



# CERT

## The CERT<sup>®</sup> Survivability and Information Assurance Curriculum

Building Enterprise Networks on a Firm Educational Foundation

CERT<sup>®</sup> 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.

# 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?

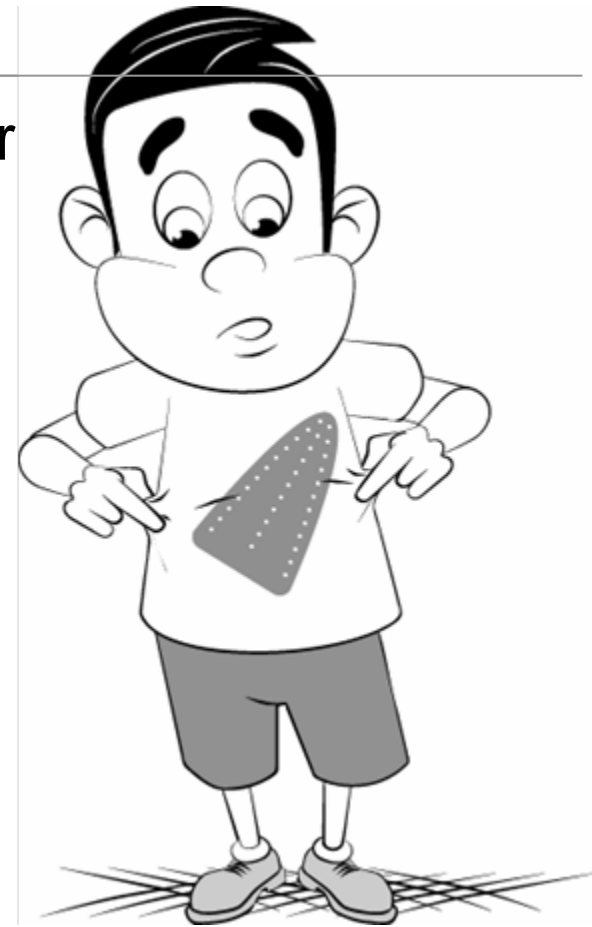
# Training vs. Education

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?”



HEY  
THERE'S A  
TEAR IN THE  
WALLPAPER!

# 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



# The Problems -5

## 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


The logo features a blue parachute with the letters 'SIA' in white. Below the parachute is a blue horizontal bar with the text 'Survivability & Information Assurance' in white. Underneath the bar is a small icon of a computer monitor and keyboard. Below the icon is the text 'The SIA Curriculum' in large, bold, black letters, followed by the subtitle 'Building Enterprise Networks on a Firm Educational Foundation' in a smaller, italicized black font. At the bottom is a blue horizontal bar with the URL 'http://www.cert.org/sia' in white. Below the URL is the CERT logo, which consists of the word 'CERT' followed by a blue diamond icon and the text 'Software Engineering Institute' in a small font.

