

Overview of

IT Fraud



Thaweesak Koanantakool

Director,

NECTEC: National Electronics and Computer
Technology Center

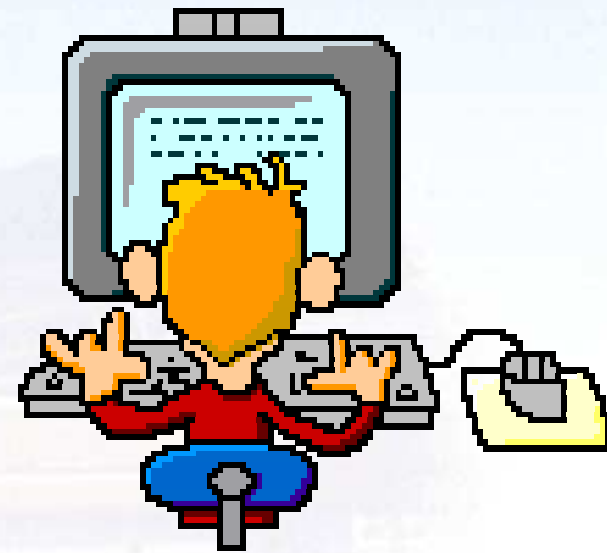
www.nectec.or.th/users/htk/publish/

Topics

- Major types of IT Frauds in a company
- Cost of IT Frauds
- Where are the weaknesses?
- Preparing your organization
- IT Laws

Basic problems of Computer Crime

*It's a lot more difficult
to investigate
and prosecute
computer crime
than it is to
perpetrate it.*



Addressing the major types of IT fraud in a company

IT Frauds



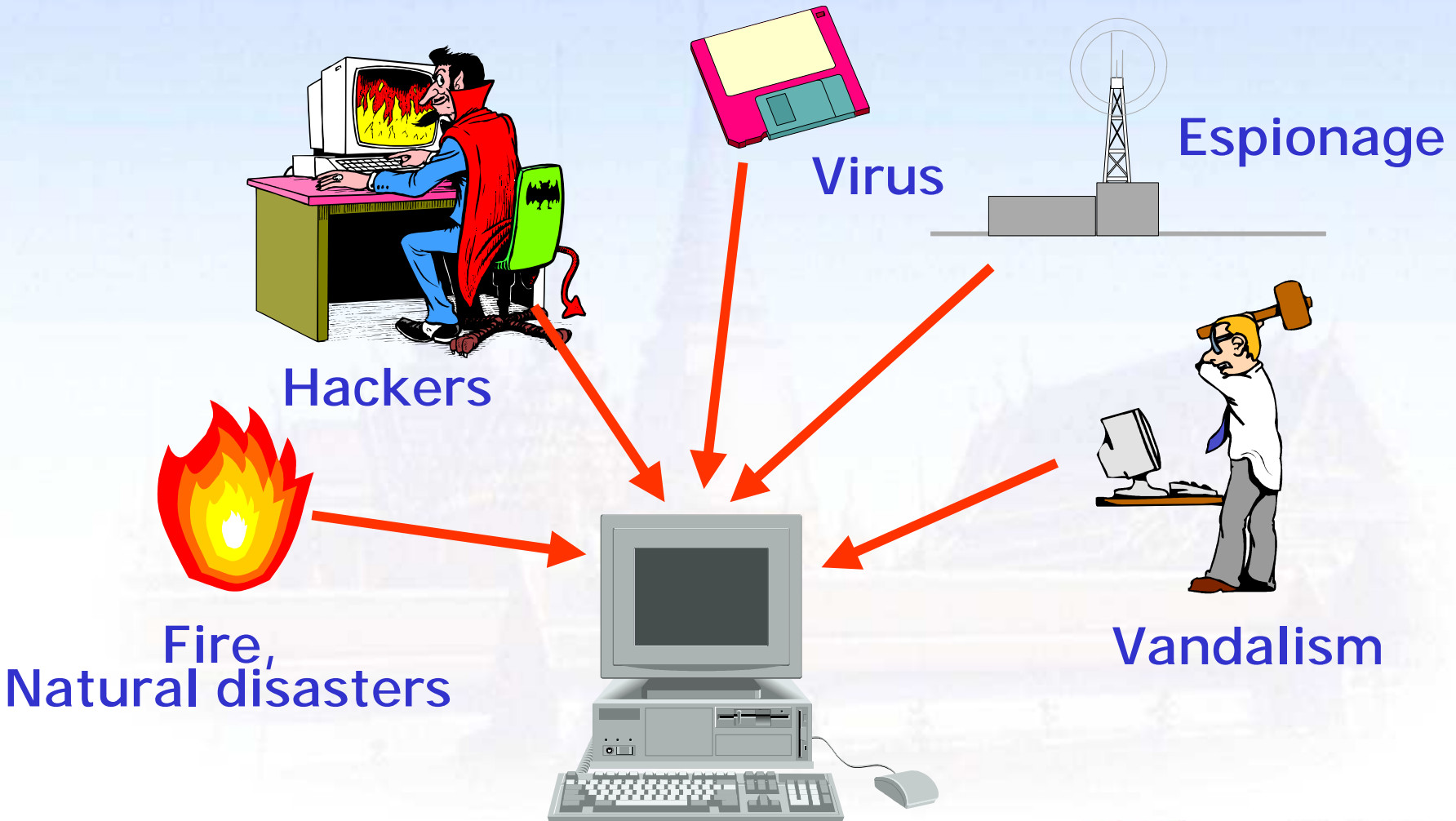
- Credit Card Frauds
- Electronic Document integrity
- Identity Thefts
- Social Engineering
- Eavesdropping

Payments in Thailand

ATM cards	20	Million cards
Credit cards	1.5	Million cards
Electronic cheque clearing	104	Billion baht/day
BAHTNET	250	billion baht/day (5% of GDP)
ATM Pool	1,553,000	Transactions/day
	5.2	Billion baht/day

Source: Bank of Thailand. Data as of Jan-June 2000.

What are the cause of IT-related losses?

