

"Since when is public safety the root password to the Constitution?"

- C. D. Tavares

*Topics*

Service Packs and Updates

The Laws of Security

Legal, Ethical and Professional Issues

Remote Access

**In the News**

**U.S.**

**Homeland Security accepts fake ID**

From Hussein Saddique  
CNN  
Monday, June 12, 2006; Posted: 9:40 p.m. EDT (01:40 GMT)

(CNN) -- A man using a fake identification card was able to enter the Homeland Security Department headquarters in Washington, he said, even though the United States government considers the type of Mexican-issued card he used invalid.



Retired New York City policeman Bruce DeCell, who had arranged to meet with DHS officials last week to lobby for document security, told CNN he purposely used a forged version of identification that Mexican consulates in the United States issue to their nationals living here illegally.

A DHS spokesman says "We seek to ensure that an incident like this does not occur again."

Undocumented Mexicans can use the cards at banks and other institutions that accept them. The cards are not valid for entry into federal government buildings.

**Homework**  
**Examine Your System**

**Examining Your System**

What did you find?

Were you surprised?

Would you let someone else examine your computer?

**Security Demo**

**Microsoft Service Packs and Updates**

**Service Packs**

Free downloads from Microsoft Updates OS for security and bugs  
Recommends fixes

Other programs rely on these updates

Internet vs. Redistributable

**Installing on W2K server on VMware**

On Host PC, create folder SP4

Download W2K SP4, Rollup

On W2K Server

Create a folder D:\Shared

Right Click / Properties / Sharing

Share as "Shared"

On Host PC

Windows Explorer: \\Server-1\shared

Copy SP4 folder to Shared

Copy BGInfo to Shared

Copy VMWareTools

**Installing the Service Packs**

Install BGInfo

Add to startup

Modify shortcut to include /timer:0

Install Service Pack 4

Do Not Archive Files

Install SP4 Rollup

Install VMWare tools

# The Ten Immutable Laws of Security

## The Ten Immutable Laws of Security

Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.

Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.

## The Ten Immutable Laws of Security

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

Law #4: If you allow a bad guy to upload programs to your web site, it's not your web site any more.

## The Ten Immutable Laws of Security

Law #5: Weak passwords trump strong security.

Law #6: A machine is only as secure as the administrator is trustworthy.

Law #7: Encrypted data is only as secure as the decryption key.

## The Ten Immutable Laws of Security

Law #8: An out of date virus scanner is only marginally better than no virus scanner at all.

Law #9: Absolute anonymity isn't practical, in real life or on the web.

Law #10: Technology is not a panacea.

# The Ten Immutable Laws of Security Administration

## The Ten Immutable Laws of Security Administration

Law #1: Nobody believes anything bad can happen to them, until it does.

Law #2: Security only works if the secure way also happens to be the easy way.

## The Ten Immutable Laws of Security Administration

Law #3: If you don't keep up with security fixes, your network won't be yours for long.

Law #4: It doesn't do much good to install security fixes on a computer that was never secured to begin with.

## The Ten Immutable Laws of Security Administration

Law #5: Eternal vigilance is the price of security.

Law #6: There really is someone out there trying to guess your passwords.

## The Ten Immutable Laws of Security Administration

Law #7: The most secure network is a well-administered one.

Law #8: The difficulty of defending a network is directly proportional to its complexity.

## The Ten Immutable Laws of Security Administration

Law #9: Security isn't about risk avoidance; it's about risk management.

Law #10: Technology is not a panacea.

## A good Idea

These laws are available for download from Microsoft as screen savers.

Use as part of a security education policy.