**SIA**

Survivability & Information Assurance

**The SIA Curriculum**  
*Building Enterprise Networks on a Firm Educational Foundation*

<http://www.cert.org/sia>

CERT  Software Engineering Institute

# 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

- 1<sup>st</sup> 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

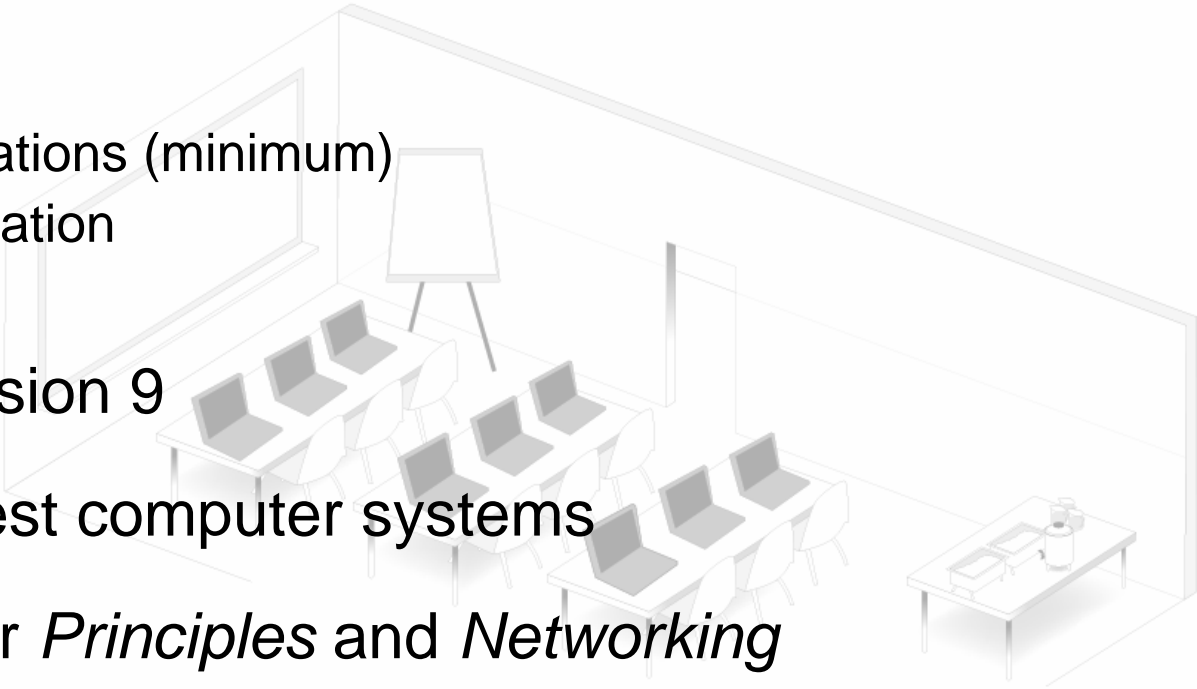
VMware virtual guest computer systems

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

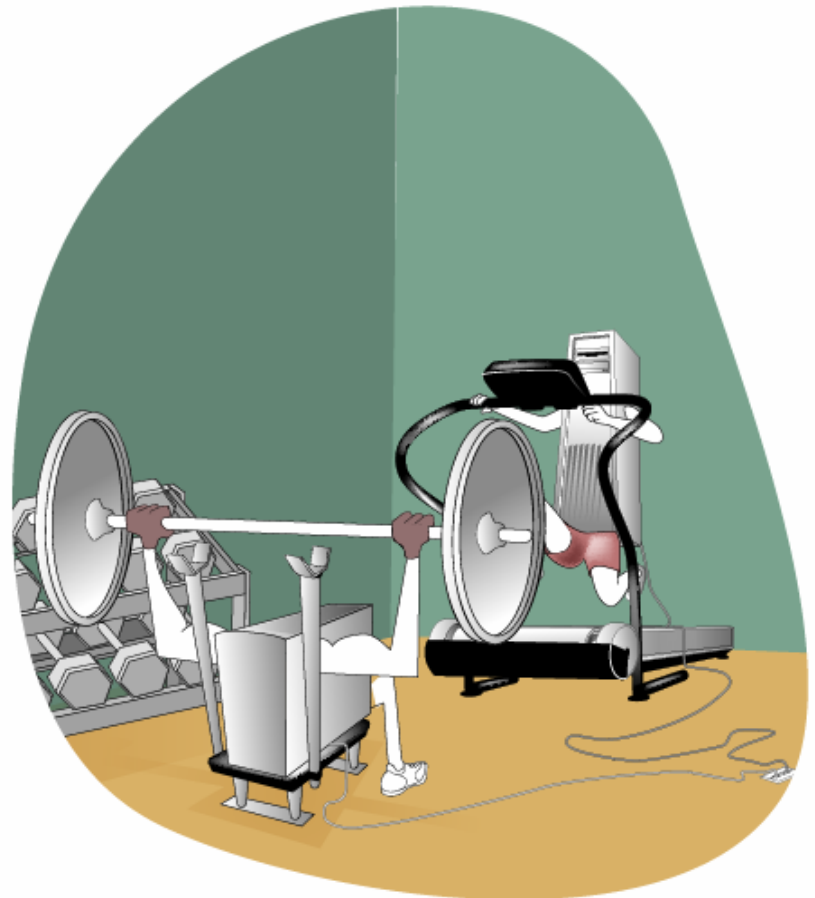
Drill down Principle 9

- 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](http://www.cert.org/nav/index_purple.html)

# Principle 2

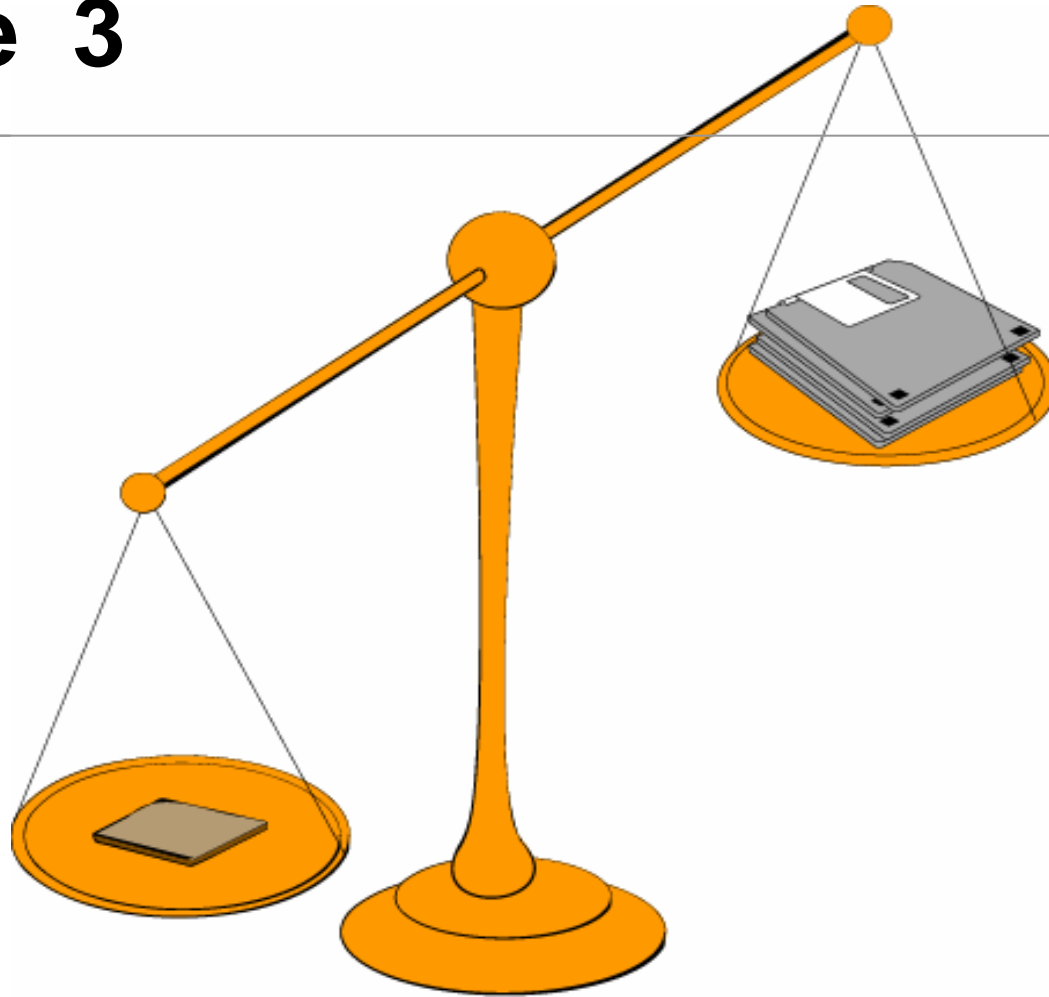


Everything is data.