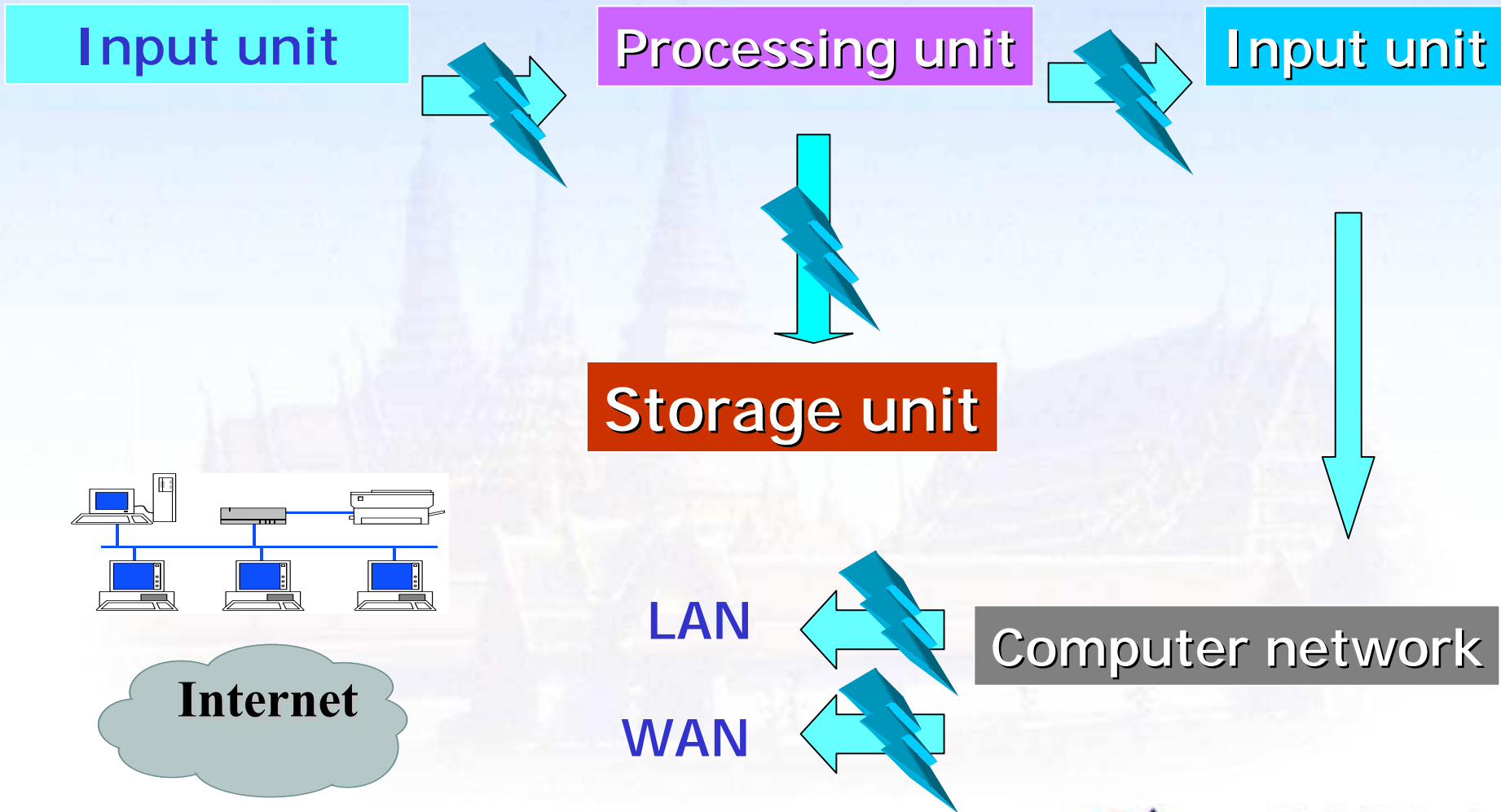


What are the target of attacks?

1. Data
2. Data system
3. Computer system
4. computer network



Computer system and attacks



Computer Crimes → IT Frauds

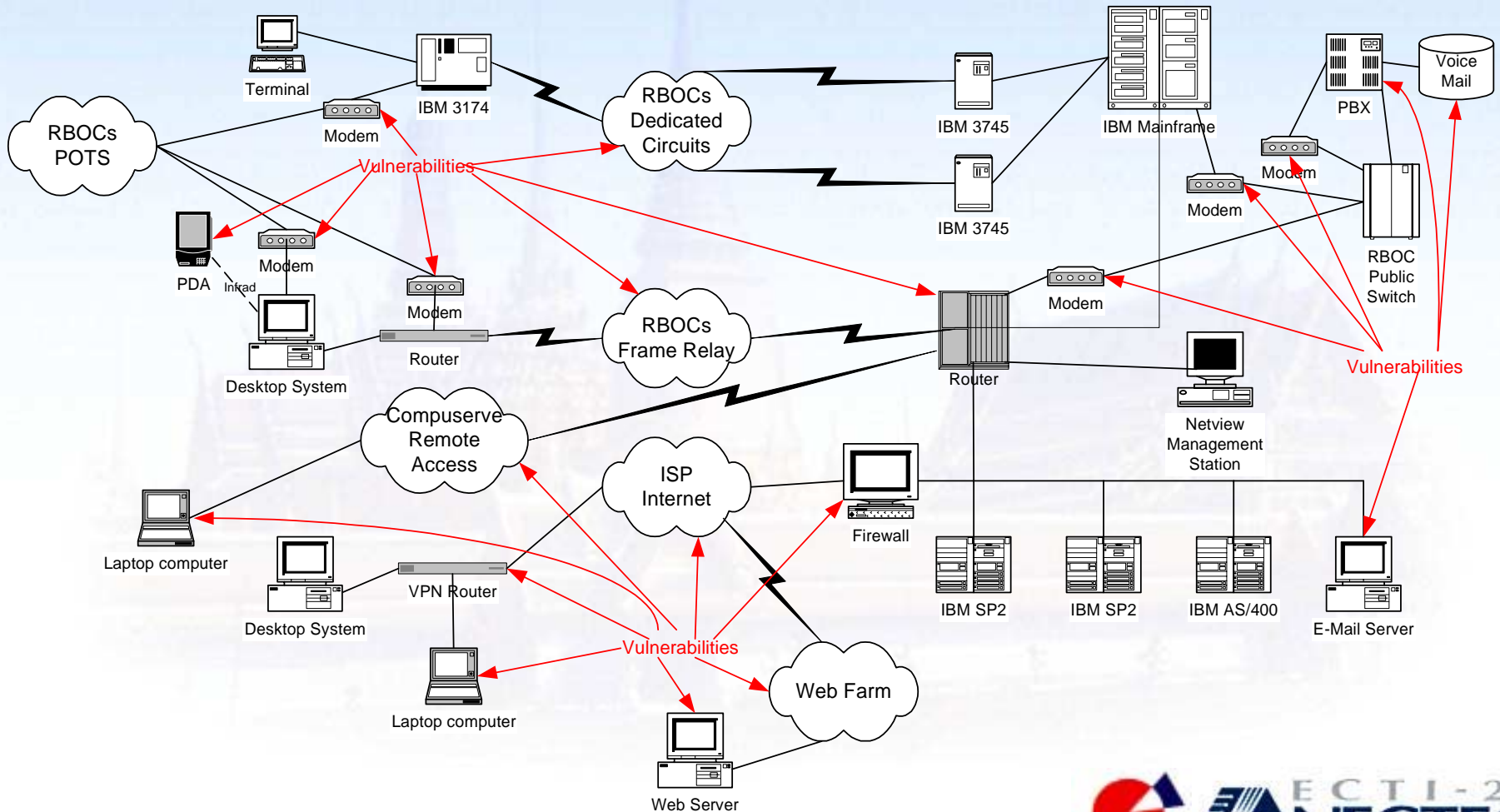


- Computer break-ins
- Web hacks
- Denial-of-service attacks
- E-mail bombings
- Viruses and worms
- Eavesdropping

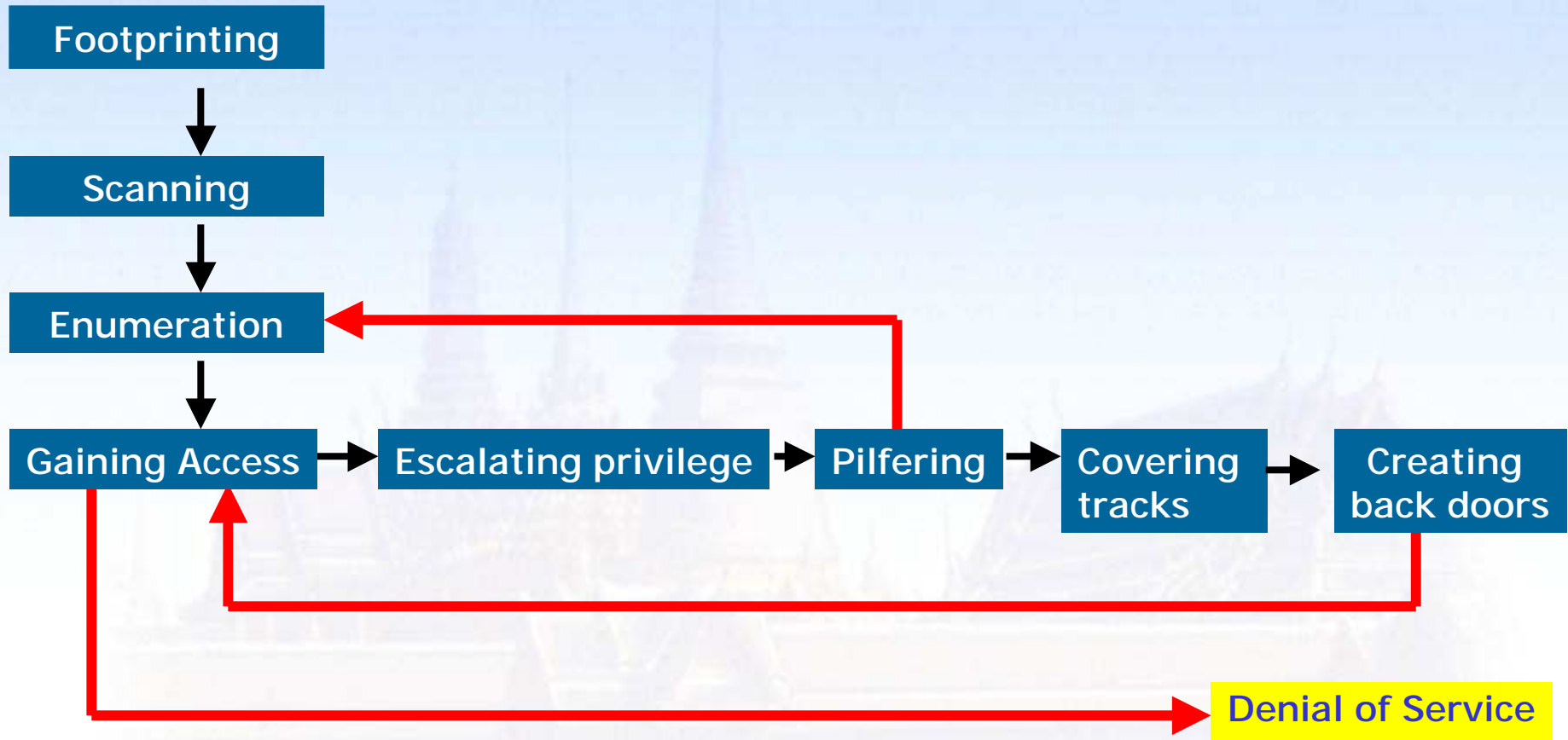
Type of Attacks

- Insider Attacks and Outsider Attacks
- Dos : SYN Flood, Ping of death, LAND, Nuke
- Application Layer Attack
- Bruce Force and Dictionary password attack
- Rootkit
- IP Spoofing
- TCP session hijacking

Computer Vulnerabilities



Anatomy of a hack



Footprinting

What is Footprinting?

