The CERT® Survivability and Information Assurance Curriculum

Building Enterprise Networks on a Firm Educational Foundation

CERT® Training and Education
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

© CERT, CERT Coordination Center, and Carnegie Mellon are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

This material is approved for public release. Distribution is limited by the Software Engineering Institute to attendees.

© 2001-2006 Carnegie Mellon University
Topics

- The Problems
- A Solution
- The Audience
- The Courses
- The Lab
- Characteristics of Successful Students and Instructors
- Availability
- The Principles
The Problems -1

1. System administrators do not always understand what they are *really* doing.

   • Follow task recipes.
   • What happens if the technology does not work as expected or changes – do they know what to do?
   • Are you a Windows/Linux/Mac-OS system administrator or are you an system administrator who knows Windows/Linux/Mac-OS?
Training vs. Education

Teach 6-year-old about burning a finger

Fire in fireplace can burn

How about an electric clothes iron?

- If only trained
  - Child touches iron and is burned
- If educated
  - Child understand that heat burns
  - Fire in fireplace is one example
  - Electric clothes iron is another example
  - Child does not touch iron

Educated system administrators can better adapt to changing technology than their only-trained counterparts
The Problems -2

2. System administrators do not always connect enterprise computer systems and network infrastructure components with business mission.

- Equipment purchased to support business mission
- If the equipment fails, the business may also fail
- Constrained by policies, procedures, and risk analysis
- Know what their job is and what their job is not
The Problems -3

3. System administrators become unnecessarily mired in enterprise network details and miss the big picture.

- They need a scheme for reducing enterprise network complexity
- Details still important, but only when necessary
- Example: the family car
  - Features initially important
  - Changes over time
  - Becomes “can I get there from here and back again safely and reliably?”
The Problems -4

4. Most system administrators inherit an existing network, yet few are taught how to analyze, maintain, and grow that type of network.

- Often taught how to build from scratch
- But the enterprise often exists already
- Computer systems and network infrastructure components already (mis-)configured
- Computer systems and network infrastructure components may have already been attacked
- Misleading and incorrect system and network documentation is a reality
5. System administrators are too trusting of technology.

- Misplaced trust puts the enterprise at unnecessary risk.
- System administrators need to:
  - Know to question technology
  - Use a methodology for systematically asking questions and seeking answers
A Solution

The Survivability and Information Assurance (SIA) Curriculum

- 3 course, 13 semester-credit-hour curriculum (162.5 total hours)
- Addresses problems
- Educationally oriented
- Technology independent
- Complementary to training
- Realistic
- Practical
- Appropriately constrained
- Subset freely available
- Full version freely available to qualified faculty
- Licensing agreement

© 2001-2006 Carnegie Mellon University
The Audience

Community colleges
Four-year colleges and universities
Graduate schools

Experienced system and network administrators
  - Two years experience recommended

System and network administrator managers
  - 1st course lecture
  - Technically oriented

But
  - General distribution is widely applicable beyond college and universities
The Courses -1

Workbook

- General/student (G)
- Instructor/faculty (F)

Module Structure

- Required Readings (G, F)
- Recommended Readings (G, F)
- Quizzes with suggested answers (F)
- Exercises with suggested answers (F)
- Recommended Exercises with suggested answers (F)
- Guided Tours (G, F)
- Demonstrations (G, F)
- Exams with suggested answers (F)
- Supplemental materials (G, F)
The Courses -2

**Principles of Survivability and Information Assurance**
- 3 semester-hour course (lecture) – SAs and SA Managers
- 1 semester-hour lab – SAs
- 10 principles

**Information Assurance Networking Fundamentals**
- 4 semester-hour course (lecture and labs)
- Applies 10 Principles to TCP/IP
- Steven’s *TCP/IP Illustrated, Volume 1 – The Protocols*

**Sustaining, Improving, and Building Survivable Functional Units (SFUs)**
- 5 semester-hour (lecture and lab)
- Inherit existing enterprise network
- Applies 10 principles to sustain and improve enterprise network
- Applies 10 principles to add new SFU to enterprise network
The Lab

Isolated network
- 14 student workstations (minimum)
- 1 instructor workstation
- 1 or more printers

Red Hat LINUX Version 9

VMware virtual guest computer systems

Guests provided for Principles and Networking

No guests for Sustaining (design documents only)

Extensive documentation for all (Guided Tours)

Instructor/Faculty DVD image
Characteristics of Successful Students and Instructors

Students
- Adopt a new way of thinking
- Flexibility
- Seek knowledge beyond technical training

Instructors
- System administrator experience
- Understand ‘business needs’
- Teaching at conceptual and technical levels
- Able to keep business mission concept in focus
- System administrator's job extends beyond technical aspects
Availability

SIA is free (must accept terms of license agreement)

Faculty/Instructor version

- Qualified faculty
- All files (Word, PowerPoint, PDF, Image files, etc)
- By module, by course, and entire curriculum
- 2 DVD set (Courseware and Lab Supplemental Materials)