<http://www.cert.org/homeusers/piglatin.html>

# Principle 3

---

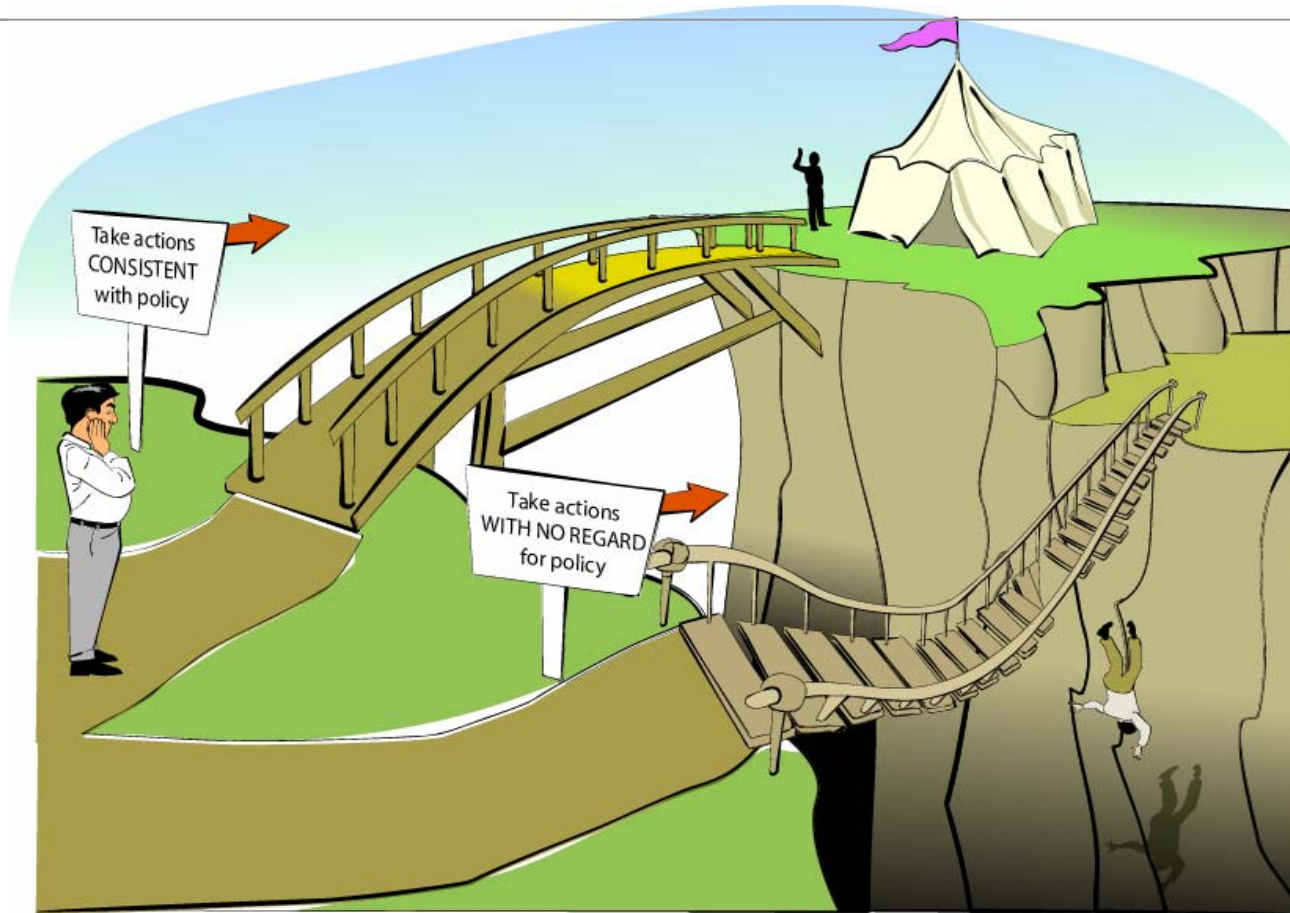


Not all data is of equal value to an enterprise – risk must be managed.

