

The CERT[®] Survivability and Information Assurance Curriculum: Education for First Defenders

Lawrence R. Rogers, CERT[®] Program, Software Engineering Institute, Carnegie Mellon University

Abstract – *First defenders (system and network administrators) can significantly benefit from an educational foundation that helps enterprise networks survive the challenges found in today's Internet. The Survivability and Information Assurance Curriculum, created by the CERT[®] Program¹, a part of the Software Engineering Institute (SEI), provides such a foundation. This paper describes this freely available curriculum.*

Index terms – Information Assurance Education, Information Assurance, First Defenders

I. INTRODUCTION

In today's world of computer and network security, much emphasis is placed on the collection of support personnel referred to as *first responders*. While responding to computer and network intrusions is important, comparable attention should also be placed on *first defenders*, that is system and network administrators whose job it is to configure and install, manage and maintain computer systems and network infrastructure components.

First defenders can be more effective in securing these computer systems and network infrastructure components if they are properly educated and trained. They need a way to think about security issues and a set of skills to help them integrate security policy, practices, and technologies into their operational infrastructure. Success in this area also reduces the tasks required of the first responders.

The Survivability and Information Assurance (SIA) Curriculum (<http://www.cert.org/sia>) is designed to teach experienced first defenders about survivability and information assurance as well as a means to integrate these ideas into their routine tasks. The intent is to produce a more secure and predictable operational state.

The concepts and philosophies described in the SIA Curriculum are old in some ways and new in others. For example, first defenders have traditionally done many tasks that now have names and an ordering as prescribed by the Security Knowledge in Practice (SKiP)² method of system administration. While the tasks are old, the ordering is new. Similarly, many first defenders have been aware of policies and procedures—the old way—but using these policies and procedures as constraints that govern actions represents a new way of thinking. Lastly, there is a direct connection between hardware and software technology and the mission of the enterprise, and this too is an example of new thinking.

The SIA Curriculum lays the educational foundation that we believe first defenders need as the basis for the technical training that they also need to be effective when managing the enterprise network. Education and training are complementary and both are needed for long-term success. It is our belief that training only addresses short-term needs and must be repeated often because technology changes often. In this regard, the SIA Curriculum is unique.

This educational orientation means that the courseware identifies, defines, and explores survivability and information assurance issues and principles independent of an instance of technology, such as Windows[®], MacOS[™], or LINUX[®]. If a first defender understands the problem to be solved, they can make better use of the technology available to them. However, if they only understand how to operate that technology without knowing why and when, they run the risk of quickly becoming obsolete and consequently unable to solve a

² See <http://www.stsc.hill.af.mil/crosstalk/2002/11/rogers.html> for more information. This is Principle 7: which is titled "Security Knowledge in Practice (SKiP) provides a structured approach."

[®] Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. See <http://www.microsoft.com/> for more information.

[™] MacOS is a trademark of Apple Computer, Inc.

[®] The registered trademark Linux[®] is used pursuant to a license from Linus Torvalds, owner of the mark in the U.S. and other countries.

¹ [®] CERT is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

problem presented by new technology. The SIA Curriculum provides a needed firm educational foundation upon which technology is layered and first defenders learn through skills training.

II. TARGET STUDENTS AND AUDIENCE

The SIA Curriculum is first and foremost a 3 course, 13-semester-credit hour (162.5 total hours), educationally-oriented product. The intended customers are community colleges, four-year colleges and universities, and graduate schools.

While the material in this curriculum does not necessarily assume that a student has a mastery of all system and network administration skills, a student who is completely new to the operational environment of an IT department in any type of organization will be at a significant disadvantage in these courses. The intended audience then is the experienced first defender.

To learn and apply the principles in a meaningful way, it is assumed that the student will be able to focus more on the principles, concepts, and ideas presented in the material and less on the low-level system administration tasks necessary to implement these concepts. The recommended amount of experience in this area is two years. In the absence of this experience, a student should have a solid computer science or information technology educational foundation, including networking.

