Survivability and Information Assurance Curriculum Overview

Survivability and Information Assurance (SIA) Curriculum Development Team
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

Introduction

Today's professional system administrators are increasingly challenged to make computer and network security a greater part of their already overflowing set of daily activities. Current workload demands can result in insufficient attention being paid to security issues and concerns, a situation that usually continues until their organization is the victim of an intrusion. After such an event, security receives an inordinate and undeserved level of attention that slowly declines over time to a level higher than previously, but still less than required. These peaks and valleys continue with each new security event until an organization integrates security into standard business processes.

System administrators can be more effective in securing 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, thereby fulfilling their job responsibilities.

The Survivability and Information Assurance (SIA) Curriculum is designed to teach experienced system administrators about security as well as a means for integrating security into their routine tasks. The intent is to avoid most of the aforementioned peaks and valleys, producing a more secure operational state. This means that the appropriate security practices, procedures, and skills should be implemented sooner rather than later, and in a more predictable fashion.

The concepts and philosophies described in the SIA Curriculum are old in some ways and new in others. For example, many traditional tasks that system administrators have done for years now have names and an ordering as prescribed by the Security Knowledge in Practice (SKiP)[1] method of system administration—the tasks are old while the ordering is new thinking. Similarly, system administrators may have been aware of policies and procedures but their recognition and use as constraints governing future actions represents new thinking. Finally, the direct connection between hardware and software technology and the mission of the enterprise is another example of new thinking.

System administrators who change their thinking from the traditional—where system administrators were kings and queens who made computer systems and network infrastructure components "dance" to their own songs—to the modern—where system administrators make computer systems and network infrastructure components dance to the organization's tune and survive in today's world—will be among the most successful and in high demand. The principles described and repeatedly applied throughout the SIA Curriculum are what system administrators need to achieve that level of success. Their knowledge of these principles and their ability to

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

[1] 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."

apply them in an enterprise sets them apart from their technologically proficient and business un-savvy counterparts.

Target Audience

While the material in this curriculum does not necessarily assume that a student has a mastery of 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. 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.

Administrators who provide management oversight of a system administrative function and who have a technical orientation can also benefit from the first course in the curriculum, even if they lack the necessary technical knowledge or interest in the remaining courses. This first course is also intended for the immediate managers of the system administrators who are enrolled in the SIA Curriculum. It is important for those managers to understand the SIA principles so they can better understand and manage the system administrators working for them.

SIA Curriculum Technology

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 9[2] as the base representative technology for the following reasons:

- It is stable.
- It is free and can be downloaded over the Internet.
- It is not feature-heavy.
- It contains all of the attributes needed to illustrate the concepts throughout the curriculum.

Red Hat LINUX Version 9 has all of the features necessary for students to apply the principles in a straightforward way, at a cost that is intended to be practical for an institution without being a financial or technological burden. 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.

The technology used in the SIA Curriculum is not the point of the curriculum. Rather the principles and their application to an arbitrary technology is the point–technology merely enables these principles to be applied. In support of this, the curriculum contains a one semester hour lab

[2] See http://www.redhat.com/ for more information.

component in the first course, "Principles of Survivability and Information Assurance," that shows and explains to students how to use Red Hat LINUX Version 9 and other key applications. This lab component helps instructors and students gain the skills needed to be successful in the SIA Curriculum.

The SIA Curriculum – A Reference Implementation

The SIA Curriculum is provided as a reference implementation that is meant to be adapted and adopted by educational institutions to suit their needs. 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.

It is also right, appropriate, and expected that some institutions will choose to substitute a different technological base for the Red Hat LINUX Version 9 base provided in this reference implementation. It is important for institutions to realize that we believe that Red Hat LINUX Version 9 has most, if not all, of the features needed to demonstrate the concepts and principles described throughout the curriculum. Any technological base substitution needs to address these concepts and 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 system administrator to be aware of and to try to do, even if the operating system of choice does not allow it or makes it difficult.

While not available in October 2005, we envision a future means by which these changes in support of an institution’s adaptation and adoption requirements will be able to be shared with the wider SIA Curriculum community. Institutions that make changes to this reference implementation are strongly encouraged to share where possible. Our mission is to apply the principles’ concepts to the technology—not the reverse.

SIA Curriculum Courses

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)

In addition, as previously noted there is a companion lab that is intended to be taught at the same time as the "Principles of Survivability and Information Assurance" course. It is designed to prepare students for the tasks they will undertake in each of these three courses. For the student who is already proficient in the technology used in this curriculum, specifically Red Hat LINUX Version 9 in the reference implementation, this companion lab component serves as a baseline or refresher for the skills they already have.

Course Structure

Each of the courses in the SIA Curriculum is broken into modules and modules are further broken into topics. Each topic contains instructor information designed to help map them into 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.
- 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. Answers, either specific or general as appropriate, are provided in the reference implementation.
- 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.
- 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.