<http://www.cert.org/octave/>

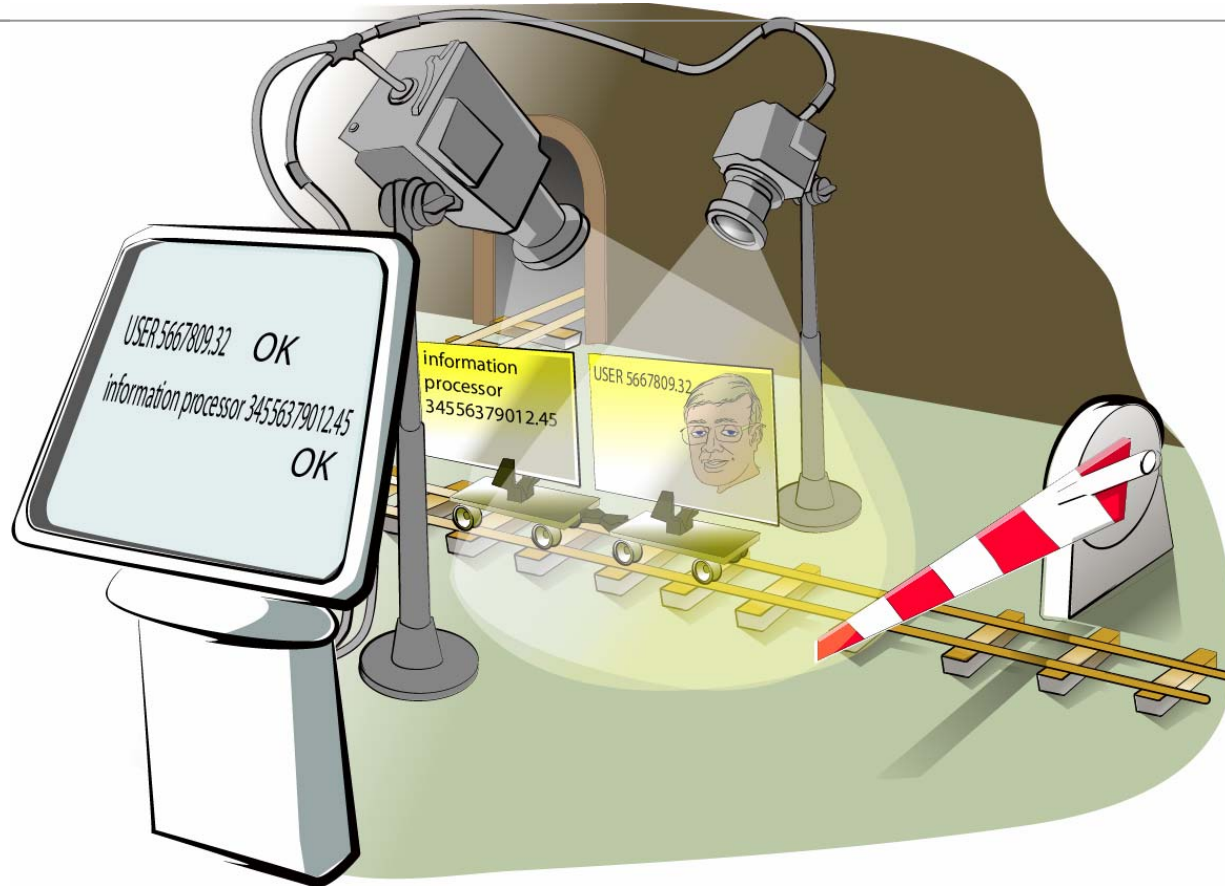


# Principle 4



Information assurance policy governs actions

# Principle 5

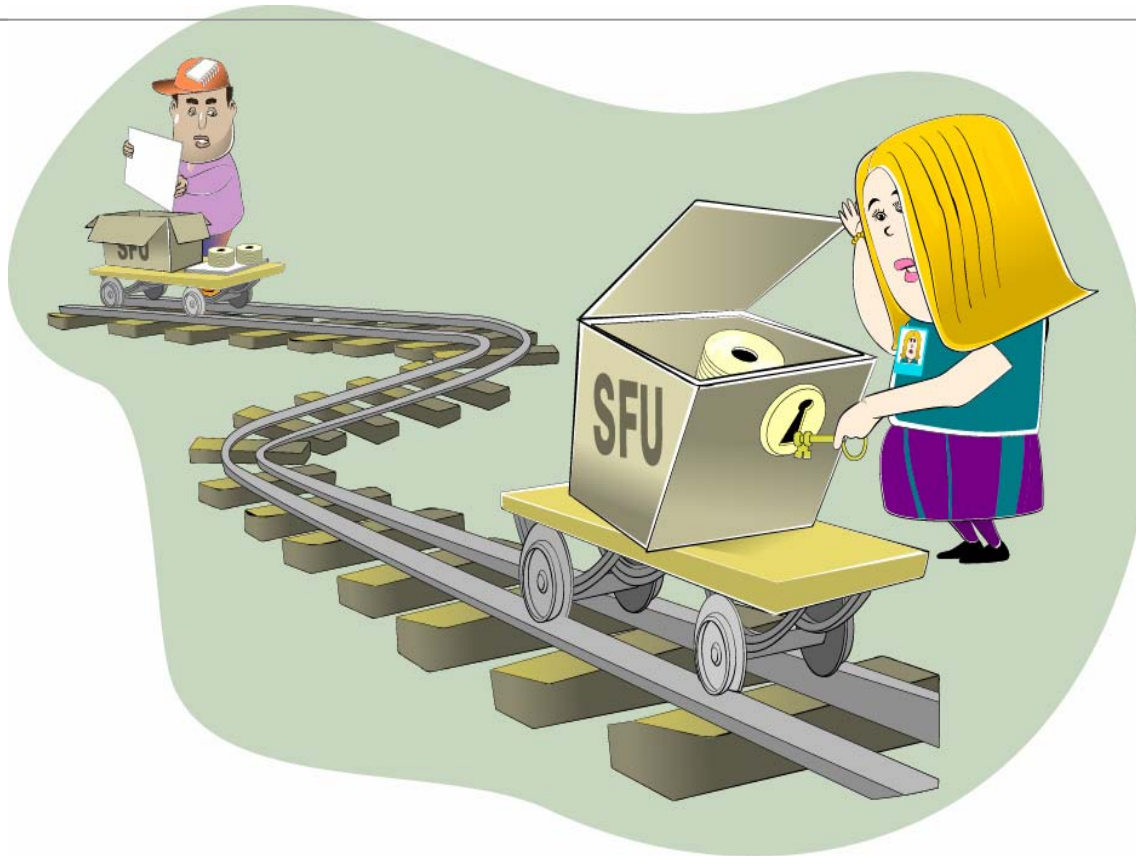


Identification of users, computer systems, and network infrastructure components is critical.



# Principle 6

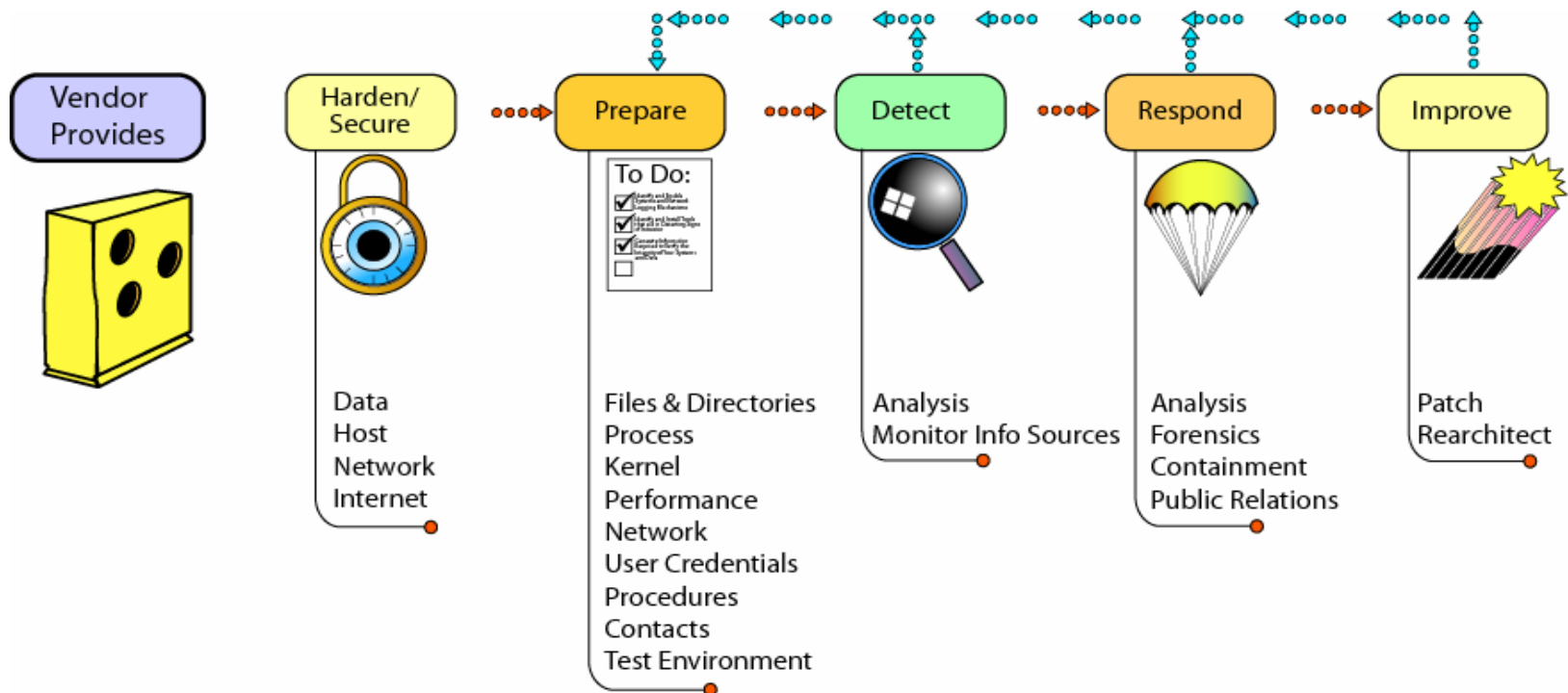
---



Survivable Functional Units (SFUs) are a helpful way to think about an enterprise's networks.

