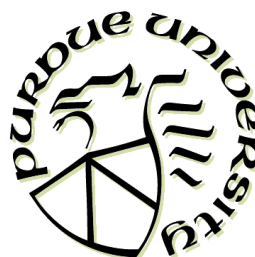


Center for Education and Research in
Information Assurance and Security

Myths, Fads and False Economies

Eugene H. Spafford
Spring 2003



<http://www.cerias.purdue.edu>



Center for Education and Research in
Information Assurance and Security

Basic Computing Infrastructure

- Experimental protocols
- Interconnection of smaller networks
- Commodity software/hardware


The Internet is a recent
phenomena. Consider.....



<http://www.cerias.purdue.edu>

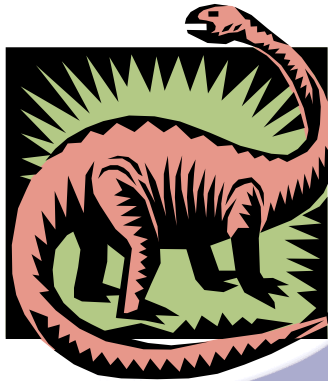
Spring 2003

2

CERIAS  Center for Education and Research in Information Assurance and Security


Looking Back: 30+ Years Ago

- No significant networks
- Mainframe computing
 - Batch, not interactive
- Computer security was physical security
- Users in the 10s of thousands
- First CS program in 1963




<http://www.cerias.purdue.edu>

Spring 2003 3

CERIAS  Center for Education and Research in Information Assurance and Security


Looking Back: ~20 Years Ago

- First Intel-based PCs
 - Apple II, Commodore Pet, others already out
- ARPAnet had 231 nodes
- Usenet created
- First computer virus about to appear
 - Apple II virus in an academic setting
- 100s of thousands of users



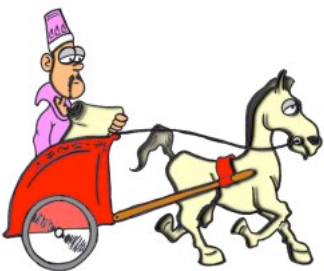
<http://www.cerias.purdue.edu>

Spring 2003 4

CERIAS  Center for Education and Research in Information Assurance and Security


Looking Back: ~15 Years Ago

- First Intel/MS computer virus ("Brain")
- Usenet had 10^5 nodes
- ARPAnet, NSFnet
- 414 gang hits the newspapers
- Cuckoo's Egg incident occurring
- Millions of users




<http://www.cerias.purdue.edu>

Spring 2003 5

CERIAS  Center for Education and Research in Information Assurance and Security


Looking Back: ~10 Years Ago

- 100s of computer viruses & worms
- WWW protocol invented
- TCP/IP has 10^6 nodes
- First security scanner (COPS)
- First general IDs (Tripwire)
- @Large incidents




<http://www.cerias.purdue.edu>

Spring 2003 6

CERIAS  Center for Education and Research in Information Assurance and Security


Looking Back: 5 Years Ago

- Commercial use of the network allowed
- 10,000+ viruses threshold reached
- First Word macro viruses (“concept”)
- First major D-O-S attack
- Initial DNS gold rush
- First root kits
- 10^7 users



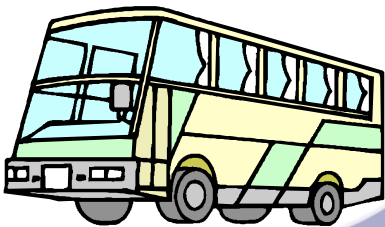
<http://www.cerias.purdue.edu>

Spring 2003 7

CERIAS  Center for Education and Research in Information Assurance and Security


The Internet Today

- Millions of systems on all 7 continents
- Perhaps 500 million users have access
- 220 countries & territories around the world have registered domains
- Online population doubling annually in much of the last decade




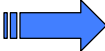

<http://www.cerias.purdue.edu>

Spring 2003 8

CERIAS  Center for Education and Research in Information Assurance and Security


Explosion of Storage

- About 200 terabytes of storage in 1995
- 2000 PCs could hold that much in 2001
 - Cost of less than \$1 million
 - Worldwide now 10 exabytes (+80% annually)
 - 2002 sales of 8500 petabytes (IDC)
- 50 PCs will hold this much in 2004

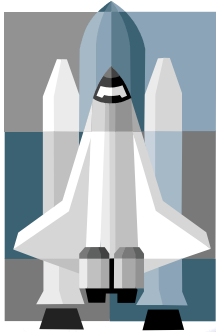
Spring 2003 9

<http://www.cerias.purdue.edu>

CERIAS  Center for Education and Research in Information Assurance and Security


Future Environment: The "Evernet"

- Cheap (free?), ubiquitous computing
- Many embedded systems connected
- High speed networking
- Widely-deployed encryption
- Truly mobile computing
- World-wide
- Billions of users
- Millions of petabytes




Spring 2003 10

<http://www.cerias.purdue.edu>

CERIAS  Center for Education and Research in Information Assurance and Security


What causes some of the security problems?