All of these items are visually distinguished in the courseware provided in the SIA Curriculum (see the section entitled “SIA Curriculum Courseware” on page 9). The specific characteristics of these representations are compatible with both color and black-and-white printing.

Course 1 – Principles of Survivability and Information Assurance

"Principles of Survivability and Information Assurance" is the first course in the SIA Curriculum. It presents the ten principles of survivability and information assurance[3] in detail. These ten

[3] See http://www.cert.org/info_assurance/principles.html for more information.

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 system administrators 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 system administrators 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 system administrator can see and their available solutions.

It is a change in mindset for today's system administrators to dig down deeply in search of the root issues and then step back to apply technology. It is also a change in mindset for their managers to allow system administrators 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.

The "Principles of Survivability and Information Assurance" course is intended for system administrators and their immediate managers.

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 system administrators 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.

These days, 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.

® Windows is a registered trademark of Microsoft Corporation. See http://www.microsoft.com/ for more information.

Course 2 – Information Assurance Networking Fundamentals

The second course in the SIA Curriculum, entitled "Information Assurance Networking Fundamentals", applies the ten principles described and explained in "Principles of Survivability and Information Assurance" to the concepts and an implementation of TCP/IP networking. This course 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*[4]. 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 is a fine line between creating educated system administrators and building hackers. A good system administrator can think like a hacker but not act like one. Thinking like a hacker causes them to dig deeper and really challenge assumptions about networking features rather than simply accepting a feature for how it appears. This is the direction where students are led in this course.

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 is essential to the successful teaching of "Information Assurance Networking Fundamentals".

This course is intended for system administrators. 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.

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

The "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" course completes the SIA Curriculum. It places students in a setting they will likely encounter during their information technology (IT) careers.

In this setting, 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 Evaluation (OCTAVE®) method, and adding a new Survivable Functional Unit (SFU)[5] 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

[4] See http://www.kohala.com/start/tcpipiv1.html for more information.

[5] See http://www.cert.org/archive/pdf/04tn004.pdf for more information.

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)". This course is intended for system administrators.

The SIA Curriculum 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 version 4.5.2 for Linux which is available from VMware, Inc[6].

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.

Specifically, 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 report[7], and the lab supplemental materials. No additional hardware, software, or configuration information beyond that identified, described, and demonstrated in these documents is needed.

For the "Sustaining, Improving, and Building Survivable Functional Units (SFUs)" course however, the lab requires an implementation that at this point is only a design[8]. 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.

Characteristics of Success

The SIA Curriculum is a practical and realistic curriculum that layers skills training on a firm educational foundation. It represents new ideas and new approaches to many of the traditional tasks of the system administrator. 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.

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

[6] See http://www.vmware.com/ for more information.
[7] See "Survivability and Information Assurance Curriculum Lab Overview" and all of the Guided Tours provided with the SIA Curriculum materials.
[8] 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."

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.

In contrast, 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.

Instructors

Instructors responsible for delivering the SIA Curriculum content should have had experience in an organization as a system or network administrator (or the manager of system or network administrators). There is clearly a need for the instructor 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 must be comfortable with teaching at both the conceptual level that the educational foundation demands and the detailed technical level that skills training requires;
- instructors should believe in 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;
- instructors must recognize that the tasks of a system administrator extend beyond directing the actions of a computer system and network infrastructure component from their keyboards;
- instructors 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.

SIA Curriculum Packaging

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

SIA Curriculum Courseware

The courseware consists of all of the files and folders for the following:

- Instructor workbook – Word, PowerPoint, PDF, and any other ancillary (e.g., graphics) files
- Student workbook – Word, PowerPoint, PDF, and any other ancillary (e.g., graphics) files
- Demonstrations, Guided Tours, Exercises, Quizzes, and Exams – Word, PowerPoint, PDF, and any other ancillary (e.g., graphics) files
- Course supplemental materials (e.g., Policy Workbook and OCTAVE materials – Word, PowerPoint, PDF, and any other ancillary (e.g., graphics) files
- Guided Tours and designs for building the lab – Word, PowerPoint, PDF, and any other ancillary (e.g., graphics) files needed to build the lab for each course in the curriculum
- All other overviews, courseware contents files, background, and other explanatory information – Word, PowerPoint, PDF, text, and any other ancillary (e.g., graphics) files

Throughout the modules and supporting documentation in the SIA Curriculum, there are references to articles, reports, specific software packages, and specific data files used in exercises and guided tours. They are also summarized in a URL reference sheet provided for retrieval as needed. None of these articles, reports, specific software packages, and specific data files are included in the courseware.

SIA Curriculum Supplemental Lab Materials

The supplemental lab materials contain 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.

Summary

The goal of the SIA Curriculum is to educate experienced system and network administrators about the principles of survivability and information assurance and to first apply them to a critical view of the TCP/IP protocols. Students then apply all of this knowledge and skill by sustaining and improving the functionality of an enterprise network built in the institution's SIA Curriculum lab. 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.

The combination of education and training is important because technology is dynamic but skills-training is not. System administrators 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, system administrators 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.