<http://www.cert.org/archive/pdf/04tn004.pdf>

# Principle 7

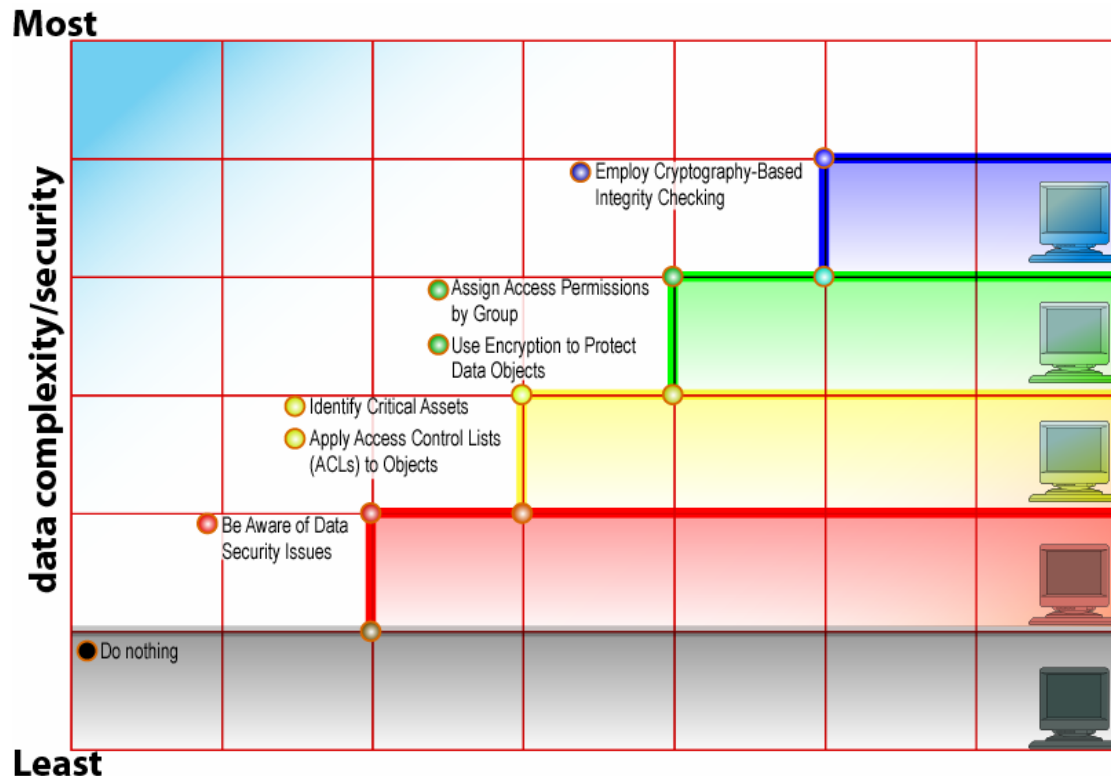


Security Knowledge in Practice (SKiP)  
provides a structured approach.

<http://www.stsc.hill.af.mil/crosstalk/2002/11/rogers.html>

# Principle 8

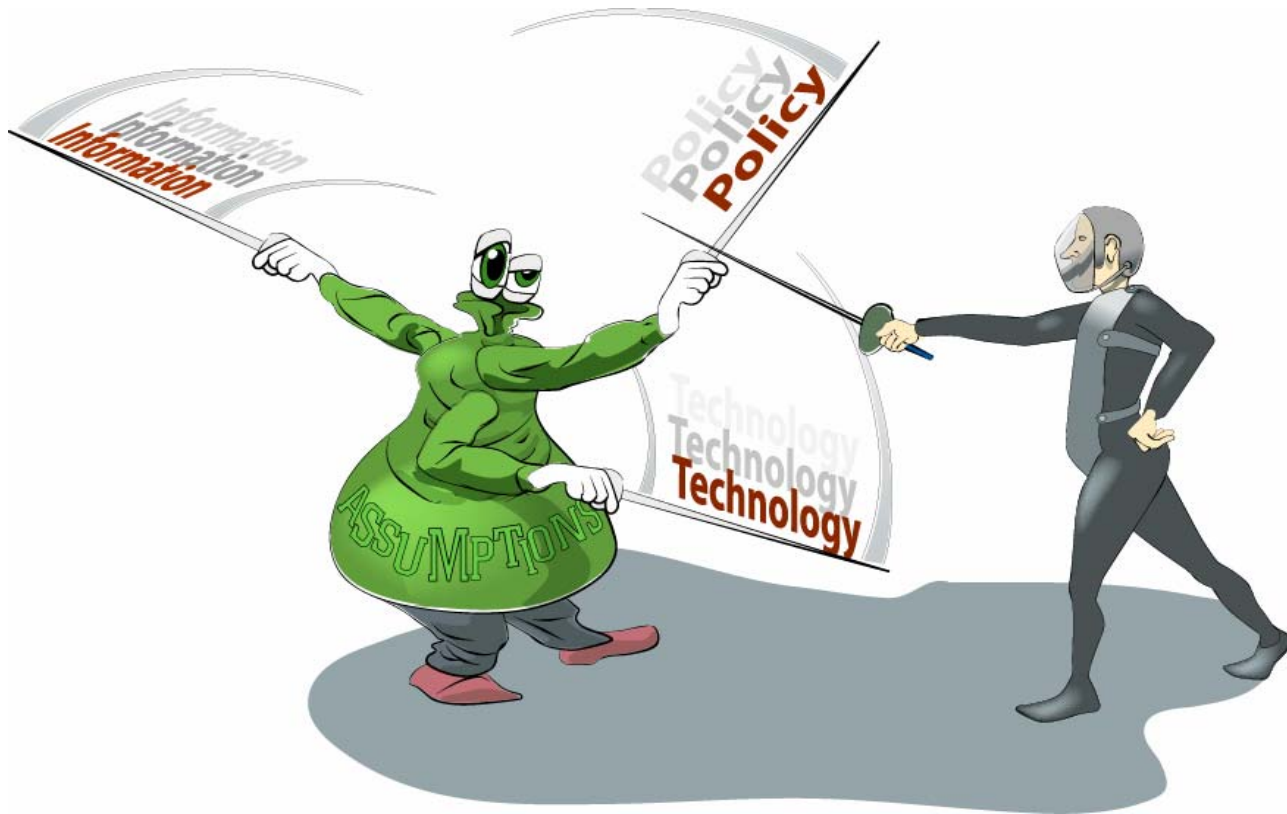
## Technology Roadmap



The road map guides implementation choices  
(all technology is not equal)