- Misunderstandings
- Crisis atmosphere
- Lack of choices
- Fads
- False economies
- Shortage of experience
- Shortage of experts



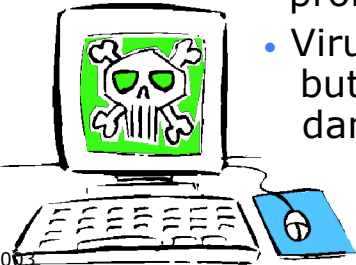
Spring 2003 11

<http://www.cerias.purdue.edu>

CERIAS  Center for Education and Research in Information Assurance and Security


Malware

- Antivirus software will protect my system
- I'll be safe if I don't open email from people I'd don't know
- Every system has the same virus problems
- Viruses are a nuisance but don't really cause damage



Spring 2003 12

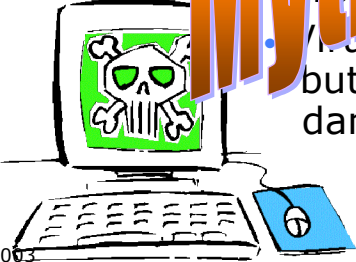
<http://www.cerias.purdue.edu>

CERIAS  Center for Education and Research in Information Assurance and Security

Malware


- Antivirus software will protect my system
- I'll be safe if I don't open email from people I'd never heard of
- Every system is susceptible to some virus
- Viruses are a nuisance but don't really cause damage

Myths!

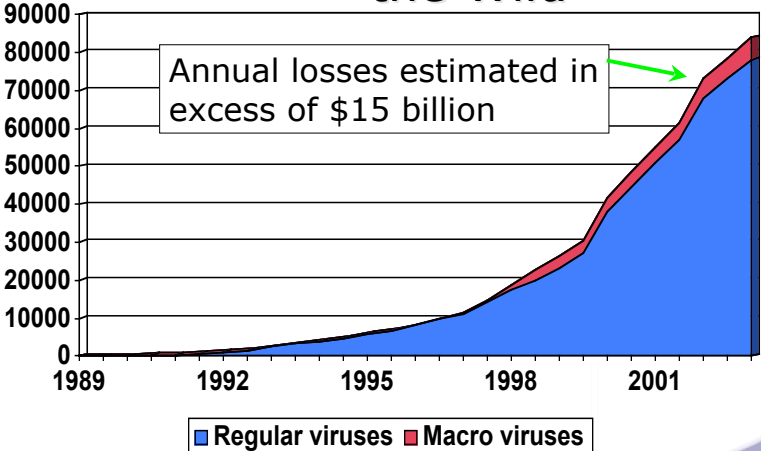


Spring 2003 13

<http://www.cerias.purdue.edu>

CERIAS  Center for Education and Research in Information Assurance and Security

Growth of Viruses "In the Wild"




Year	Regular viruses	Macro viruses	Total
1989	0	0	0
1992	~1,000	0	~1,000
1995	~5,000	0	~5,000
1998	~15,000	~5,000	~20,000
2001	~70,000	~15,000	~85,000


Annual losses estimated in excess of \$15 billion

Spring 2003 14

<http://www.cerias.purdue.edu>



CERIAS

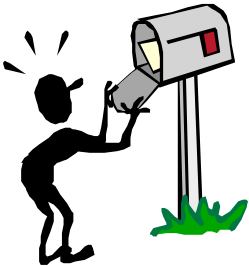


Center for Education and Research in
Information Assurance and Security

Real losses

- Melissa, March 1999
 - Word 97, Word 2000
 - \$300 million in damages
 - Approximately 4 days, 150,000 systems
- ILOVEYOU, May 2000
 - Outlook
 - As much as \$10 billion in damages
 - Approximately 24 hours, > 500,000 systems
- Code Red I, Nimda
 - IIS flaws, with fixes published months earlier
 - 400,000 systems in 14 hours, several billion in damages


("Brain" took 5 years to do \$50 million)




http://www.cerias.purdue.edu

Spring 2003

15




CERIAS



Center for Education and Research in
Information Assurance and Security

Encryption


- To be secure, I need 4096 bit keys
- If only everyone used encryption, we'd all be safe
- If my browser connection (SSL) is encrypted, my information is safe




http://www.cerias.purdue.edu

Spring 2003

16



CERIAS




Center for Education and Research in
Information Assurance and Security

Encryption


- To be secure, I need 4096 bit keys
- If only everyone used encryption, we'd all be safe
- If my browser's connection (SSL) is encrypted, my information is safe

Myths!