Footprinting is the method of hackers for collect all data pertaining to the target, such as IP Address, Domain names, Access Control List, Intrusion Detection System, for hack in the future.

Types of footprinting

1. Internet Footprinting
2. Intranet Footprinting
3. Remote Access
4. Extranet



Security Risks

- Cleartext transmission (Sniffer Attack)
- Internet Worm (network congestion!!)
- Denial of Service or DoS
(Server cannot serve)
- Trojan Horse and Back Door
(Somebody is controlling your computer)
- Ip spoofing, mail Spam
(Somebody pretends to be you!)
- Exploit
(God knows who did that, you didn't!)
- Hacking through the Firewall via HTTP port

The crossroads of technology and management responsibilities of senior management to IT frauds detection and prevention

Technology and Management

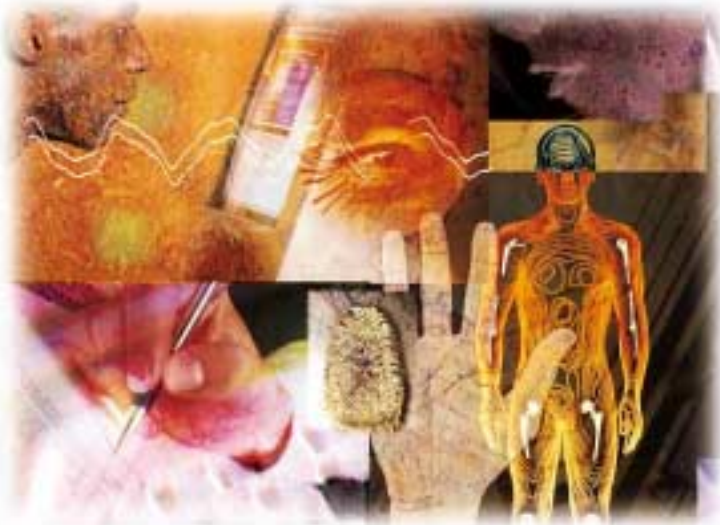
Your check list:

- “Chief Security Officer” in your organization?
- “Code of conduct” for IT users in an organization?
- “Best Practice” in securing IS in your organization?



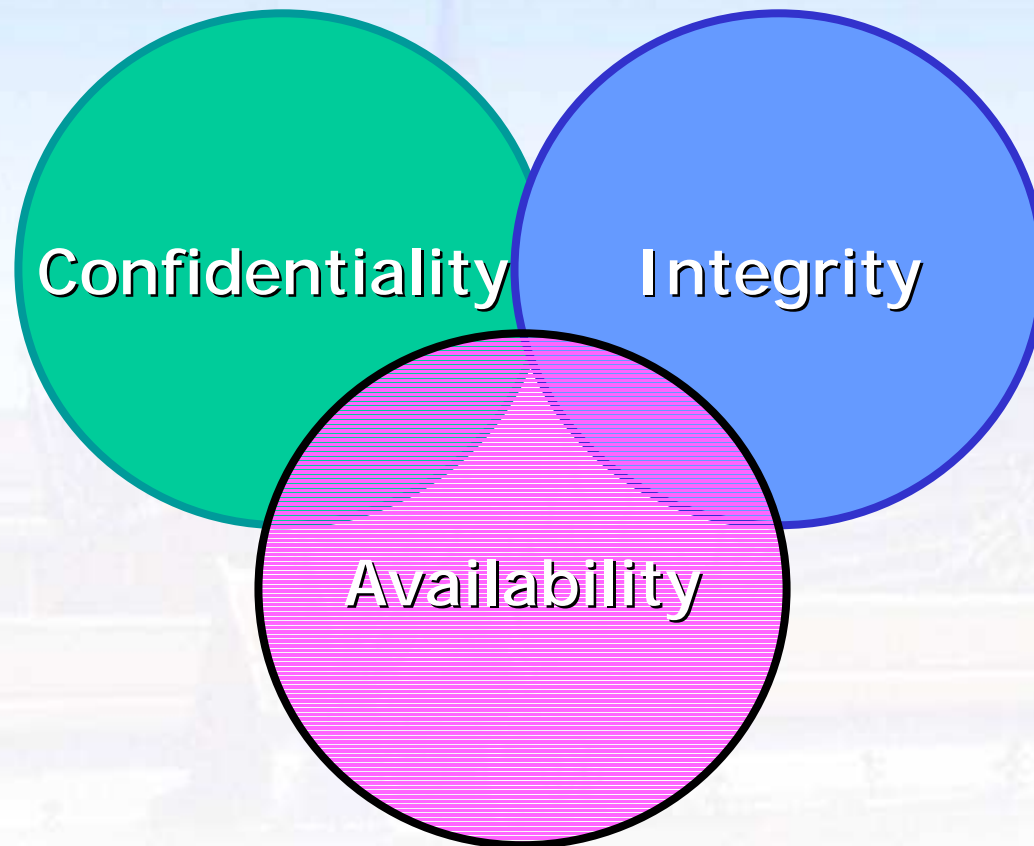
Technology and Management

- Performing “System Security Vulnerability” evaluation of your IT system
- Develop and practice a “Privacy Policy” to protect your customers personal information
- Investment in Security mechanisms, staff and working procedures



Preparing on organization from further IT fraud activities

Purposes of using security system



Computer Vulnerabilities



- **Hardware Security Threats**

Ex. Power Surge

- **Software Surity Threats**

Ex. Delete, Software Theft, Software modification, Computer Virus, Trojan Horses, Information Leaks, Trapdoor

- **Data Threats**

Ex. Breach of Secrecy, Beach of Integrity, Breach of Availability

Who is Hacker?

A slang term for a computer enthusiast, i.e., **a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).**

- the term can be either **complimentary** or **derogatory**, (increasingly derogatory connotation).
- The pejorative sense of hacker is becoming more prominent largely because the popular press has opted the term to refer to **individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data.**
- Hackers, themselves, maintain that the proper term for such individuals is **cracker.**

www.webopedia.com

Hackers' Hall of Fame

by Michelle Slatalla

Famous hackers. Infamous crackers. Modern-day Robin Hoods ... or educated thugs? Before you decide, check out our Hackers' Hall of Fame.



Vladimir Levin

A hacker of the old school, Stallman walked in off the street and got a job at MIT's Artificial Intelligence Lab in 1971.



Kevin Poulsen

In 1990 Poulsen took over all telephone lines going into Los Angeles area radio station KIIS-FM to win a call-in contest.



Dennis Ritchie and Ken Thompson

The driving creative force behind Bell Labs' legendary computer science operating group, Ritchie and Thompson created UNIX in 1969.



Johan Helsingius

Operated the world's most popular anonymous remailer, called penet.fi, until he closed up shop in September 1996.



John Draper

Figured out how to make free phone calls using a plastic prize whistle he found in a cereal box.



This mathematician allegedly masterminded the Russian hacker gang that tricked Citibank's computers into spitting out \$10 million.



Mark Abene

Inspired thousands of teenagers around the country to "study" the internal workings of our nation's phone system.



Steve Wozniak

The co-founder of Apple Computer got his start making devices for phone phreaking.



Robert Morris

This Cornell University graduate student accidentally unleashed an Internet worm in 1988.



Tsutomu Shimomura

Shimomura outhacked and outsmarted Kevin Mitnick, the nation's most infamous cracker/phreaker, in early 1994.



Kevin Mitnick

The first hacker to have his face immortalized on an FBI "Most Wanted" poster.