# Linux Demo

# Ubuntu



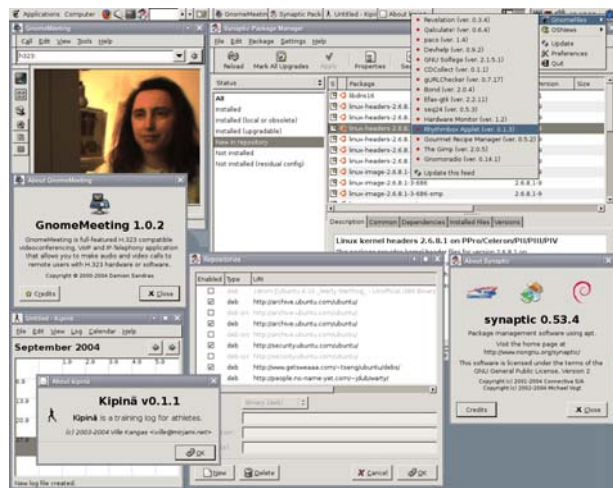
Linux for Human Beings



## Ubuntu

is an ancient African word, meaning "humanity to others". Ubuntu also means "I am what I am because of who we all are". The Ubuntu Linux distribution brings the spirit of Ubuntu to the software world.

[www.ubuntu.com](http://www.ubuntu.com)



## Commitment to Users

Ubuntu will always be free of charge, and there is no extra fee for the "enterprise edition", we make our very best work available to everyone on the same Free terms.

Ubuntu includes the very best in translations and accessibility infrastructure that the Free Software community has to offer, to make Ubuntu usable by as many people as possible.

## Commitment to Users

Ubuntu is released regularly and predictably; a new release is made every six months. Each release is supported with security updates for at least 18 months.

Ubuntu is entirely committed to the principles of free and open source software development; we encourage people to use free and open source software, improve it and pass it on.

## Specs

Ubuntu is suitable for both desktop and server use. The current Ubuntu release supports Intel x86 (IBM-compatible PC), AMD64 (Hammer) and PowerPC (Apple iBook and Powerbook, G4 and G5) architectures.

Ubuntu includes more than 1,000 pieces of software: OpenOffice, Internet Access, Programming, Tools, Games.

## A Big Splash...

Ubuntu has been getting a lot of good press

#1 at Distowatch.com

PC World #25 in the top 100 products of 2005

Page Hit Ranking		
Data span: Last 6 months		
Refresh		
Rank	Distribution	H.P.D*
1	Ubuntu	2276▲
2	Mandriva	1637→
3	MEPIS	1372▼
4	Fedora	1297▲
5	SUSE	1233→
6	Debian	946▲
7	kNOPIX	849▼
8	Gentoo	698→
9	Slackware	611→
10	Damn.Small	588▲

## Geek Quote

Ubuntu is "a distribution which is based on Debian's powerful package manager, is as user friendly as Mandrake thinks it is, yet is as lightweight as Slackware is capable of being.

www.osnews.com

## Getting it

Download it  
Mirrors, BitTorrent

Order it... For free (even postage!)  
Ordering multiple copies encouraged

Versions  
Stable - Production version  
Development version

## Using It

Live CD  
Boots from CDs, can play with OS

Install it  
Repartition the Hard Drive  
Make sure you backup first!

# Chapter 3 Legal, Ethical & Professional Issues

In civilized life, law floats in a sea of ethics.  
- Earl Warren, Chief Justice, US Supreme Court,  
November 12, 1962

### Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain societal behavior
- Ethics: define socially acceptable behavior
- Cultural mores: fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

### Types of Law

- Civil
- Criminal
- Tort
- Private
- Public

### Relevant U.S. Laws (General)

- Computer Fraud and Abuse Act of 1986 (CFA Act)
- National Information Infrastructure Protection Act of 1996
- USA Patriot Act of 2001
- Telecommunications Deregulation and Competition Act of 1996
- Communications Decency Act of 1996 (CDA)
- Computer Security Act of 1987

## Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously unheard of

## Privacy of Customer Information

- Privacy of Customer Information Section of common carrier regulation
- Federal Privacy Act of 1974
- Electronic Communications Privacy Act of 1986
- Health Insurance Portability and Accountability Act of 1996 (HIPAA), aka Kennedy-Kassebaum Act
- Financial Services Modernization Act, or Gramm-Leach-Bliley Act of 1999

## Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Security And Freedom Through Encryption Act of 1999 (SAFE)