<http://www.cerias.purdue.edu>

Spring 2003 17




CERIAS



Center for Education and Research in
Information Assurance and Security

Reality


- For most applications, 128-bit symmetric keys are fine
 - Brute force attack would involve 10^8 - 10^{12} years
- Security involves
 - Confidentiality
 - But also integrity, availability, accountability, and more



“Using an armored truck to transport rolls of pennies between someone on a park bench and someone doing business from a cardboard box.”


<http://www.cerias.purdue.edu>

Spring 2003 18

CERIAS  Center for Education and Research in Information Assurance and Security


Vulnerability

- I have nothing on my system — no one will want to break into it
- I never download anything, so I'm safe
- I'm only connected to the network a few hours a day, so I'm okay



http://www.cerias.purdue.edu


Spring 2003 19

CERIAS  Center for Education and Research in Information Assurance and Security

Vulnerability


- I have nothing on my system — no one will want to break into it
- I never download anything, so I'm safe
- I'm only connected to the network a few hours a day, so I'm okay

Myths!




http://www.cerias.purdue.edu

Spring 2003 20



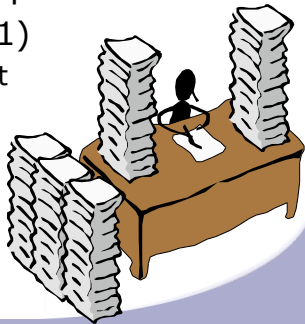
CERIAS



**Center for Education and Research in
Information Assurance and Security**

Everyone is at risk


- CERT/CC fielded 82,094 incidents in 2002
 - 52,658 incidents in 2001
 - Growth from 3,734/1998, 9,859/1999, 21,765/2000
- Estimated 4000+ DDOS attacks per week
- On-going probes (via Intel, 2001)
 - 50-60 incidents per day on Internet
 - 10-12 incidents per day on DSL
 - 5-6 incidents per day on dial-up




Spring 2003

<http://www.cerias.purdue.edu>

21




CERIAS



**Center for Education and Research in
Information Assurance and Security**

Software Ownership


- Proprietary source is more secure
- Open source is more secure
- Being able to examine code makes my code more secure
- Being able to patch my code makes it more secure




Spring 2003

<http://www.cerias.purdue.edu>

22



CERIAS




Center for Education and Research in
Information Assurance and Security

Software Ownership

- Proprietary source is more secure
- Open source is more secure
- Being able to view the code makes my code more secure
- Being able to modify my code makes it more secure


Myths!