Linus Torvalds

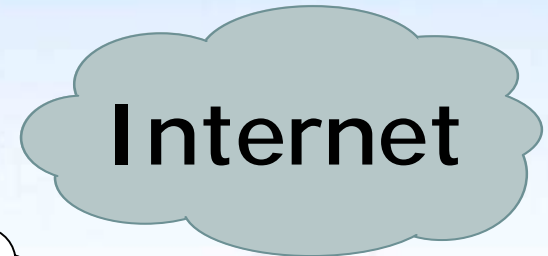
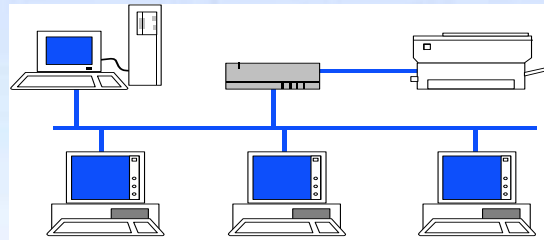
Torvalds was a computer science student at the University of Helsinki when he wrote the operating system Linux in 1991.

Advanced Techniques

- TCP Hijacking
- Back Doors
- Trojans Horse
- Web Hacking
- Hacking Internet User
- Email Hacking
- File Attachment Attack
- IRC Hacking



Unauthorized Access

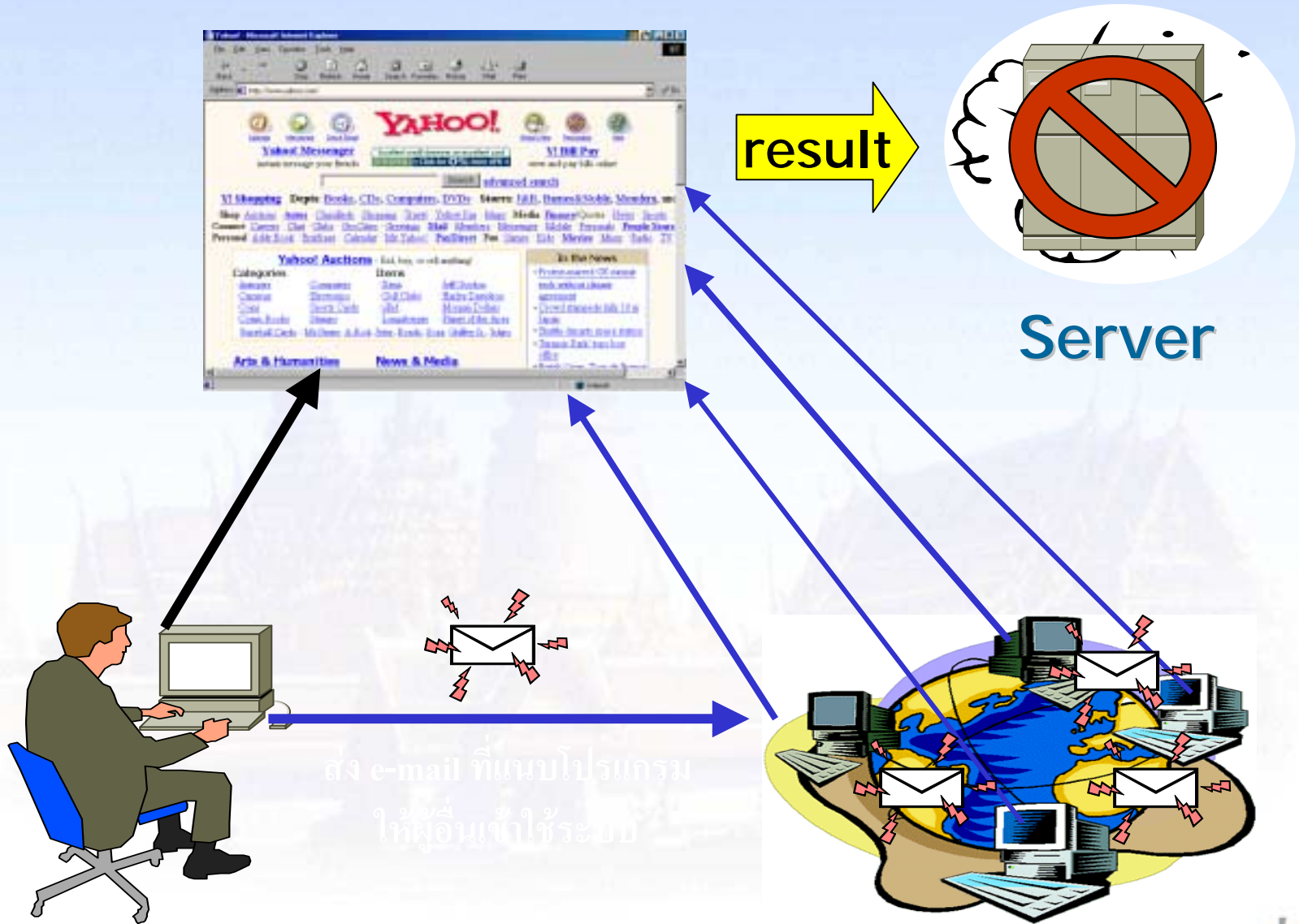


Insider



Outsider

Denial of Service : DoS





Closed doors: The trouble began on Monday, when hackers brought Web giant Yahoo to its knees. Over the next three days other victims suffered traffic jams and service breaks.

YAHOO!

Yahoo: First hit Monday morning, the portal was immobilized for three hours; at times availability ranged from zero to 10 percent

eBay: The auction house was almost totally incapacitated for hours Tuesday afternoon; a second attack was thwarted the next day

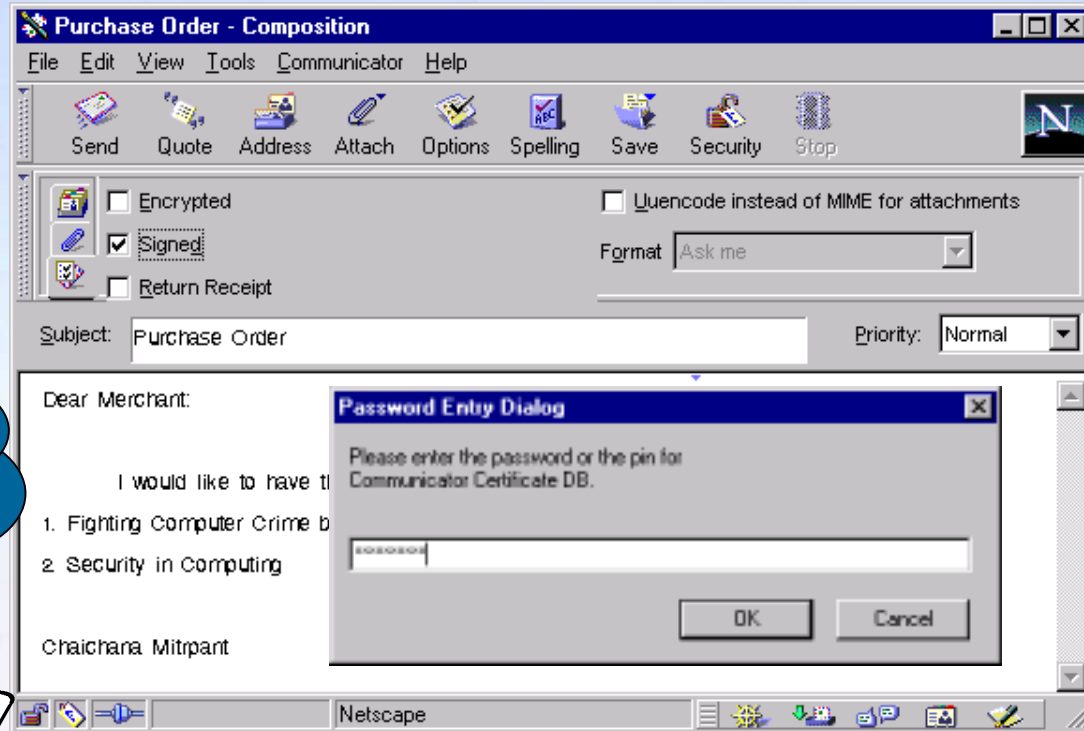
ebay

CNN.com: Tuesday afternoon, the site was crippled from 4:45 to 5:30, when less than 5 percent of users could reach the home page

CNN

Password interception

Now! I know your username and password.