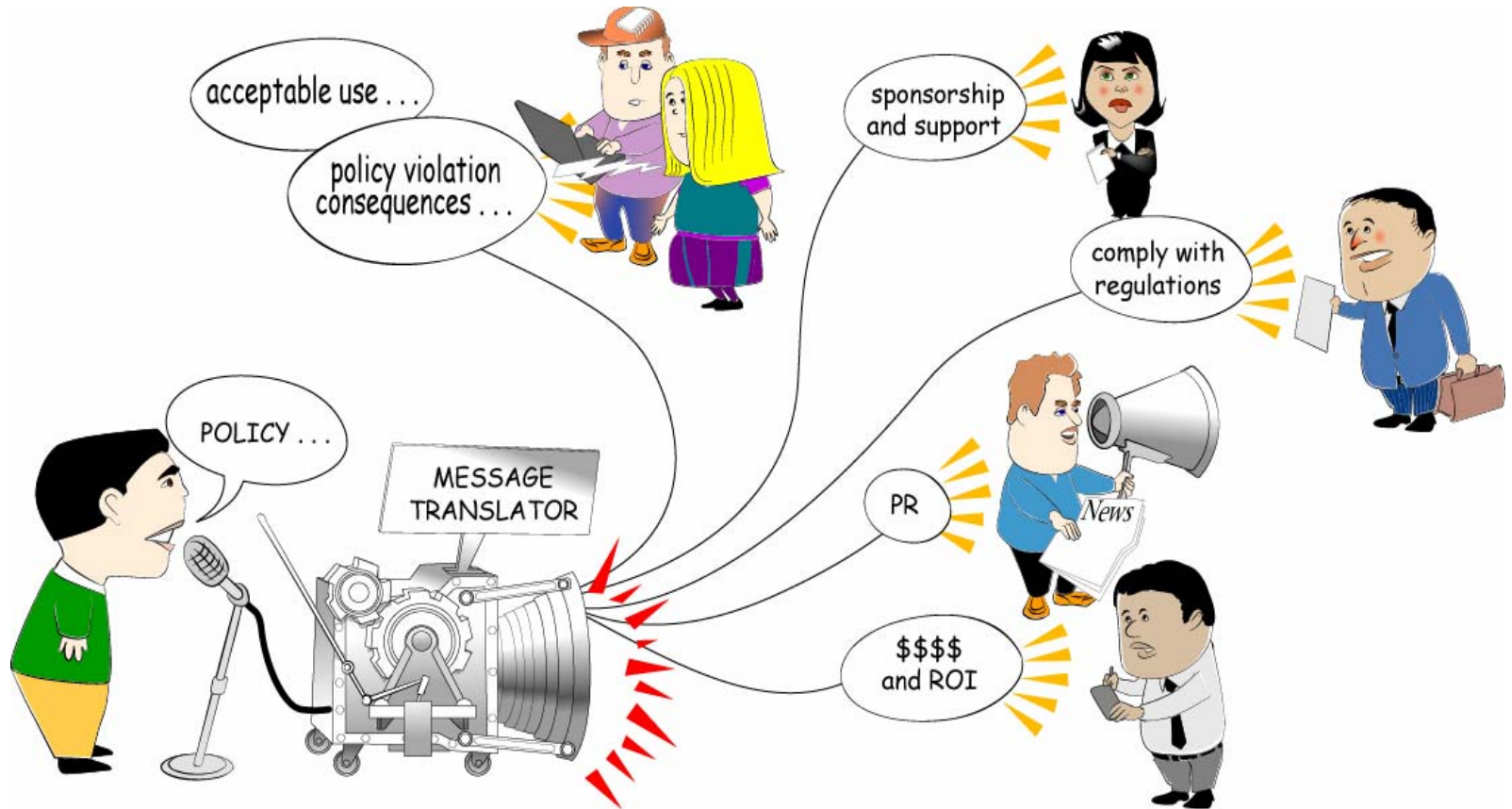
# Principle 9

---



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





# Trusting Untrustworthy Information



Does this product satisfy my doctor and can it be trusted?



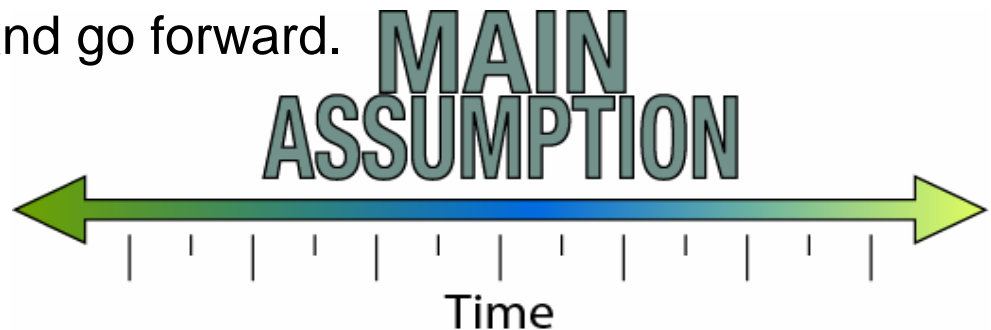
# Principle 9 - Abstract the Process -1

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?