Managers of first defenders can also benefit from the first course in the curriculum, even if they lack the necessary technical knowledge or interest in the remaining courses. It is important for those managers to understand the SIA principles so they can better understand and manage the first defenders who work for them.

Even though this product is called the SIA *Curriculum*, we believe that all organizations—not just the aforementioned educational institutions—can benefit from the General distribution³. Much of the writing is in the spirit of the short articles found at <http://www.cert.org/homeusers>, though the SIA Curriculum contains a higher technical content as is appropriate for the first defender target audience. We believe that the General distribution of these materials have applicability beyond the classroom.

III. TECHNOLOGY OF THE SIA CURRICULUM

The SIA Curriculum focuses primarily on providing an educational foundation for systems and network administrators that they can use during their professional careers. Because of this, the curriculum does not

emphasize specific technologies and the skills required to master those technologies. Students who are looking for in-depth training on particular hardware or software need to look elsewhere for that training.

Instead, the SIA Curriculum highlights representative technologies so that instructors and students can connect the concepts in the educational foundation with real-world tasks that they typically perform. To this end, the SIA Curriculum uses Red Hat LINUX Version 9⁴ as the base representative technology.

Red Hat LINUX Version 9 has all of the features necessary for students to apply the principles in a straightforward way and is free to all. Instructors and students who truly understand the system administration problems they are trying to solve will be able to use Red Hat LINUX Version 9 to solve those problems even though they may not be masters of that operating system.

For students and faculty who are not steeped in any version of LINUX, the curriculum contains a one semester-hour lab component in the first course, "Principles of Survivability and Information Assurance." This lab component shows and explains how to use Red Hat LINUX Version 9 and other key applications. Where possible and practical, the graphical interface (GUI) versions of tools are used. This course and the tools demonstrated and used help instructors and students gain the skills needed to be successful when doing the exercises later in the SIA Curriculum.

IV. THE SIA CURRICULUM – A REFERENCE IMPLEMENTATION

The SIA Curriculum is meant to be adapted and adopted by educational institutions to suit their needs. What is provided on the SIA web site is considered to be a *reference implementation*. Some institutions may find that the curriculum meets their requirements as distributed, whereas others may decide, for example, that more business concepts need to be added to integrate it into a wider curriculum. These approaches are right, appropriate, and expected.

Some institutions may choose to substitute a different technological base for the Red Hat LINUX Version 9 base provided in the release. To this end, we have documented at a high level the concepts and philosophies behind making these changes. Institutions must realize that while we believe that Red Hat LINUX Version 9 has most of the features needed to demonstrate the concepts and principles described throughout the curriculum, any substitution needs to address these concepts and

³ Free to those who register and accept the terms and conditions of SIA Curriculum license: see/available at <http://www.cert.org/sia>

⁴ See <http://www.redhat.com/> for more information.

principles even if that substitution does not have a key feature already present in Red Hat LINUX Version 9.

For example, another operating system may not provide the fine grained packaging concept found in Red Hat LINUX Version 9, making the task of removing unneeded system software difficult, if not impossible. This does not disqualify that operating system as the technological base for the SIA Curriculum as long as the task of removing unneeded system software remains in the curriculum. The point is that this task is still a task for the first defender to be aware of and to try to do, even if the operating system of choice does not allow it or makes it difficult.

V. COURSES IN THE SIA CURRICULUM

This curriculum teaches a new method for performing traditional systems administration tasks, and it integrates the concepts of survivability and information assurance into those tasks. The curriculum consists of the following major topic areas, each of which corresponds to one course:

- Principles of Survivability and Information Assurance
- Information Assurance Networking Fundamentals
- Sustaining, Improving, and Building Survivable Functional Units (SFUs)

A. Course Structure

Each course is broken into modules and modules are further broken into topics. Each topic contains instructor information designed to help map the modules into actual class time. This information also provides background notes that help to further explain the module or topic.