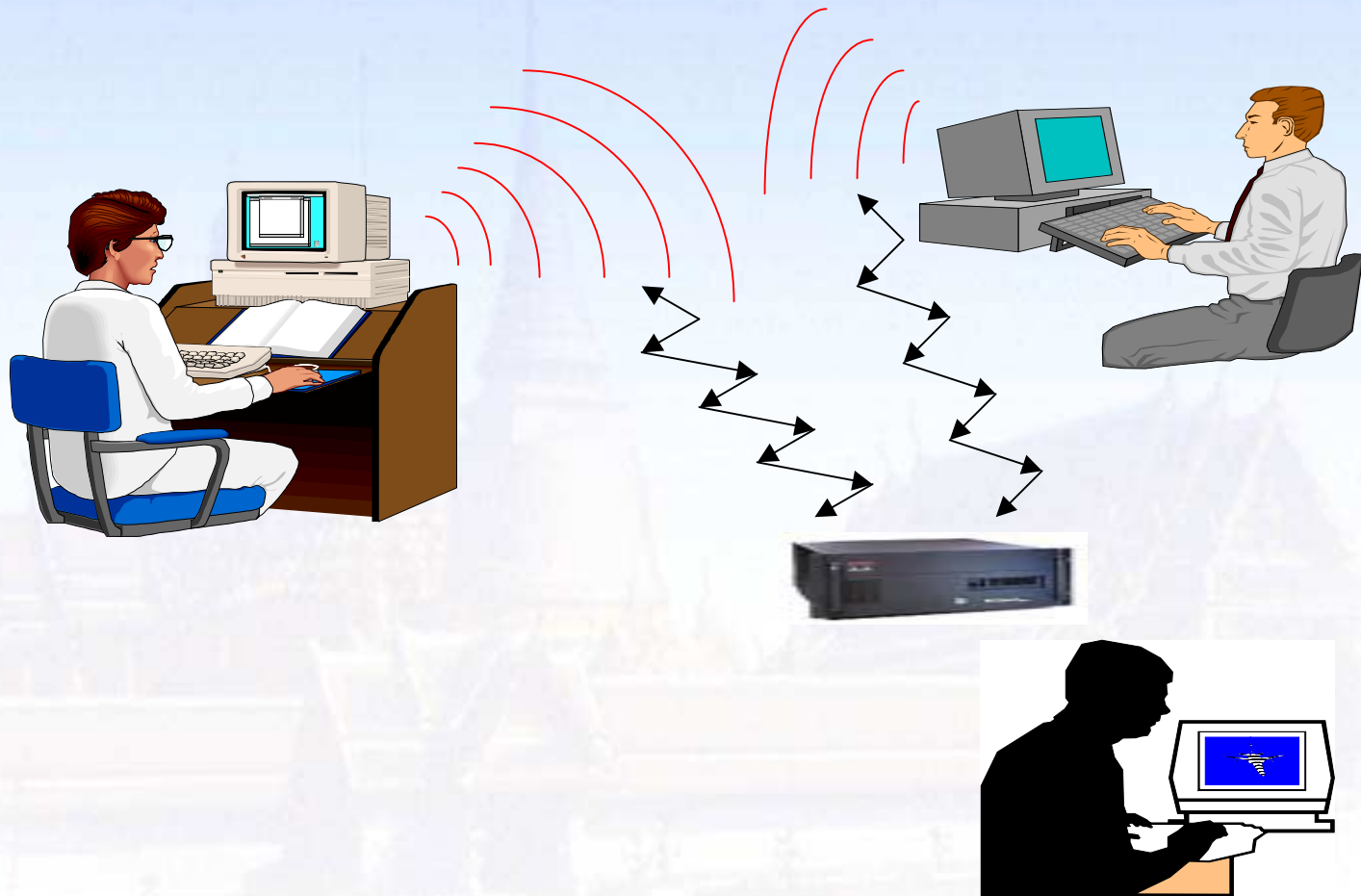
Send the program for intercept password by e-mail



82378161secret password: jozwohsink 172371931 Houston, Texas
www.financialwizard.com 3456192301982 Mary, Riley 756320112
322 Sparky 3847bbx Stan@somewhere/nd 172371931 S. Thompson
August Report/Confidential 78,777
Chapter One 7629382, San Francisco
78" password:mother's maiden name
e-mail address: tarazan@yahoo.
for grandmas famous cookies 984
9834712001-111- Kalamazoo, Pine
Transfer of funds 6/12/99 939231101
grst, 1st quarter Tucker and Brown 83
17231822334 Star.com second chapter
doc/lode/ref/mac 3910-98232
load81206 into forward dom
02938120 date of birth: 9/1
forwarding information c
cable access #665281923
cable access #66528192381123321123 credit number 82378161



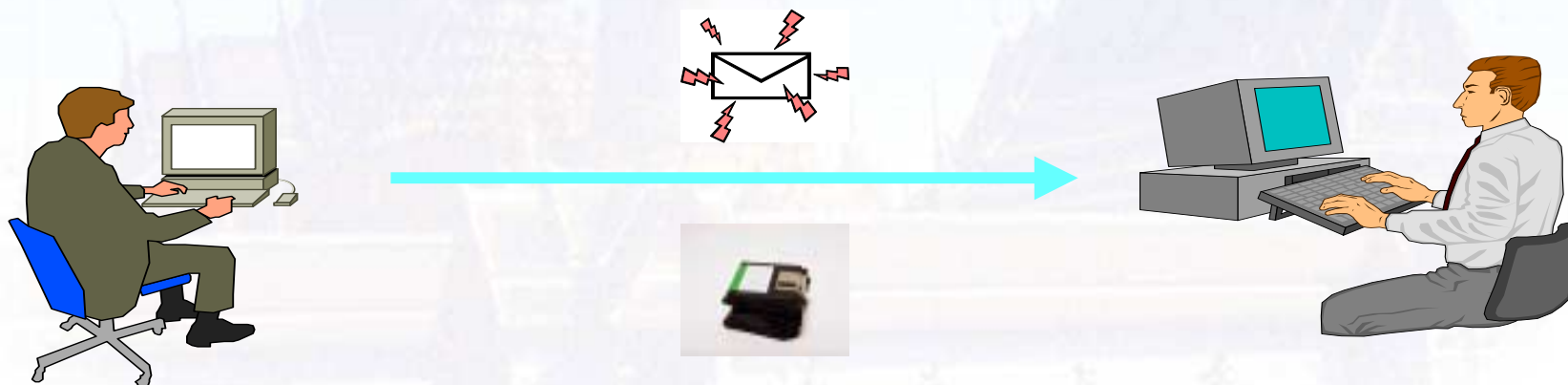
Data Leakage



Trojan Horse



Result : Intruder able to do any thing like authorized person.



Send Malicious Program
by Diskette or e-mail to the target.

Fraud : Salami Techniques



Programmer write a small program to take away a small amount of money (eg. \$0.001) for every transaction that needs rounding...

Control & Secure the information system principles

1. Encryption Techniques



Control & Secure the information system principles

2. Software Controls

- 2.1 Internal Program Controls
- 2.2 Operating System Controls
- 2.3 Development Controls



Control & Secure the information system principles

3. Hardware Controls

Ex. Smart cards, lock key...