## U.S. Copyright Law

- Intellectual property recognized as protected asset in the U.S.; copyright law extends to electronic formats
- With proper acknowledgement, permissible to include portions of others' work as reference
- U.S. Copyright Office Web site: [www.copyright.gov](http://www.copyright.gov)

## Freedom of Information Act of 1966 (FOIA)

- Allows access to federal agency records or information not determined to be matter of national security
- U.S. government agencies required to disclose any requested information upon receipt of written request
- Some information protected from disclosure

## State and Local Regulations

- Restrictions on organizational computer technology use exist at international, national, state, local levels
- Information security professional responsible for understanding state regulations and ensuring organization is compliant with regulations

## International Laws and Legal Bodies

- European Council Cyber-Crime Convention:
  - Establishes international task force overseeing Internet security functions for standardized international technology laws
  - Attempts to improve effectiveness of international investigations into breaches of technology law
  - Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution
  - Lacks realistic provisions for enforcement

## Digital Millennium Copyright Act (DMCA)

- U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement
- A response to European Union Directive 95/46/EC, which adds protection to individuals with regard to processing and free movement of personal data

## United Nations Charter

- Makes provisions, to a degree, for information security during information warfare (IW)
- IW involves use of information technology to conduct organized and lawful military operations
- IW is relatively new type of warfare, although military has been conducting electronic warfare operations for decades

## Policy Versus Law

- Most organizations develop and formalize a body of expectations called policy
- Policies serve as organizational laws
- To be enforceable, policy must be distributed, readily available, easily understood, and acknowledged by employees

## Ethics and Information Security

### The Ten Commandments of Computer Ethics\*

#### From The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

## Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical
- Difficulties arise when one nationality's ethical behavior conflicts with ethics of another national group
- Example: many of ways in which Asian cultures use computer technology is software piracy

## Ethics and Education

- Overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training vital to creating informed, well prepared, and low-risk system user

## Deterrence to Unethical and Illegal Behavior

- Deterrence: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - Probability of being caught
  - Probability of penalty being administered

## Codes of Ethics and Professional Organizations

- Several professional organizations have established codes of conduct/ethics
- Codes of ethics can have positive effect; unfortunately, many employers do not encourage joining of these professional organizations
- Responsibility of security professionals to act ethically and according to policies of employer, professional organization, and laws of society

## Association of Computing Machinery (ACM)

- ACM established in 1947 as "the world's first educational and scientific computing society"
- Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others' privacy, and respecting others' intellectual property

## International Information Systems Security Certification Consortium, Inc. (ISC)<sup>2</sup>

- Non-profit organization focusing on development and implementation of information security certifications and credentials
- Code primarily designed for information security professionals who have certification from (ISC)<sup>2</sup>
- Code of ethics focuses on four mandatory canons

## System Administration, Networking, and Security Institute (SANS)

- Professional organization with a large membership dedicated to protection of information and systems
- SANS offers set of certifications called Global Information Assurance Certification (GIAC)

## Information Systems Security Association (ISSA)

- Nonprofit society of information security (IS) professionals
- Primary mission to bring together qualified IS practitioners for information exchange and educational development
- Promotes code of ethics similar to (ISC)<sup>2</sup>, ISACA and ACM

## Other Security Organizations

- Internet Society (ISOC): promotes development and implementation of education, standards, policy and education to promote the Internet
- Computer Security Division (CSD): division of National Institute for Standards and Technology (NIST); promotes industry best practices and is important reference for information security professionals

## Other Security Organizations (continued)

- CERT Coordination Center (CERT/CC): center of Internet security expertise operated by Carnegie Mellon University
- Computer Professionals for Social Responsibility (CPSR): public organization for anyone concerned with impact of computer technology on society

## Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation's National Infrastructure Protection Center (NIPC)
- National Security Agency (NSA)
- U.S. Secret Service

## Organizational Liability and the Need for Counsel

- Liability is legal obligation of an entity; includes legal obligation to make restitution for wrongs committed
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that an organization make valid effort to protect others and continually maintain that level of effort

# Computer Crime

## Some Legal Cases

### **Lund v. Commonwealth,** 217 Va. 688, 232 S.E.2d 745 (1977)

Lund - grad student at Virginia Tech used computer time and services to work on his doctoral thesis, charging the costs back to other departments.