Spring 2003

<http://www.cerias.purdue.edu>

23



CERIAS



Center for Education and Research in
Information Assurance and Security

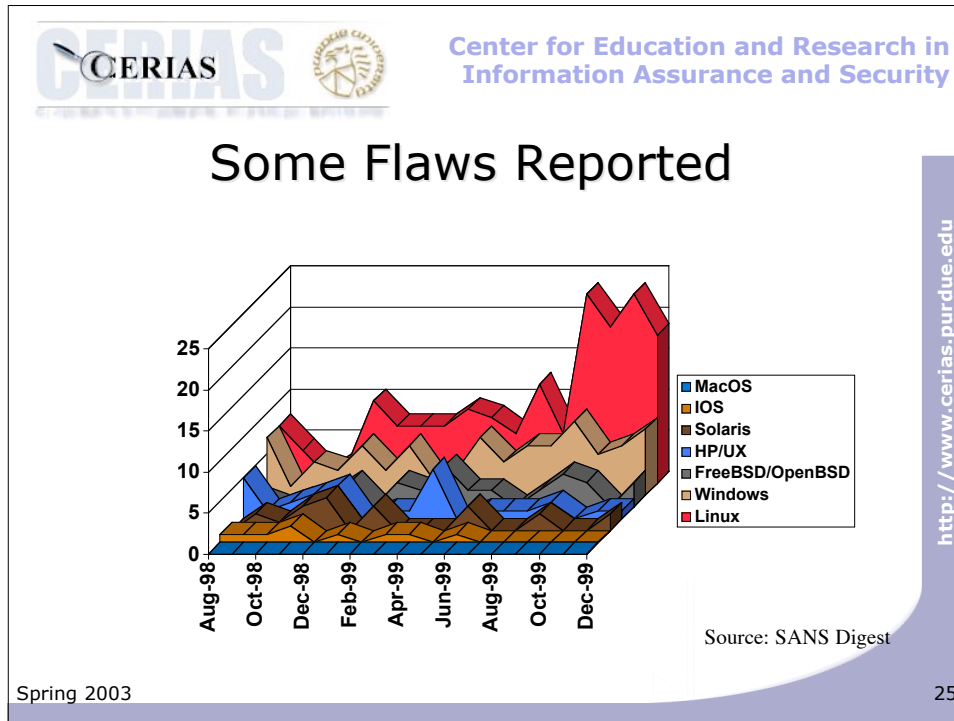
Reality

- Ownership has little to do with code quality. Training, tools, and process are more important.
- Comparing against current systems creates a false impression
 - S/COMP, GEMSOS, Trusted-VMS
- Examples such as sendmail trojan, SSL overflows, Kerberos flaws, etc.

Spring 2003

<http://www.cerias.purdue.edu>

24



Spring 2003

25

<http://www.cerias.purdue.edu>



Operating System	Percentage
Microsoft Windows	44%
Linux	19%
*BSD	9%
Sun Solaris	7%
SGI Irix	6%
Novell Netware	4.5%
IBM AIX	4%
Compaq Tru64	1.9%
Mac OS	1.9%
SCO Unix	0.5%
Totals	97.8%

Statistics for 1/1/02–11/1/02
As collected by mi2g.net
1162 vulnerabilities

Spring 2003

26

<http://www.cerias.purdue.edu>

Center for Education and Research in Information Assurance and Security

Data from 1/1/2000–1/15/2003



Linux security vulnerabilities	206
Windows (2000 & NT) vulnerabilities	144
Solaris security vulnerabilities	87
HP-UX security vulnerabilities	78
AIX security vulnerabilities	54
OpenBSD vulnerabilities	46
Microsoft Internet Explorer	89
Microsoft IIS	55
Apache	32

Spring 2003

Taken from <https://cassandra.cerias.purdue.edu/resource/products.php>

<http://www.cerias.purdue.edu>

27

Center for Education and Research in Information Assurance and Security

Break-ins Reported by Selected FIRST Teams (2001)



- Linux compromises dominated
 - Nearly 4 to 1 over Windows
- Commercial Unix compromises quite rare
- Windows/Unix compromises were 2 to 1
- MacOS compromises did not occur

Computer viruses are a different issue

Spring 2003

<http://www.cerias.purdue.edu>

28



Center for Education and Research in
Information Assurance and Security

Experience at Major Hosting Sites



- Windows
 - Too unstable
 - Can't handle load well
- Linux
 - Too "hackable"
 - Requires too many updates
- *BSD – system of choice

(Source: article at upside.com about CaveCreek)

Spring 2003

<http://www.cerias.purdue.edu>

29



Center for Education and Research in
Information Assurance and Security


Full Disclosure

- Vendors won't fix problems otherwise
- All the bad guys know about them already
- Lets the good guys apply their own fixes
- People need the details to see if they are affected

Spring 2003

<http://www.cerias.purdue.edu>

30



Center for Education and Research in Information Assurance and Security


Full Disclosure

- Vendors won't fix problems otherwise
- All the bad guys have been already
- Lets vendors know their own fixes
- People want details to see if they are affected

Misconceptions!

<http://www.cerias.purdue.edu>

Spring 2003 31





Center for Education and Research in Information Assurance and Security

Disclosure

- Many vendors now proactively fixing problems
 - Patches released for problems not known before
 - Increasing consumer demand
 - Increasing government pressure

<http://www.cerias.purdue.edu>

Spring 2003 32



Center for Education and Research in
Information Assurance and Security



Disclosure

- Hacker/Cracker community more fragmented
- Many more script kiddies than experts
- Same is true of the sysadmin crowd!
 - Most operators unable to create and apply patches

Spring 2003

<http://www.cerias.purdue.edu>

33



Center for Education and Research in
Information Assurance and Security

Endangering the Community



Studies by researchers and anecdotal evidence by response teams shows that the majority of break-ins from a flaw go from zero to maximum AFTER the disclosure.