4. Policies

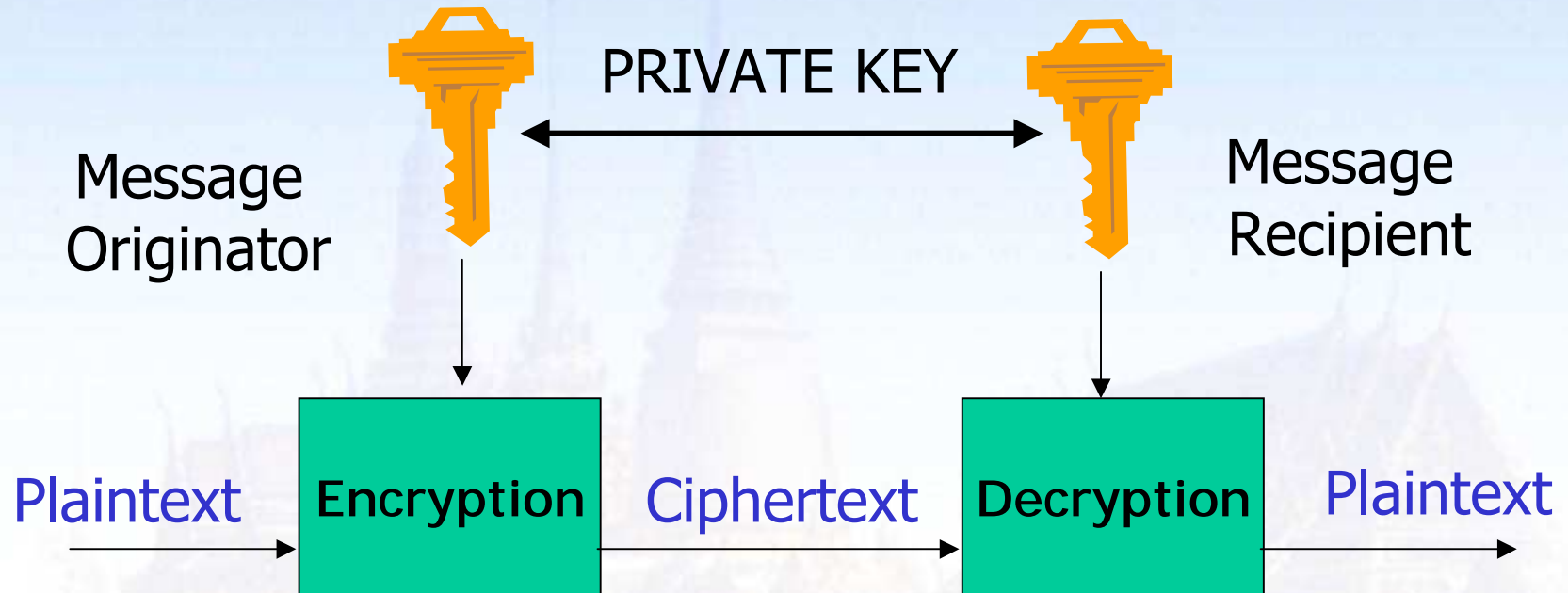
Who are

- entitled to access the system?
- authorized to modification data?
- authorized to recovery ?

5. Physical Control

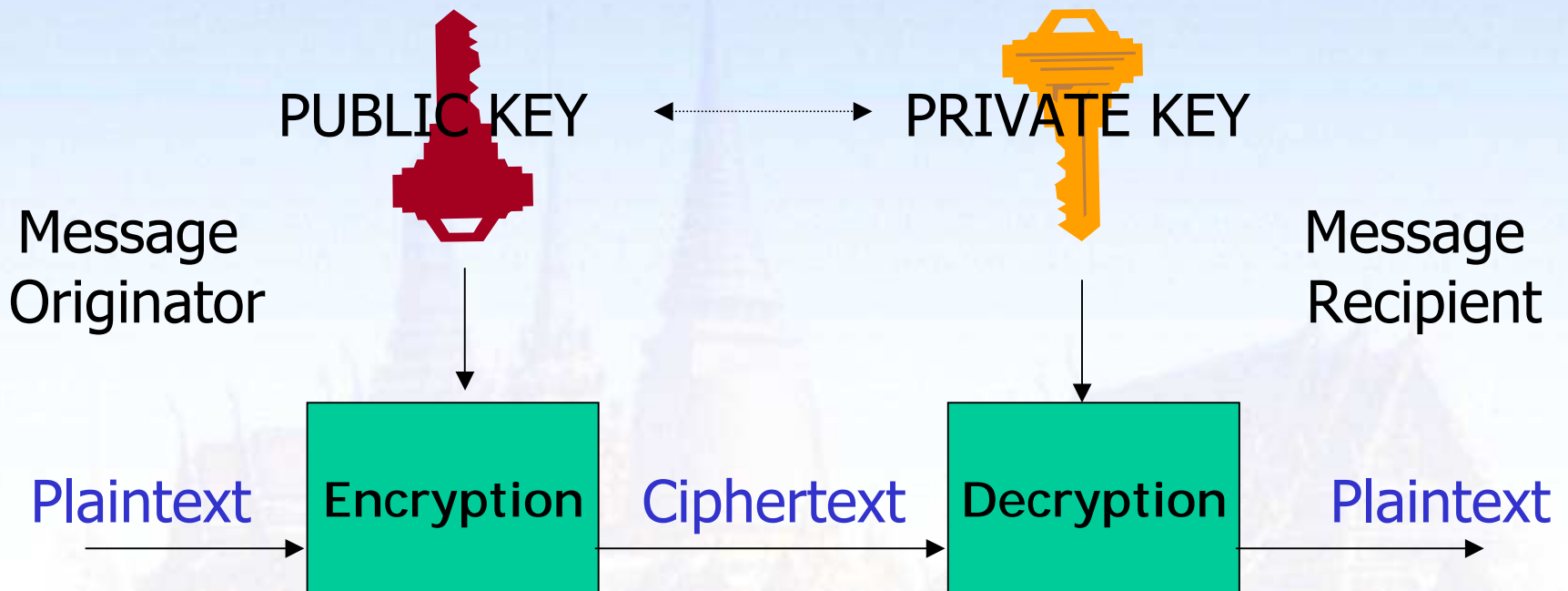


Symmetric Key System



- Same **Private Key** used to encrypt and decrypt
- Security depends on ability to keep key Private
- Need to distribute Key to Recipient

Asymmetric Key System



- Mathematical relationship between **Public** and **Private** Keys assuring that possession of one can not re-create the other
- Public Key used to encrypt while Private Key is used to decrypt
- No need to distribute key to recipient

How to protect your computer system?

Insider attacks

*USER ID,
PASSWORD,
ENCRYPTION,
STAFF CODE OF CONDUCTS,
PRIVACY POLICY..*

Outsider attacks

*Firewall,
Antivirus software,
Router settings,
Server settings,*

...



How to Keep From Getting Hacked

If you're connected to the Internet, you're vulnerable to intruders. But there are ways to keep your data safe.

- 1** Use antivirus software and update it often to keep destructive programs off your computer
- 2** Don't allow online merchants to store your credit-card information for future purchases
- 3** Use a hard-to-guess password that contains a mix of numbers and letters, and change it frequently
- 4** Use different passwords for different Web sites and applications to keep hackers guessing
- 5** Use the most up-to-date version of your Web browser, e-mail software and other programs
- 6** Send credit-card numbers only to secure sites; look for a padlock or key icon at the bottom of the browser
- 7** Confirm the site you're doing business with. Watch your typing; it's amazon.com, not amozon.com.
- 8** Use a security program that gives you control over 'cookies' that send information back to Web sites
- 9** Install firewall software to screen traffic if you use DSL or a cable modem to connect to the Net
- 10** Don't open e-mail attachments unless you know the source of the incoming message

After new viruses, you have to be careful in opening attachments, even from their close friends.

Security Planning

- Policy

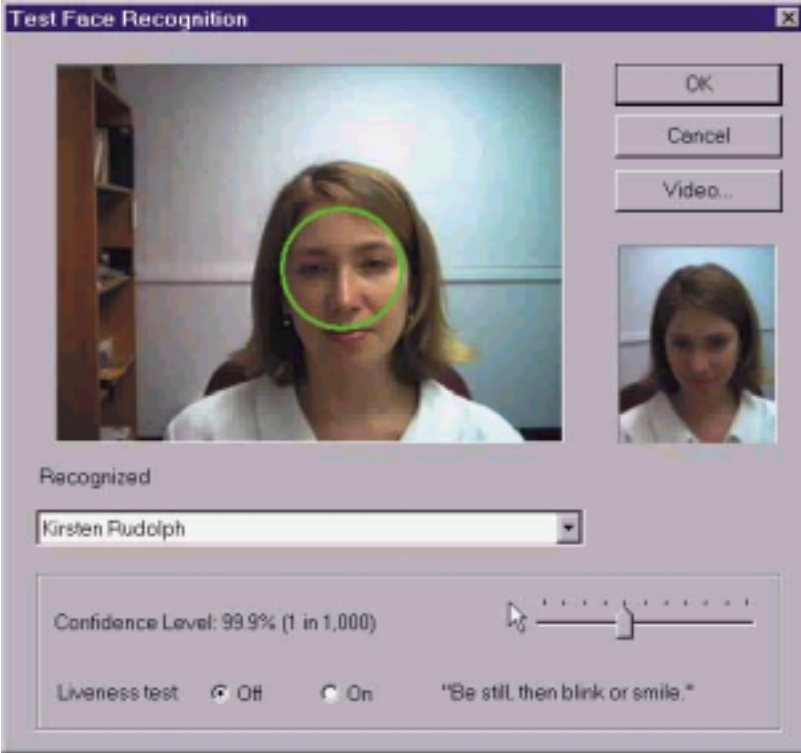
- Who is the operator
- To what resource
- How procedures are enforced



- Current State

- Recommendations and Requirements
- Accountability
- Timetable
- Continuing Attention