He was charged with grand larceny and larceny by false pretense

### **Result**

The Supreme Court of Virginia reversed his conviction.

Court held that computer time and services were not goods and chattels (personal property) within the meaning of the statutes. They could not be carried away.

### **United States v. Jones,** 553 F.2d 351 (4th Cir. 1977)

Case of altered accounts payable data. Altered accounts payable documents by changing vendor number 99900 to 98844

Computer issued five checks to Jones for over \$130,000

<b>Charges</b>  Five counts of transporting securities of more than \$5,000, knowing them to have been stolen, converted, or taken by fraud.  Five counts of selling or receiving these securities, knowing them to have been stolen, converted, or taken by fraud.	<b>Defense</b>  Jones moved to dismiss the indictment, contending that the securities (checks) were forgeries, which are excluded from the code sections under which she was indicted.	<b>Result</b>  The statutory exclusion refers to forgeries, so the question was whether the checks were forgeries.  The court held that the checks were not forged, but that they were genuine instruments that were illegally issued.  Guilty.
<b>United States v. Sampson,</b> 6 Comp.L.Serv.Rep. 879 (N.D.Cal. 1978)  Use of a government computer without authorization. Sampson had accessed a NASA computer from his home telephone, using its time and storage capacity for his own business.	<b>Charge</b> Offenses under 18 U.S.C. § 641,  Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency ...	<b>Defense</b>  Argued that computer time and storage capacity are not property within the meaning of the statute.  Defendants characterized them as "mere philosophical concepts as distinguished from interests capable of being construed as property."
<b>Result</b>  The consumption of its time and the utilization of its capacities seem to the court to be inseparable from the physical identity of the computer itself. That the computer is property cannot be questioned. Thus, the uses of the computer and the product of such uses would appear to the court to be a "thing of value"	<b>People v. Weg,</b> 113 Misc.2d 1017, 450 N.Y.S. 957 (N.Y.City Crim Ct. 1982)  Weg was a computer programmer for the Board of Education of New York City. He was accused of using the computer system for his own commercial benefit.	<b>Charge</b> Theft of services under New York Penal Code § 165.15(8), which reads: Obtaining or having control over labor of another person, or of business, commercial or industrial equipment or facilities of another person, knowing that he is not entitled to the use thereof, and with intent to deprive a commercial or other substantial benefit ...

<p><b>Results</b></p> <p>The Board's computer service was not rented or sold to outsiders for a fee so it was not "business" equipment. Unauthorized use of computers was not a crime.</p> <p>165.15(8) only applies to unauthorized tapping into a computer whose service is for hire.</p>	<p><b>Arizona v. Moran,</b> 162 Ariz. 524, 784 P.2d 730 (Ariz. App. 1989)</p> <p>Moran developed a program relating to depreciation of company costs. He encoded his programs, as was company custom. When Moran asked for a period of personal leave, he refused to decrypt.</p>	<p><b>Charges</b></p> <p>Prosecution under Arizona's computer fraud statute (A.R.S. § 13-2316 (B)) and a more general criminal damage statute. A.R.S. § 13-1601(4).</p>
<p><b>Results</b></p> <p>Moran was acquitted on the unauthorized access charge because his access, and the encoding, were authorized under company policy.</p> <p>Criminal damage requires reckless tampering or interference with the property of another. Moran's behavior was probably spiteful. Few forms of spiteful conduct are criminal.</p>	<p><b>Prosecuting Computer Crimes</b></p> <p>Lack of uniform reporting Lack of interest Charging the suspect Evidence Documentation Technical Jargon Informants Audit Trails</p>	<p><b>Sysop Liability</b></p> <ul style="list-style-type: none"> <li>- Failure to provide access, as promised.</li> <li>- Negligently allowing spread of a virus.</li> <li>- Cooperating with a fraudulent scheme.</li> <li>- Invading the privacy of a user.</li> <li>- Collaborating in criminal activities.</li> <li>- Allowing distribution of copyrighted material</li> <li>- Facilitating dissemination of defamatory material posted by a user.</li> </ul>
<p><b>Three types of sysop liability</b></p> <p>Direct: liability for the sysop's own actions or negligence.</p> <p>Vicarious: liability of the sysop for the actions of its employees and agents.</p> <p>Contributory: liability of the sysop for the actions it takes that contribute in some way to wrongdoing by others.</p> <p>Publisher or Post Office?</p>	<p><b>Cases</b></p> <p>Chubby vs. Compuserve CIS not held for message content Frena v. Playboy Frena held liable for photos Stratton Oakmont v. Prodigy Prodigy held liable for messages Netcom v. Scientology Netcom not liable for storage Zeran v. AOL AOL not liable for messages Germany v. Compuserve Compuserve held liable for child porn</p>	<p><b>In the News...</b> 09 Mar 2001</p> <p>The state Supreme Court said Thursday that federal law shields AOL from responsibility for illegal transactions - in particular, the sale of child pornography - that take place on its service.</p>