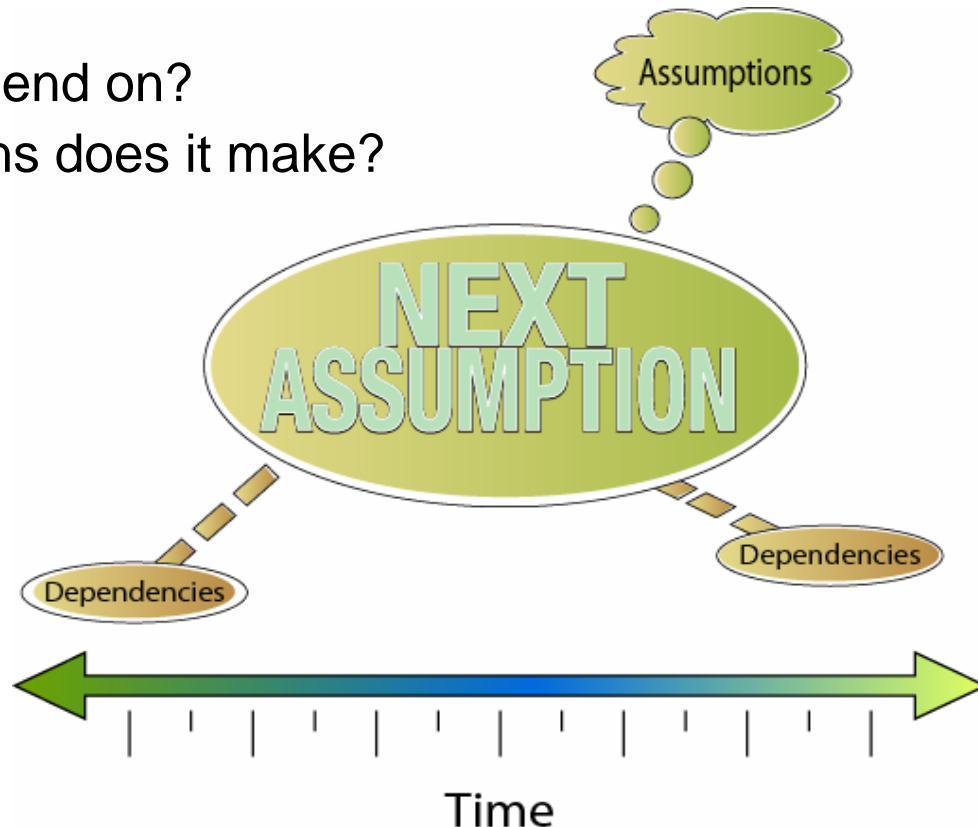


**Move in the time direction, that is, forward to backward**

# 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**

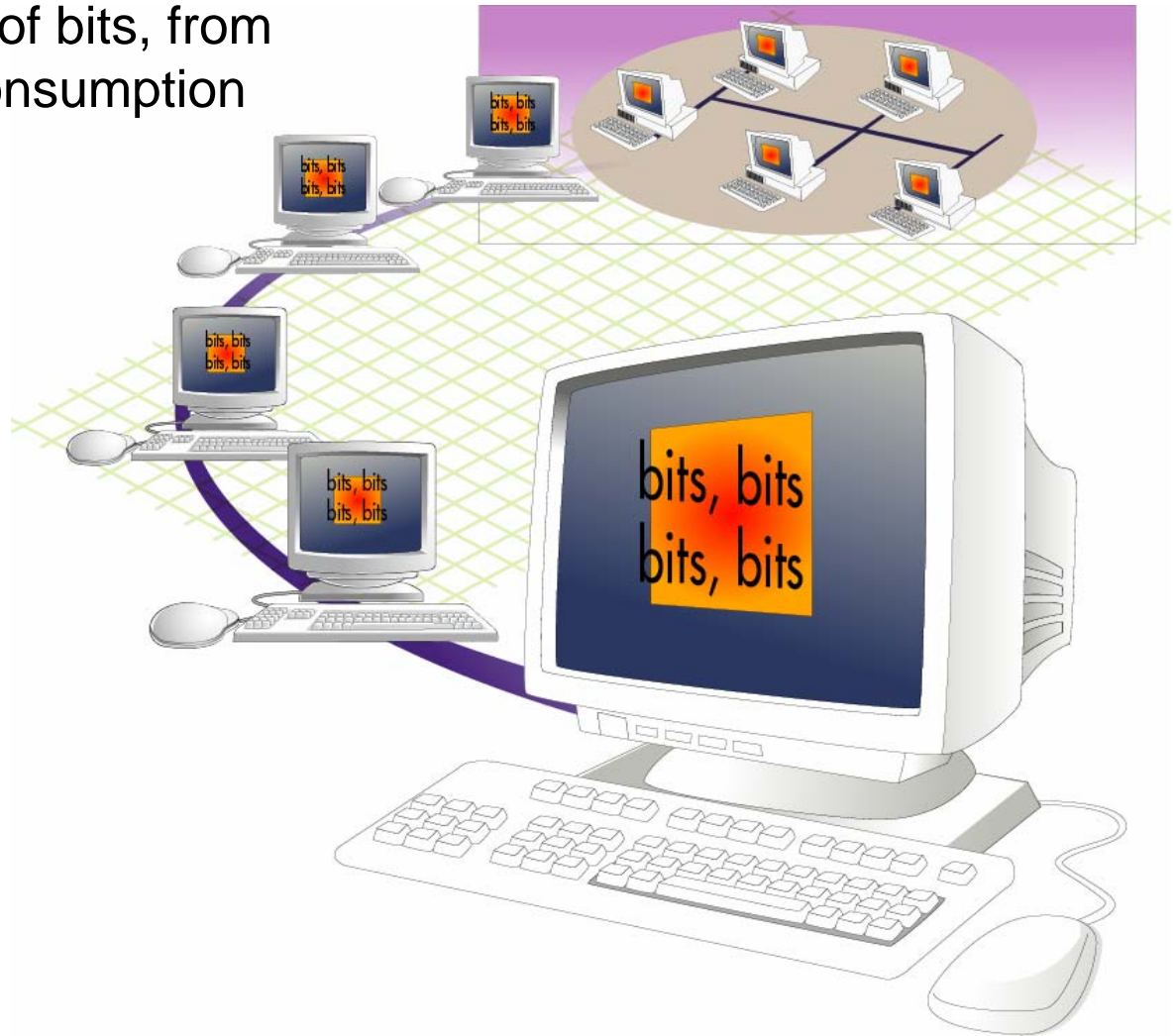
# Principle 9 - Says Who!

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 -1

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

The screenshot shows the Wireshark interface with a capture filter set to `(tcp.port == 80 || tcp.port == 443)`. The packet list pane displays 18 captured packets. Packet 1 is a SYN-ACK from 10.1.3.1 to 172.16.0.12. Packets 2-18 show a sequence of SYN, ACK, and HTTP requests/responses, including a 404 Not Found and a 200 OK response.