Physical Protection



Access Control

Disaster Recovery

1. Disaster from Peril Intention

- Destruction by people
- Unauthorized Usage

2. Natural Disasters

- Flood
- Fire

3. Power Losses

- Use UPS: Uninterrupt Power Supplies
- Use Surge Suppressor for protect disaster from inadequate power

4. Heat

- Use Air Conditioning



www.gocsi.com

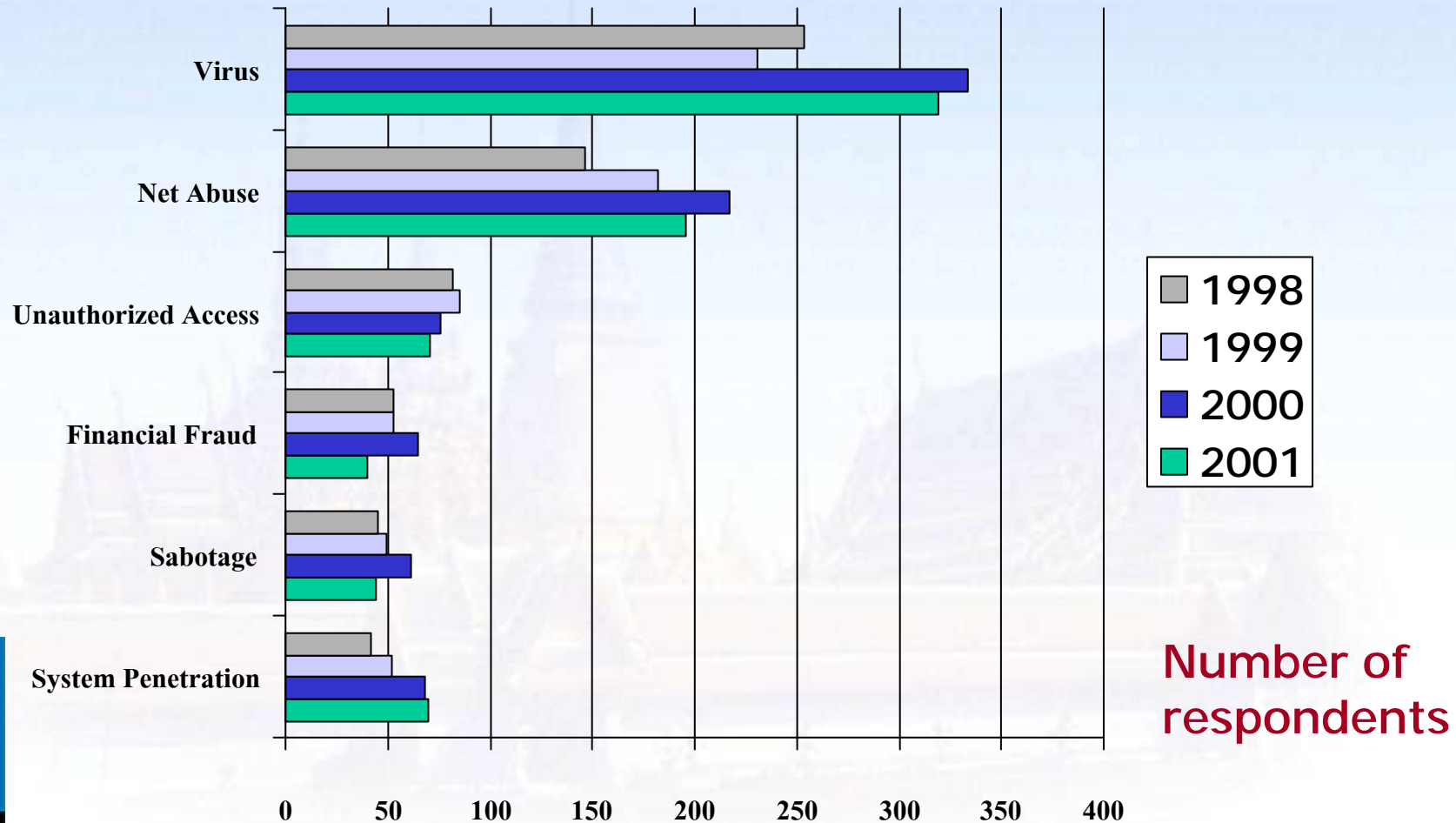
2001 CSI/FBI Computer and Security Survey

Overview of IT Fraud, *Thaweesak Koanantakool*
National Electronics and Computer Technology Center.