Most modules contain the following sets of information:

- Required readings – These readings are expected to be done out of class by students in advance of the module or topic to which they are connected.
- Recommended readings – These readings provide more information for students who want to learn more about a specific topic.
- Quizzes – Primarily in the "Information Assurance Networking Fundamentals" course, quizzes are intended to strongly encourage students to do the required readings before class time. Note that quizzes are only available to qualified faculty.

- Exercises – Primarily in the "Information Assurance Networking Fundamentals" and "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" courses, exercises are step-by-step tasks that students do on computer systems in the institution's lab built specifically for the SIA curriculum. There are tasks to do and questions to answer. These too are only available to qualified faculty.
- Recommended Exercises – These optional exercises are strongly recommended. Students have the chance to do more in-depth work in the lab to learn more about the topic at hand. These too are only available to qualified faculty.
- Guided Tours – Guided Tours show step-by-step tasks needed to complete a job. Most steps are accompanied by a screen capture showing what should happen when the directions are followed. While the screen shots should exactly mirror what one would see when following the specified tasks, in some cases they will not be able to, especially where time and date stamps, network captures, and other volatile information is involved. Students are given the full text and screen captures for all of the Guided Tours for their reference and use.
- Demonstrations – Sometimes the instructor will just show students an instance of technology that they should know about but are not expected to use it in an exercise. In fact, that technology may not even be installed in the lab for students to use. As with Guided Tours, students also have the full text and screen captures for Demonstrations for their reference and use.
- Exam – The last section in a module is the exam. The suggested weight of an exam in a course is provided along with answers, either specific or general as appropriate, in the reference implementation. These materials are only available to qualified faculty.

All of the above items are visually distinguished in the courseware provided in the SIA Curriculum. The specific characteristics of these representations are compatible with both color and black-and-white printing. Table 1 provides the statistics for the entire curriculum.

| Area | Version | Modules Reports | Guided Tours | Demos | Exercises | Exams | Quizzes | Suppl Materials | Total Pages |
|--|-------------------|-----------------|--------------|-----------|------------|-----------|-----------|-----------------|--------------|
| <i>Principles of Survivability and Information Assurance</i> | General | 13 | 12 | 2 | | | | 4 | 792 |
| | Instructor | | | | 12 | 11 | 1 | | 968 |
| <i>Information Assurance Networking Fundamentals</i> | General | 26 | 21 | 7 | | | | | 834 |
| | Instructor | | | | 50 | 21 | 19 | | 1,152 |
| <i>Sustaining, Improving and Building SFUs</i> | General | 11 | 35 | 1 | | | | 5 | 844 |
| | Instructor | | | | 42 | 7 | 1 | | 1,120 |
| Curriculum-Wide | Overview | 28 | | | | | | | 86 |
| | Lab | 2 | 5 | | | | | | 245 |
| Grand Totals | General | 50 | 68 | 10 | | | | 9 | 2,801 |
| | Instructor | | | | 104 | 39 | 21 | | 6,482 |

Table 1 - SIA Curriculum Version 3.1 Statistics

B. Course 1 – Principles of Survivability and Information Assurance

This course presents the ten principles of survivability and information assurance⁵. These ten principles are the basis for the entire SIA Curriculum. Much as a highway is only as sound as the roadbed upon which it was built, the enterprise network is only as sound—from a survivability and information assurance perspective—as the roadbed of principles used to build it. The principles of survivability and information assurance provide a firm, modern, and realistic roadbed for today’s and tomorrow’s enterprise computer networks.

The principles of survivability and information assurance are presented in a technology-independent way. It is very important for first defenders to grasp the fundamental issues of these principles, independent of instances of technology that apply to them. The reason for this approach is that all too often first defenders view the set of problems they face and the solutions to those problems through the eyes of the technologies they know. This technology-constrained perspective limits the space of problems and issues that a first defender can see and their available solutions.