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.3.1	172.16.0.12	TCP	80 > 32833 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2108819 TSER=2868753
2	0.000042	10.1.3.1	172.16.0.1	TCP	80 > 32834 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2108819 TSER=2868753
3	0.000080	10.1.3.1	172.16.0.12	TCP	80 > 32835 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2108819 TSER=2868753
4	0.000698	10.1.3.1	172.16.0.12	TCP	80 > 32833 [ACK] Seq=1 Ack=147 Win=5792 Len=0 TSV=2108819 TSER=2868755
5	0.000749	10.1.3.1	172.16.0.1	TCP	80 > 32834 [ACK] Seq=1 Ack=131 Win=6432 Len=0 TSV=2108819 TSER=2868755
6	0.000787	10.1.3.1	172.16.0.12	TCP	80 > 32835 [ACK] Seq=1 Ack=145 Win=5792 Len=0 TSV=2108819 TSER=2868755
7	0.007772	10.1.3.1	172.16.0.12	HTTP	HTTP/1.1 404 Not Found (text/html)
8	0.007797	10.1.3.1	172.16.0.12	TCP	80 > 32833 [FIN, ACK] Seq=1320 Ack=147 Win=5792 Len=0 TSV=2108820 TSER=2868755
9	0.008289	10.1.3.1	172.16.0.12	TCP	80 > 32833 [ACK] Seq=1321 Ack=148 Win=5792 Len=0 TSV=2108820 TSER=2868762
10	0.010631	10.1.3.1	172.16.0.1	HTTP	HTTP/1.1 200 OK (text/html)
11	0.010777	10.1.3.1	172.16.0.1	HTTP	Continuation
12	0.011408	10.1.3.1	172.16.0.1	HTTP	Continuation
13	0.011525	10.1.3.1	172.16.0.1	HTTP	Continuation
14	0.011659	10.1.3.1	172.16.0.1	HTTP	Continuation
15	0.011803	10.1.3.1	172.16.0.1	HTTP	Continuation
16	0.011978	10.1.3.1	172.16.0.12	TCP	80 > 32836 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSV=2108820 TSER=2868766
17	0.012266	10.1.3.1	172.16.0.1	HTTP	Continuation
18	0.012388	10.1.3.1	172.16.0.1	HTTP	Continuation

Frame 1 (74 bytes on wire, 74 bytes captured)  
Ethernet II, Src: 00:0c:29:c0:25:81, Dst: 00:90:27:5a:f3:ee  
Internet Protocol, Src Addr: 10.1.3.1 (10.1.3.1), Dst Addr: 172.16.0.12 (172.16.0.12)  
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 32833 (32833), Seq: 0, Ack: 1, Len: 0

```
0000  00 90 27 5a f3 ee 00 0c 29 c0 25 81 08 00 45 00  ..'Z.... ).%...E.
0010  00 3c 00 00 40 00 3f 06 82 9e 0a 01 03 01 ac 10  .<..@.?.....
0020  00 0c 00 50 80 41 2d 61 5c 07 24 38 a0 a0 a0 12  ...P.A-a \.#8....
0030  16 a0 b5 76 00 00 02 04 05 b4 04 02 08 0a 00 20  ...v.....
0040  2d 93 00 2b c6 11 01 03 03 00  -..+.....
```

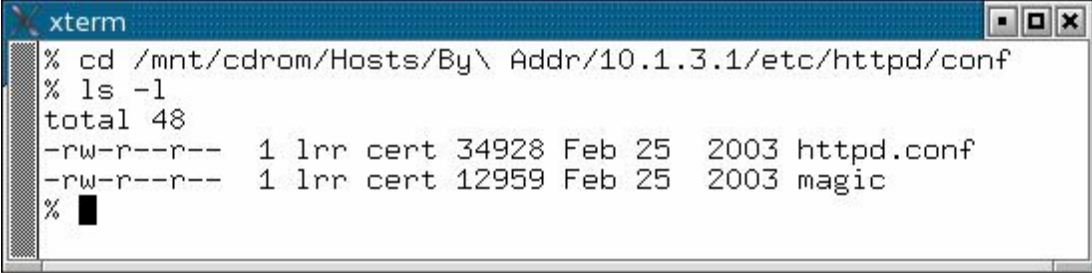
File: Capture.pcap 259 KB 00:05:31 P: 357 D: 250 M: 0

# Principle 9 – Host Artifact Analysis -1

```
xterm
% cd /mnt/cdrom/Hosts/By\ Addr/10.1.3.1/root/
% grep COMMAND lsof.txt | head -1 ; grep ':80' lsof.txt
COMMAND      PID      USER      FD  TYPE      DEVICE      SIZE      NODE NAME
httpd        1797     root       3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2120     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2121     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2122     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2123     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2124     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2125     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2126     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2127     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        12069    apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        1797     root       3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2120     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2121     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2122     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2123     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2124     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2125     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2126     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2127     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        12069    apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        1797     root       3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2120     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2121     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2122     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2123     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2124     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2125     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2126     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2127     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        12069    apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        1797     root       3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2120     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2121     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2122     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2123     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2124     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2125     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2126     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        2127     apache    3u  IPv4      2218                TCP *:80 (LISTEN)
httpd        12069    apache    3u  IPv4      2218                TCP *:80 (LISTEN)
% █
```

# Principle 9 – Host Artifact Analysis -2

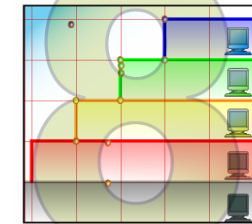
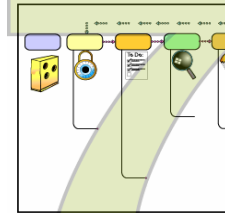
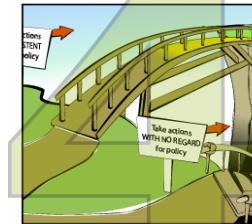
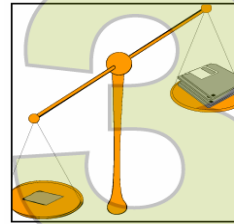
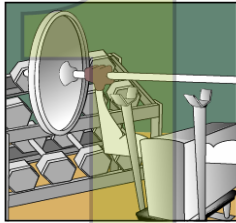
---



```
xterm
% 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](mailto: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/>