## Details

In a 4-3 decision, Florida's high court said the Communications Decency Act gives the Internet service provider immunity from a lawsuit filed by a Florida woman, whose 11-year-old son appeared in a lewd videotape sold by one AOL user to another.

# Hands On Security+

## Lab 3: Basic Security Tasks

## Basic Security Tasks

Disable Guest Account  
Rename Administrator Account  
Limit Administrator Accounts  
Set Legal Message  
Disable Unneeded Software

### Disable Guest Account

Programs / Administrative Tools  
Computer Management  
Local Users and Group  
Users

Make sure Guest account is disabled

### Rename Administrator Account

Programs / Administrative Tools  
Computer Management  
Local Users and Group  
Users

Right-Click on Administrator  
Rename  
Select something unique  
Don't forget it!

### Limit Administrator Accounts

Programs / Administrative Tools  
Computer Management  
Local Users and Group  
Groups

Open Administrators Group  
How many users had Admin rights?  
Do they all need it?

### Set Legal Message

Programs / Administrative Tools  
Local Security Policy  
Local Policy / Security Options

Edit Message Text for Users...  
Edit Message Title for Users...

### Disable Unneeded Software & Services

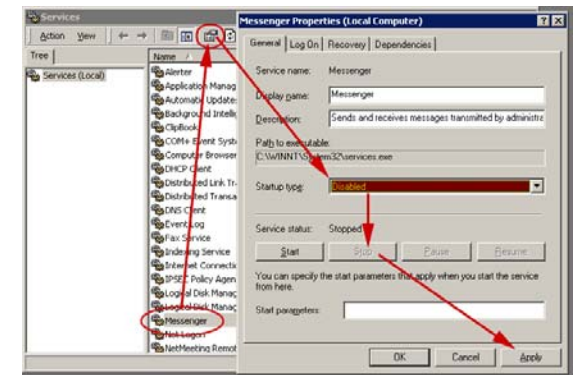
Delete anything that is not needed

Control Panel  
Add/Remove programs  
Add/Remove Windows Components

Programs / Administrative Tools  
Services  
Set Startup Type & Service Status

### Disabling Messenger Service

Stops some pop-up spam



# Security+

## Domain 2: Remote Access

### Communication Security

Accessing the system

Internet

Dial Up

Wireless

### 802.1x

Protecting Wireless Transmissions

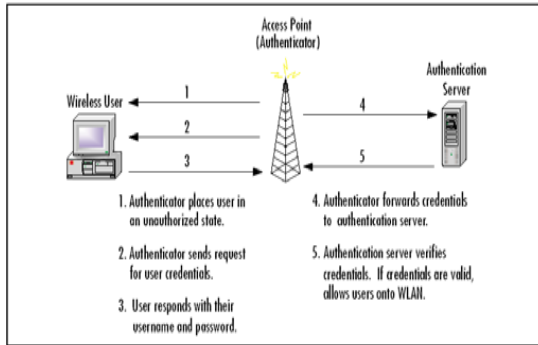
Wired Equivalent Privacy (WEP)