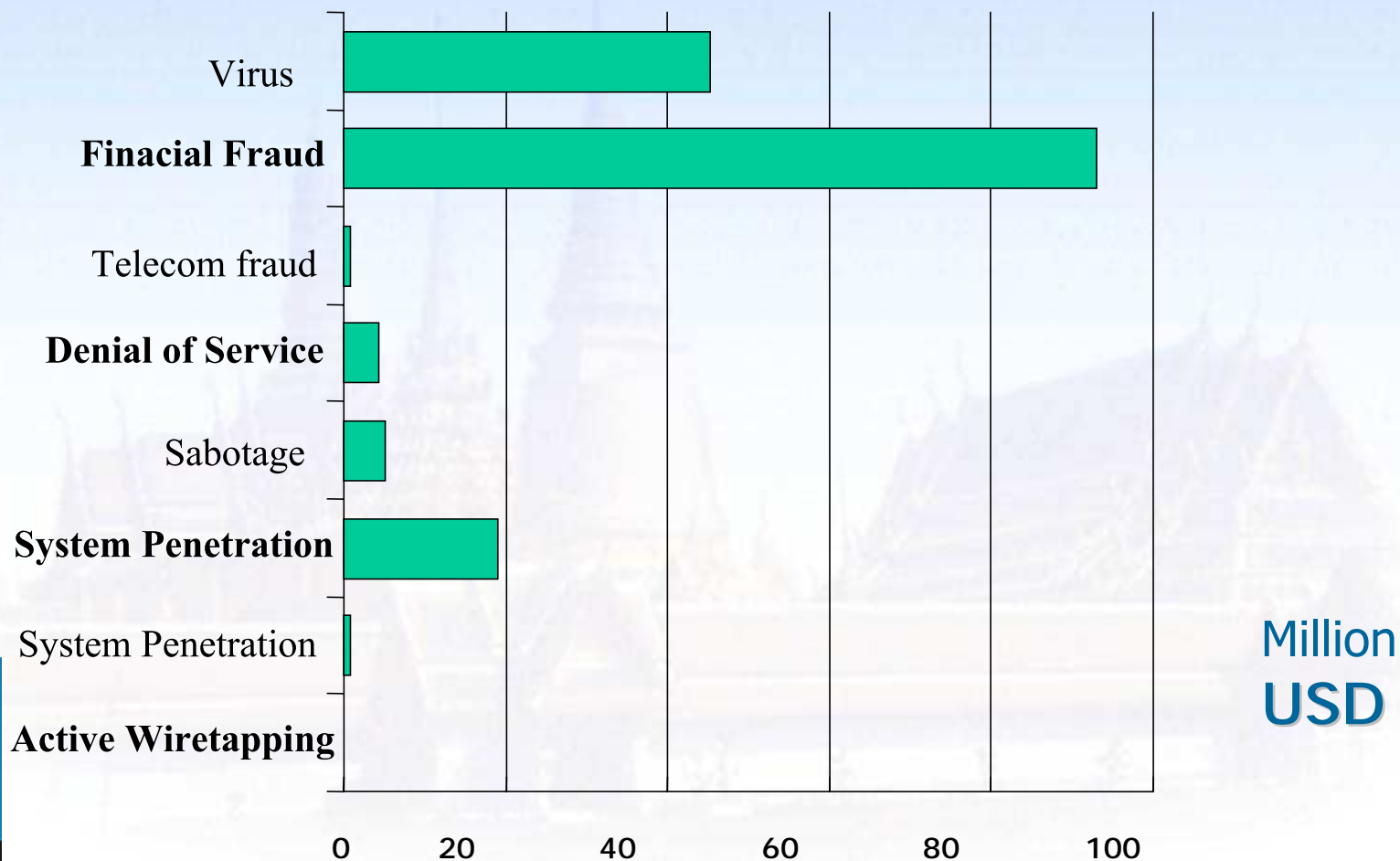


ECTI-21
NECTEC
a member of NSTDA

Financial Losses by Type of Attack or Misuse



Losses / 2001



Million
USD

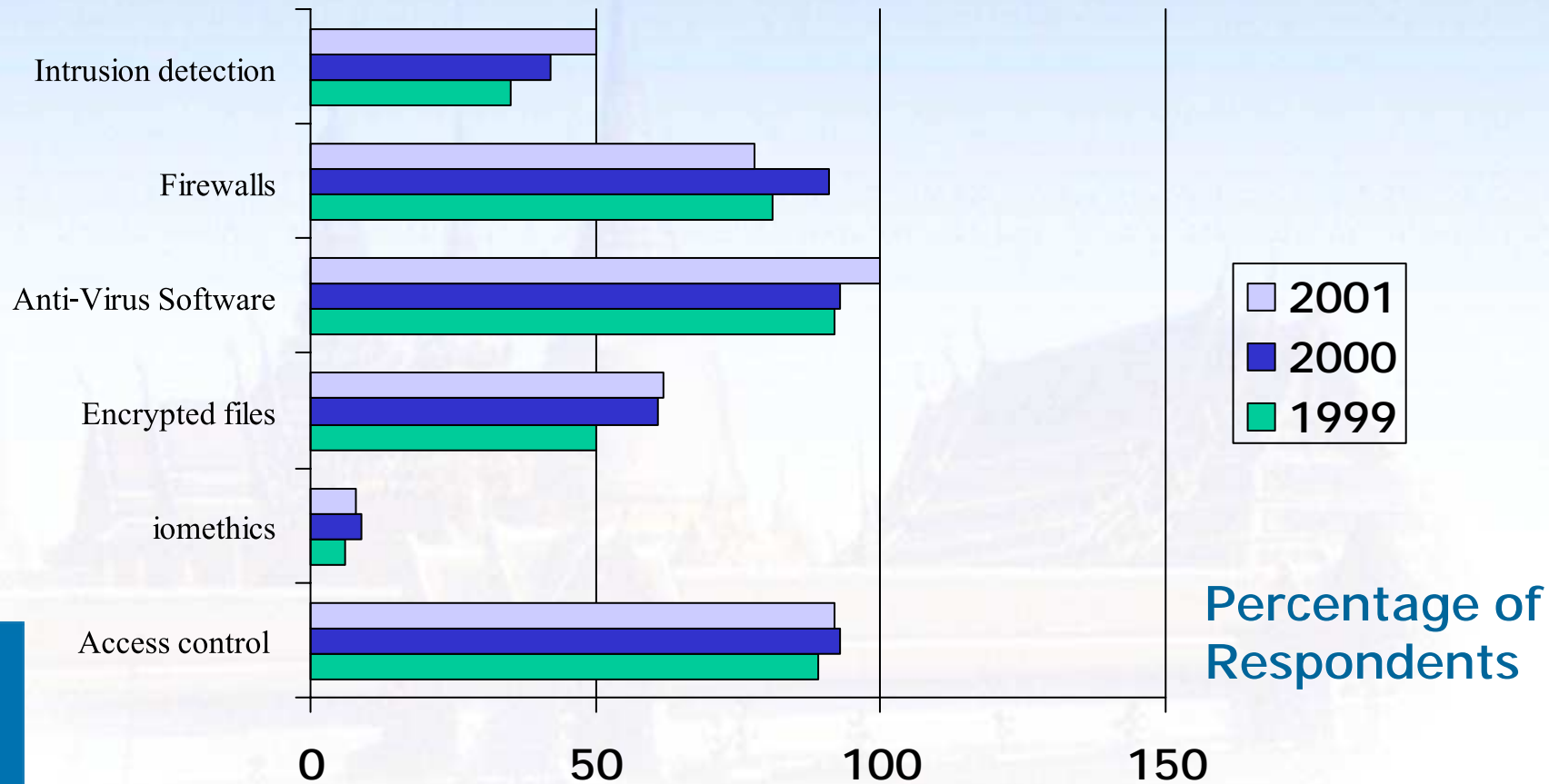


Source: www.gocsi.com

Overview of IT Fraud, *Thaweesak Koanantakool*
National Electronics and Computer Technology Center.



Security technologies used



Percentage of Respondents

IT Laws in Thailand

- Electronic Transactions Act, BE.2544
(Royal Gazette Dec 4, 2001)
[incorporating electronic signature provisions]
- Computer Crime Bill
- Data Protection Bill
- Electronic Funds Transfer Bill
- Credit Card Bill

Convention on Cybercrime

ETS. No. 185

Convention on Cybercrime was opened for signature in Budapest on 23 November 2001.

It is the first ever international treaty on criminal offences committed against or with the help of computer networks such as the Internet.

26 Member States signed the treaty:

Albania, Armenia, Austria, Belgium, Bulgaria, Croatia, Cyprus, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Moldova, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, "the Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom.

Canada, Japan, South Africa and the United States, who took part in the drafting, also signed the treaty too.

Convention on Cybercrime ETS. No. 185

Purposes

1. Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime.
2. Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form
3. Setting up a fast and effective regime of international co-operation

Convention on Cybercrime ETS. No. 185

Offences against the Confidentiality, integrity and availability of computer data and systems (Title 1)

- Illegal Access (Art. 2)
- Illegal Interception (Art. 3)
- Data Interference (Art. 4)
- System Interference (Art. 5)
- Misuse of devices (Art.6)

Convention on Cybercrime ETS. No. 185

Computer -related offences (Title 2)

- Computer-related forgery (Art. 7)
- Computer-related fraud (Art. 8)

Content-related offences (Title 3)

- Offences related to child pornography (Art.9)

Convention on Cybercrime ETS. No. 185

Offences related to infringements of copyright and related right (Title 4)

- Offences related to infringement of copyright and related rights (Art. 10)

Convention on Cybercrime ETS. No. 185

Ancillary liability and sanctions (Title 5)

- Attempt and aiding or abetting (Art. 11)
Corporate liability (14)

Computer Crime law in various countries

ASIA

china : - Computer Information Network and Internet Security, Protection and Management Regulations
- Decree No. 147 of the State Council of the Peoples Republic of China, February 18, 1994. Regulations of The Peoples Republic of China on Protecting the Safety of Computer Information

Hong Kong : Telecommunication Ordinance

India : The Information Technology Act, 2000

Israel : Computer Law 5755-1995

Japan : Unauthorized Computer Access Law

Malaysia : Computer Crime Act 1997

Philippines : Electronic Commerce Act

Singapore : Computer Misuse Act

Computer Crime law in others countries

Belgium, Netherlands : Criminal Code

Denmark, Finland, France, Norway, Poland,

Italy : Penal Code

Luxembourg : The Act of 15th, 1993

Portugal :

Criminal Information law of August 17,1991

Sweden : The Data Act of 1973

United Kingdom : Computer Misuse Act 1990

U.S.A. : Computer Fraud and Abuse Act 1986

Computer Crime Bill of Thailand

Offences against the Confidentiality, integrity and availability of computer data and systems

- Illegal Access (Sec. 6)
- Illegal Interception (Art. 7)
- Data Interference (Art. 8)
- System Interference (Art. 9)
- Illegal..... (Art. 10)
- Misuse of devices (Art.11)

Computer Crime Bill of Thailand

Computer-related offences

- Computer-related forgery (Art. 13)
- Computer-related fraud (Art. 14)

Computer Crime Bill of Thailand

Content-related offences

- Offence related to child pornography (Art. 15)

Statistics of computer crime cases in Singapore

	1997	1998	1999	2000
Hacking	3	5	19	9
Access with intention to commit other offences	4	2	3	1
Unauthorised Use of computer Service	20	101	159	157
Other CMA offences	12	8	10	24
Total	39	116	185	191

Source : CRIMINAL INVESTIGATION DEPARTMENT : Singapore

Overview of IT Fraud, Thaweesak Koahantakool

National Electronics and Computer Technology Center.



a member of NSTDA



เครือข่ายกาญจนาภิเษก
The Golden Jubilee Network
 เติมนားเกียติ
พระบิดาแห่งเทคโนโลยีของไทย
 http://technology.thai.net

โครงการเทคโนโลยีสารสนเทศ ตามพระราชดำริ
 สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี

Thank you.



สวทช. NSTDA

ECTI-21
NECTEC
 National Electronics and Computer Technology Center

ไทยสาร ThaiSarn

SCHOOL NET THAILAND @ 1509

GITs

E-commerce Resource Center

SOFTWARE PARK

E-Thailand

E-Government Project

Internet Thailand

ผลิตภัณฑ์จากกรมฯ สวทช. เนคเทค

In operation: 1 March 1995
 Incorporated: October 1997
 IPO: 14 November 2001

- <http://www.nectec.or.th/users/htk/>

Q & A



Thank you.