Maximum activity is often 4-6 weeks after exploit publication and patch release!

Spring 2003

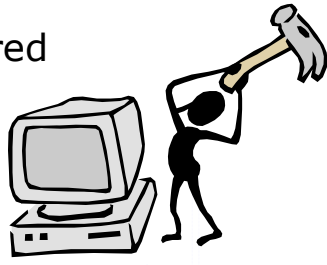
<http://www.cerias.purdue.edu>

34

  Center for Education and Research in Information Assurance and Security

Security Expertise

- Hackers make the best security specialists
- Breaking into systems is the best way to learn about security
- Security can be assured with attack tools



<http://www.cerias.purdue.edu>

Spring 2003 35

  Center for Education and Research in Information Assurance and Security

Security Expertise


- Hackers make the best security specialists
- Breaking into systems is the best way to learn about security
- Security can be assured with attack tools

Misconceptions!




<http://www.cerias.purdue.edu>

Spring 2003 36




CERIAS



Center for Education and Research in
Information Assurance and Security

Reality


- Infosec experts need to know
 - Software engineering
 - Law
 - Psychology and management issues
 - Networking
 - ... and much more
- Criminal history is not a job qualifier
- Again, comparison against the norm is misleading
- Major defense-related sites will not hire hackers




Spring 2003

37

<http://www.cerias.purdue.edu>



CERIAS



Center for Education and Research in
Information Assurance and Security


Cheaper, Safer, Better

- The government should use COTS whenever possible
- I only need to invest in a good ... to be safe.
 - Firewall
 - IDS
 - Anti-virus system
- Standardizing software will be cheaper


Spring 2003

38

<http://www.cerias.purdue.edu>



CERIAS



Center for Education and Research in
Information Assurance and Security

Cheaper, Safer, Better


False Economy!

- The government should buy COTS whenever possible
- I only need to invest in a good... to be safe.
 - Firewall
 - IDS
 - Anti-virus system
- Standardizing software will be cheaper


Spring 2003

39

http://www.cerias.purdue.edu



CERIAS



Center for Education and Research in
Information Assurance and Security

Realities

- Insider threats are not countered by most firewalls, AV or IDS
- New malware is not stopped by most products
- Denial-of-service is not prevented
- COTS software is not designed to be secure...and this is widely known

Spring 2003

40

http://www.cerias.purdue.edu

  Center for Education and Research in Information Assurance and Security



Secure Design Principles

- Least privilege
- Economy of mechanism
- Complete mediation
- Open design
- Separation of privilege
- Least common mechanism
- Psychological acceptability

J. H. Saltzer & M. D. Schroeder 1975

Spring 2003 41

<http://www.cerias.purdue.edu>

  Center for Education and Research in Information Assurance and Security



Apocryphal Quote

"If you build software without [requirements and] specifications, it can never be incorrect – it can only be surprising."

Brian Kernighan

Spring 2003 42

<http://www.cerias.purdue.edu>



Center for Education and Research in
Information Assurance and Security



Using the Wrong Requirements

- Ensuring Successful Implementation of Commercial Items in Air Force Systems, USAF Scientific Advisory Board, April 2000
 - "COTS software is not secure. ... It is strongly recommended that COTS products, particularly software, not be used for critical applications."
- GCN, Sept 11, 2000
 - "The Navy's next-generation aircraft carrier will use Microsoft Windows 2000 to run its communications systems, aircraft and weapons launchers, and other ship electronics...[Windows] should reduce lifecycle crewing and maintenance costs, as well as procurement costs..."

Spring 2003

<http://www.cerias.purdue.edu>

43



Center for Education and Research in
Information Assurance and Security



Cutting-edge Technology

- Wireless
- Voice over IP (VOIP)
- Convergence
- PDAs/portable computing
 - Bluetooth
- RFID

Spring 2003

<http://www.cerias.purdue.edu>

44

  Center for Education and Research in Information Assurance and Security



Cutting-edge Technology

- Wireless
- Voice over IP (VOIP)
- Convergence
- PDAs/portable devices
 - Bluetooth
- RFID

Fads!

<http://www.cerias.purdue.edu>

Spring 2003 45

  Center for Education and Research in Information Assurance and Security

Concluding comments


Security is an unattainable absolute.

We should be seeking high levels of trust, based on sound methods of assurance.

Assurance is an on-going process, not a set of add-on features.