It is a change in mindset for today’s first defenders to dig down deeply in search of the root issues and then step back to apply technology. It may also be a change in mindset for their managers to allow first defenders to approach problem understanding and solutions in this manner. This approach is less satisfying in the short term because results (completion of tasks) happen more slowly but is more satisfying in the medium to long term because problems are more thoroughly understood. Instructors will likely face an amount of resistance from students and managers who expect every problem to be resolved quickly. Being able to sacrifice short-term gains for long-term benefits is an acquired skill and the SIA Curriculum can be a vital part of that process.

⁵ See http://www.cert.org/info_assurance/principles.html for more information.

C. Course 1 – Lab Component

This lab component for "Principles of Survivability and Information Assurance" course is intended to familiarize the students with the specifics of the technology base used in the reference implementation, specifically Red Hat LINUX Version 9. It is intended for first defenders to help them better understand the guided tours and demonstrations presented by their instructors and to do the exercises in the rest of the SIA Curriculum.

It is likely that students will have more specific knowledge of Microsoft Windows. This lab component was conceived, designed, and built to bridge the gap between that system and the specifics of Red Hat LINUX Version 9.

If a student understands the goals of various system administration tasks and can carry out those tasks using Microsoft Windows, then this lab component will teach them how to do many of those same tasks using Red Hat LINUX Version 9. However, if a student does not fully grasp the underlying system administration tasks but instead knows only how to operate specific tools in specific circumstances using Windows or some other operating system, then this lab component and likely the entire SIA Curriculum will be more difficult for them to master.

The key is to first understand the problem to be solved or task to be accomplished and then and only then to apply technology to that solution or task. It matters less whether the technology selected is Windows, LINUX, or some other operating system and its applications.

D. Course 2 – Information Assurance Networking Fundamentals

This course applies the ten principles described and explained in "Principles of Survivability and Information Assurance" to the concepts and an implementation of TCP/IP networking. It takes a critical view of the TCP/IP protocols so that the students are well-informed when

they are challenged to make network-related decisions in the workplace.

Students learn and reinforce their knowledge of networking specifics through out-of-class readings using W. Richard Steven's *TCP/IP Illustrated, Volume 1 – The Protocols*⁶. Quizzes based upon these readings strongly encourage students to do these assignments in a timely fashion.

The bulk of the lectures in the class consist of more detailed, critical, and thought-provoking discussions of the TCP/IP protocols. Challenging protocol assumptions and gauging the risks to the enterprise when using these protocols are important parts of these discussions.

There are many guided tours, demonstrations, and exercises in this course. In addition, a correctly functioning lab as defined by those guided tours and other reports are essential to the successful teaching of "Information Assurance Networking Fundamentals". Due to the volume of material in this course, an educational institution may choose to break it into two course offerings, rather than one higher-credit course offering.

E. Course 3 – Sustaining, Improving, and Building Survivable Functional Units (SFUs)

This capstone course completes the SIA Curriculum. In this course, students inherit an existing enterprise network and their objective is to manage it according to the principles learned in "Principles of Survivability and Information Assurance". "Information Assurance Networking Fundamentals" provides the basis for understanding the network underlying the existing network they have inherited. This course is designed to provide a framework for managing existing Functional Units (FUs) with SKiP, assessing the critical information asset risks with the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE[®]) method, and adding a new Survivable Functional Unit (SFU)⁷ to the existing infrastructure.

This is a laboratory-based course where students work mostly in teams. Each team sustains and improves a Functional Unit identified in a lab-based enterprise network. Improvement, in this case, refers to improving the level of survivability of the Functional Units, thereby making them Survivable Functional Units. The instructor then demonstrates how to add a new SFU to the network, which is the "building" part in the title of "Sustaining,

Improving, and Building Survivable Functional Units (SFUs)". Time permitting, students design and build this SFU and integrate it into the enterprise network in the lab.

As in "Information Assurance Networking Fundamentals", there are many guided tours, demonstrations, and exercises in this course. Again, a correctly functioning lab, as defined by guided tours and other reports, is essential to the successful teaching of "Sustaining, Improving, and Building Survivable Functional Units (SFUs)".