User: Supplicant

System: Authenticator

Extensible Authentication Protocol

### 802.1x Authentication Process



### EAP

Defined by RFC 2284

Revised by IETF 09/13/03

Runs at Data Link layer

Does not require IP

### EAP Formats

EAP over IP (EAPoIP)

Message Digest Algorithm/Challenge-Handshake Authentication Protocol (EAP-MD5-CHAP)

Transport Layer Security (EAP-TLS)

Tunneled Transport Layer Security (EAP-TTLS)

RADIUS

Light Extensible Authentication Protocol (LEAP) Cisco

### Vulnerabilities

WEP uses RC4 encryption

Can be cracked

AirSnort

Capture 5-10 million packets

Recreate key

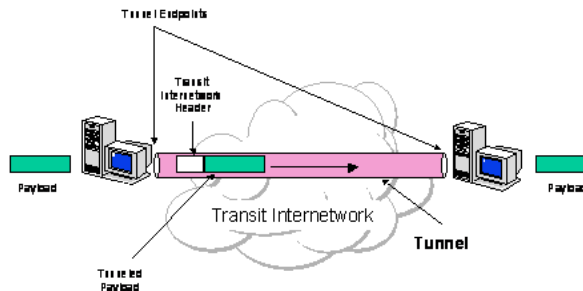
WEPCrack

Breaks secret key

### Virtual Private Network (VPN)

Secure connections over public Internet

Data is encrypted (tunneled)



### Tunneling Protocols

Carrier Protocol

Typically IP

Encapsulating Protocol

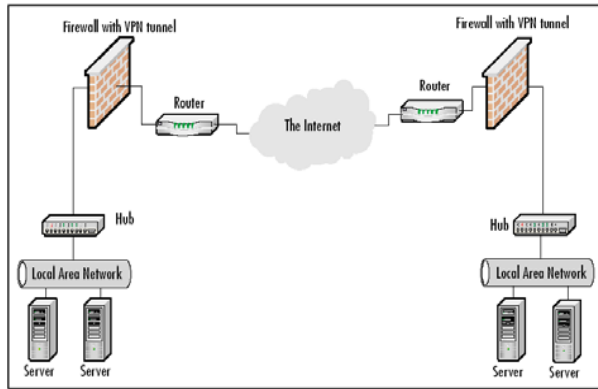
Wrapping the Data

PPTP, L2TP, IPSec, SSH

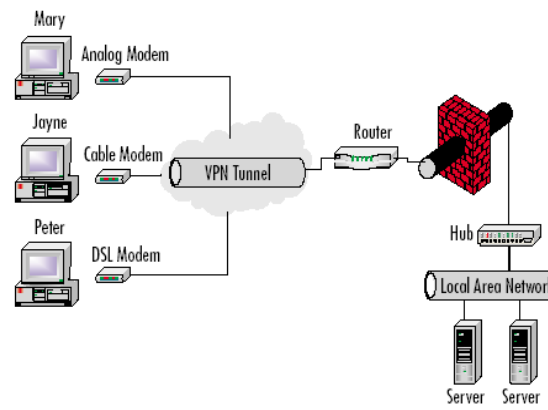
Passenger Protocol

The original data

## Site to Site VPN



## Remote Access VPN



## Next Class - Exam Computerized

The screenshot shows a computerized exam window titled 'Item 460 exam 2'. The question is: '1. Which of the following is NOT a project management cause of failed projects?'. The options are:

- A shortcuts taken during the project
- B lack of or imprecise targets
- C inadequate systems analysis and design tools
- D budget overruns
- E schedule delays

The interface includes a status bar at the bottom with the text 'Item 460 exam 2 Section 1 Question 1 8:14:09 PM' and a Windows taskbar with icons for Start, Back, Forward, and Stop.

End of This Lesson