on the wiki page which contains interesting exam questions covering many topics. These are es-

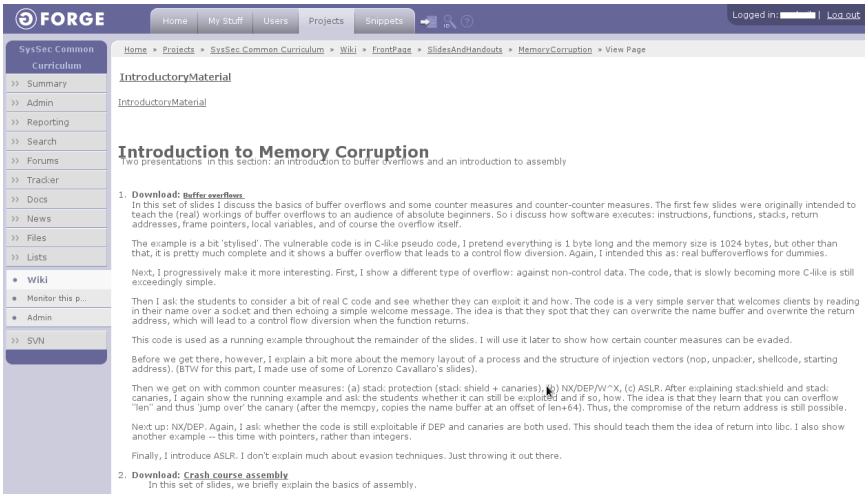

Figure 3.4: Introduction to memory corruption description page

pecially helpful for starting instructors who might have trouble coming up with interesting questions for the exams and can be used as is or as a starting point.

Finally, a special section of the wiki hosts a review of security courses which are taught in universities from Europe or U.S. These are provided as suggestions of how security courses/programs could look like in terms of topics or size. These may be useful for instructors who are designing their courses or degree programs. However we believe that having the single topic (atomic) presentations is one of the key assets of the common curriculum.

The common curriculum infrastructure also provides other means of access to the material than the wiki such as Subversion [1] which is a versioning and revision control system. This augments the wiki with several important benefits such as:

- a full revision history of the files containing the material. This allows to track the changes of every presentation.
- different versions of the same presentation for a topic. This allows for example different level of detail for a presentation.
- the possibility of setting e-mail triggers for modifications of files belonging to a topic or individual files. This would keep members of the project informed of the changes when they occur without the need to visit the project wiki.

When a contributor adds material to the common curriculum infrastructure (s)he can use either the wiki or the subversion repository. In order to

make this simple the wiki keeps a simple tutorial advertised on the main page of the wiki about how to add content. In practice the contributor would use the wiki to upload the initial version of the content and write the description for each topic and then use a subversion client for future updates of the content.

4 Curriculum adoption

In this chapter, we discuss the common curriculum adoption by the Syssec project partners and associate members[1]. We stress that the numbers mentioned in this chapter are very preliminary, since the common curriculum was only recently opened to the associated partners.

When we started designing the curriculum, we initially opened it up for consortium members only. The reason for this is twofold: (1) we wanted to find the most severe problems first, before opening up to the broader community, and (2) we wanted to have some control over the content provided on the Wiki (to create an example for future users). We have currently opened up the site to associated partners. Next year, we plan to make the site available to instructors everywhere.

At the time of writing, the Syssec common curriculum has approximately 25 active users, 11 of whom are not from the project consortium. Given that the common curriculum was created very recently and that we have been restrictive in allowing access to the common curriculum so far, we are quite satisfied with these numbers. The partner universities use the material from the wiki based common curriculum infrastructure in various ways ranging from content for lectures being taught to other events such as summer schools.

To date, the common curriculum contains a number of 30 presentations, a compilation of exam questions, and an overview of curriculums at other universities. So far, we had fifteen downloads of presentations. While these numbers are small, recall that the system has 25 users. We do not know whether the presentation have been used in actual courses outside the consortium, but we know that within the consortium, various several partners have adopted each other's course material to improve their courses. For instance, VU adopted course material from Chalmers and Eurecom for use in

[1] Associate members are usually security researchers which can take part and contribute to the Syssec activities. For details see http://www.syssec-project.eu/community/

a course on computer and network security, and a completely new course on binary and malware analysis, while Chalmers and Eurecom in turn VU's presentations on buffer overflows and taint analysis.

Bibliography

[1] Apache Subversion. http://subversion.apache.org/.

[2] Gforge Collaborative Development Environment. http://gforge.com.