<http://www.cerias.purdue.edu>

Spring 2003 46


CERIAS  Center for Education and Research in Information Assurance and Security

Understanding Assurance

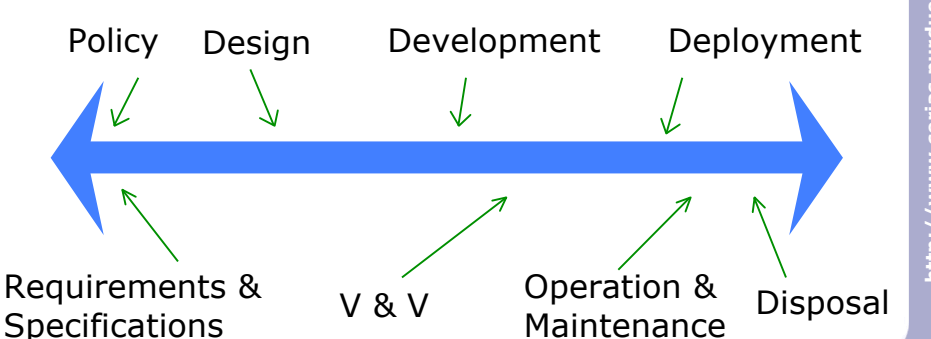
- Assurance requires
 - Limiting what happens
 - Limiting who can make it happen
 - Limiting how it happens
 - Limiting who can change the system
 - Providing recovery mechanisms
- Users don't tolerate limits well
- But users don't understand risks

Spring 2003 47

http://www.cerias.purdue.edu

CERIAS  Center for Education and Research in Information Assurance and Security

Where to Assure

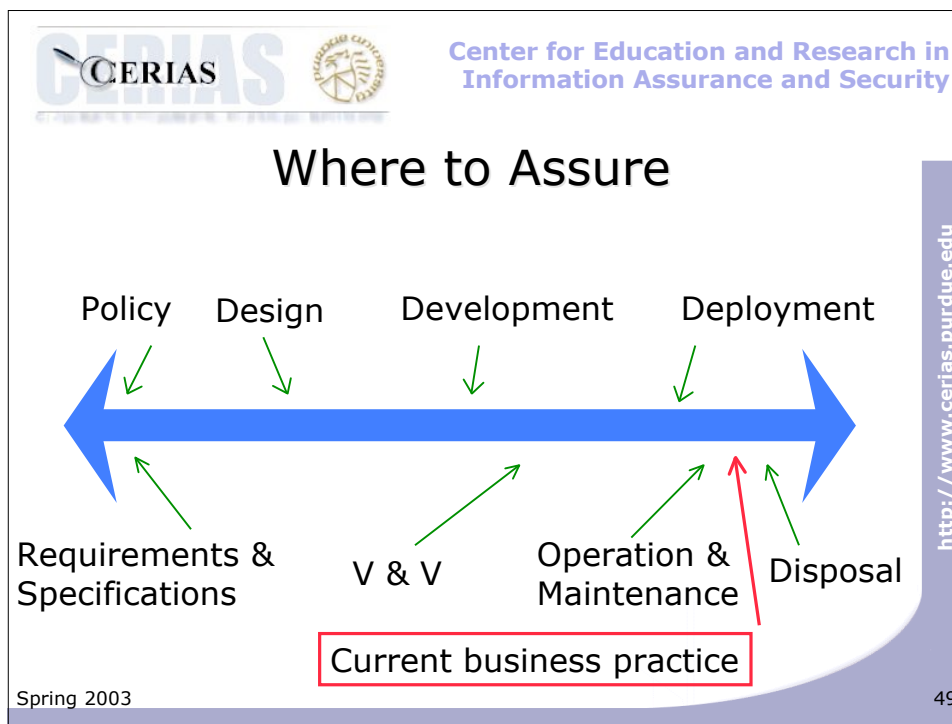


Policy Design Development Deployment


Requirements & Specifications V & V Operation & Maintenance Disposal

Spring 2003 48

http://www.cerias.purdue.edu



-
- In summary**
- Security is not simple.
 - Security is not an add-on.
 - Quality and security are closely linked.
 - Training and knowledge are critical to counter superstition and folklore
- ... but trends and lack of resources mean we are likely to face many challenges.
- The slide is part of a presentation from CERIAS, Center for Education and Research in Information Assurance and Security, dated Spring 2003.



Center for Education and Research in
Information Assurance and Security

Thank you!
Questions?

Spring 2003

51

<http://www.cerias.purdue.edu>