General/Student version

- Available to all
- PDF files only (printing and viewing)
- By module, by course, and entire curriculum
- 1 CDROM (Courseware)

Available now! http://www.cert.org/sia
How to Use the SIA Curriculum

As is (the clothes rack by itself)

- Ready as is
- Complete lab for Sustaining not yet developed
- Instructor versions tightly controlled

“Hang” your existing courseware on the SIA clothes rack

- Integrate your courses into an expanded SIA Curriculum
- Expand SIA 3 courses into …
- Principles is the basis

Adapt and adopt

Change technology base

Share with SIA Curriculum Community
Principles

10 Principles in 10 minutes

Drill down Principle 9

- How explained in *Principles*
- How applied in *Networking*
- How used in *Sustaining*
Principle 1

Survivability is an enterprise-wide concern.

http://www.cert.org/nav/index_purple.html
Principle 2

Everything is data.

http://www.cert.org/homeusers/piglatin.html
Principle 3

Not all data is of equal value to an enterprise – risk must be managed.

http://www.cert.org/octave/
Principle 4

Information assurance policy governs actions
Principle 5

Identification of users, computer systems, and network infrastructure components is critical.
Survivable Functional Units (SFUs) are a helpful way to think about an enterprise’s networks.

http://www.cert.org/archive/pdf/04tn004.pdf
Security Knowledge in Practice (SKiP) provides a structured approach.

Principle 8

Technology Roadmap

The road map guides implementation choices (all technology is not equal)
Challenge assumptions to understand risk
Principle 10

Communication skill is critical to reach all constituencies.
Drill Down Principle 9

**Principles**
- Explain the principle
- Give non-computer-based explanation
- Give computer-based explanation

**Networking**
- Apply the principle to TCP/IP
- Example: ARP

**Sustaining**
- Apply to the enterprise
- Example
  - Discover web traffic
  - Check host process service
  - Verify package and configuration files are installed
Does this product satisfy my doctor and can it be trusted?
Define Main Assumption

Select starting point from either
- now and go backwards in time, or
- beginning of time and go forward.
Principle 9 - Abstract the Process -2

Main Assumption

- What does it depend on?
- What assumptions does it make?

Move in the time direction, that is, forward to backward
Principle 9 - Abstract the Process -3

Next Assumption

- What does it depend on?
- What assumptions does it make?

Continue to move in the time direction, that is, forward or backward
Principle 9 - Says Who!

Imagine a web browser showing the lock on a web page. Who says that the lock represents an SSL or otherwise encrypted page?
Principle 9 - Custodian Assumptions

Chain of custody of bits, from construction to consumption
Principle 9 - Custodian Assumptions -2

Different computers, same view?
Principle 9 - Custodian Assumptions -3

Assumptions about the Internet service provider
Principle 9 – The Address Resolution Protocol (ARP)

Creates IP Address→MAC Address binding

Dynamic

Similar to Directory Assistance and Telephone Books

Guided Tour and Exercise
Principle 9 - ARP Traffic

Telephone book
- Legitimate?
- Authoritative?

ARP traffic
- Legitimate?
- Authoritative?

Guided Tour and Exercise
Network-Traffic-First Method

Assumption: Network traffic identifies all computer systems and network infrastructure components

Every packet belongs to some Functional Unit

Domain Name System (DNS) example

Other artifacts further identify functional unit attributes

Method makes few assumptions about the enterprise network
Guided Tour

Business of enterprise is serving requests for comments (RFCs) through Web.

Must be a Web Development and Delivery Functional Unit.

Identify attributes.

Use network-traffic-first method.

- Web server traffic identifies computer systems.
- Use other artifacts to define additional FU attributes.

Formally define the Web Development and Delivery Functional Unit.
Principle 9 – Network Artifact Analysis
Principle 9 – Host Artifact Analysis -1

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>root</td>
<td>1797</td>
<td>IPv4</td>
<td>2210</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2120</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2123</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2124</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2125</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2126</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2127</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>12000</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2120</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2123</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2124</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2125</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2126</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2127</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>12000</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2120</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2123</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2124</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2125</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2126</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2127</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>12000</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2120</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2123</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2124</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
<tr>
<td>apache</td>
<td>2125</td>
<td>3u</td>
<td>IPv4</td>
<td>2218</td>
<td>TCP</td>
<td>:80</td>
<td>LISTEN</td>
</tr>
</tbody>
</table>
Principle 9 – Host Artifact Analysis -2

% cd /mnt/cdrom/Hosts/By\Addr/10.1.3.1/etc/httpd/conf
% ls -l
total 48
-rw-r--r--  1 lrr  cert  34928 Feb 25 2003 httpd.conf
-rw-r--r--  1 lrr  cert 12959 Feb 25 2003 magic
%
Principles Summary
Questions?
Contact Information

Lawrence R. Rogers

- Office Phone: 412/268-8042
- E-mail: lrr@cert.org

CERT website: http://www.cert.org/

SIA website: http://www.cert.org/sia

SEI website: http://www.sei.cmu.edu/

SEI Education and Training:
http://www.sei.cmu.edu/products/courses/