VI. THE LAB

The lab for the SIA Curriculum is used in all of the courses in the curriculum. It is built from commodity hardware and public domain software. The only purchased software is VMware Workstation for LINUX⁸ which is available from VMware, Inc⁹.

Guided Tours explain how an institution should install and configure various key parts of the lab, but not all of the parts. There are several parts for which the institution is responsible and must make installation, configuration, and maintenance decisions.

The lab for the "Principles of Survivability and Information Assurance" and "Information Assurance Networking Fundamentals" courses can be built entirely using the Guided Tours, the list of hardware and software identified in lab overview report¹⁰, and the lab supplemental materials.

However, for the capstone course, entitled "Sustaining, Improving, and Building Survivable Functional Units (SFUs)", the lab requires an implementation that at this point is only a design¹¹. It is hoped that there will eventually be an implementation built by one of the institutions that adopts the SIA Curriculum. That implementation should be as complete as possible, and able to be used not only by the initial institution building it, but also by others to build their lab. Until that time, the detailed design documentation must suffice.

VII. CHARACTERISTICS OF SUCCESS

The SIA Curriculum represents new ideas and new approaches to many of the traditional tasks of the first

⁶ See <http://www.kohala.com/start/tcpipiv1.html> for more information.

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

[®] OCTAVE is registered in the U.S. Patent & Trademark Office.

⁷ See <http://www.cert.org/archive/pdf/04tn004.pdf> for more information.

⁸ Version 4.5.2 has been used for development and later versions should also work properly. Preliminary tests show that Version 5.5.1 also works after first converting the virtual machines provided as part of the Supplemental Lab Materials.

⁹ See <http://www.vmware.com/> for more information.

¹⁰ See "Survivability and Information Assurance Curriculum Lab Overview" (http://www.cert.org/sia/Lab_Overview.pdf) and all of the Guided Tours provided with the SIA Curriculum materials.

¹¹ See the report entitled "The Design and Operation of the Lab for the 'Sustaining, Improving, and Building Survivable Functional Units (SFUs)' Course in the SIA Curriculum.

defender. It is a practical and realistic curriculum that layers skills training on a firm educational foundation. This section describes some of the characteristics for students to be successful when taking the courses in the curriculum and instructors to be successful when teaching these courses.

A. Students

Much of the focus of this curriculum involves approaching information technology and system administration within the organization as a support function, allowing the business to operate more effectively and efficiently. This requires a student who is willing and able to approach IT and system administration from a business perspective—not simply from a technology perspective.

For students who have been administrators for a while, this may be a difficult task because many administrators consider the information technology assets of an organization independent of the organization's mission. A student who is willing and able to embrace this new perspective and see the information infrastructure as an enabler of the business mission will have a good chance to succeed in this curriculum.

This curriculum is new and different than anything currently being taught at higher-education institutions. As with any new course(s), there will be unforeseen challenges in the delivery of the materials. Students who are inflexible in their approach to the educational environment and who demand that information exchange in a classroom setting be only one way (instructor to student) may be faced with frustrations in this curriculum.

On the other hand, students who are willing to be actively involved in their own learning and are willing to accept new challenges and overcome them in a partnership with the instructor will be rewarded with the materials included in this curriculum. They are likely to be among the more successful systems administrators in tomorrow's businesses.

B. Instructors

To be successful in delivering the SIA Curriculum, instructors should have experience as a system or network administrator or as a manager of system or network administrators. Instructors need to be able to relate real-life experiences to the students by describing the fundamental benefits of following the tenets of the SIA Curriculum and the pitfalls inherent in ignoring them.

Because the focus of much of the curriculum is on determining the information assurance needs of the organization and then making information technology decisions based on these needs, it is imperative that an

instructor understand 'business needs.' An instructor who does not understand how information technology supports the business may lack the vision needed to properly put information assurance in perspective within the organization. Instructors without this vision may focus so much on the information assets that the needs of the business are lost. An instructor who believes IT exists independent of the business and the mission will undermine many of the key points in this curriculum.

All demonstrations, guided tours, and exercises are done using Red Hat LINUX Version 9 as the technological base in the reference implementation. There may be times when troubleshooting is required. This troubleshooting may be impossible unless the instructor has used some version of LINUX.

To be successful in teaching this curriculum, instructors

- should believe and be able to communicate to students the need to keep business mission in focus while tending to the technology that supports it. An instructor's ability to recognize the proper place for technology in a business is a plus;
- must recognize that the tasks of a first defender extend beyond directing the actions of a computer system and network infrastructure component from their keyboards;
- should be able to allay student concerns by pointing out that the principles of the SIA Curriculum increase their value to the business and set them apart from their peers;
- must be comfortable with teaching at both the conceptual level that the educational foundation demands and the detailed technical level that skills training requires.

VIII. CONTENTS

The SIA Curriculum consists of two distinct entities: the courseware and the lab supplemental materials.

A. SIA Curriculum Courseware

The courseware consists of all of the files and folders for the following. For each, Microsoft Word, PowerPoint, PDF, and other ancillary (e.g., graphics) files are also provided.

- Instructor and Student workbook
- Demonstrations, Guided Tours, Exercises, Quizzes, and Exams
- Course supplemental materials (e.g., Policy Workbook and OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) materials)

- Guided Tours and designs for building the lab
- All other overviews, courseware contents files, background, and other explanatory information

The SIA Curriculum contains many references to articles, reports, specific software packages, and specific data files used in exercises and guided tours. All are included by reference only and none are included in the courseware.

B. SIA Curriculum Supplemental Lab Materials

The supplemental lab materials contain VMware-based virtual computer systems and configuration files that are to be installed in the lab in support of the lab component for a course. These files are documented in Guided Tours and design documents that are provided for the lab component for a particular course.

IX. PACKAGING AND AVAILABILITY

The SIA Curriculum is packaged into two distinct sets. These are:

- The General Materials – This set consists of Adobe Acrobat PDF versions of all student materials (workbooks, demonstrations, guided tours, supplemental materials, guided tours and lab design and overview reports and the curriculum-wide materials). These materials are password protected so that they may only be read and printed. They are available to all who accept the licensing agreement (http://www.cert.org/sia/agreement_s.html) and complete the required form (<http://www.cert.org/sia/download/general.html>). Materials are packaged by module, by course, and as an ISO-9660 image containing all files. This image fits on a CD-ROM.
- The Faculty Materials – This set consists of all courseware and supplemental lab materials. These are available to qualified faculty who accept the licensing agreement (http://www.cert.org/sia/agreement_f.html) and complete the required form (<http://www.cert.org/sia/download/faculty.html>) which is validated by Software Engineering Institute personnel. Materials are packaged by module, by course, and as two ISO-9660 images containing all courseware and supplemental lab materials files. Each image is a DVD.

X. SUMMARY

The SIA Curriculum's goal is to provide a basis to educate experienced first defenders about the principles of survivability and information assurance. Students first apply them to a critical view of the TCP/IP protocols. They then apply these principles to the task of sustaining and improving the functionality of an enterprise network built in the institution's SIA Curriculum lab. Time permitting, students design, build, and integrate a new Survivable Functional Unit into that network. This enterprise network is practical, realistic, and appropriately constrained by policy, procedures, and risk management philosophies where the emphasis is on supporting the mission of the enterprise.

Combining education and training is an important part of creating successful first defenders because technology is dynamic but skills-training is not. First defenders who grasp the fundamental issues facing them can continue to be successful even as workplace technology changes. By balancing the enterprise mission and the technology that enables it, first defenders who are able to change their way of thinking can increase their value to the enterprise and make the enterprise network better able to survive in today's and tomorrow's increasingly Internet-oriented world.

The SIA Curriculum is practical, appropriately constrained, and business-oriented. It creates a firm educational foundation upon which skills training can be layered. But it goes beyond the walls of educational institutions because it contains something for all first defenders concerned with survivability and information assurance. We believe the SIA Curriculum to be unique in the marketplace of survivability and information assurance educational materials.

