Security and Dependability
Issues of the Future Internet

Syed Naqvi

Syed.Naqvi@cetic.be

cetic

Your connection to ICT research

Future Internet Assembly

Introduction

(Current) Internet Security

Some misconceptions

- Login/password is sufficient
- Cryptography is a silver bullet
  - Availability, Denial of Service, …
- No security for non-confidential data
  - Integrity, Availability, …
- Security is a pure technical problem
  - Awareness, Usability, TRUST, …
- Security solutions already exist
  - We only need to assemble them in the right proportion

Security Requirement

- Only one overall security requirement of the Internet:

  The Internet should be SECURE

- Internet had limited scope at the time of its inception in the 1970s
  - Therefore its security requirement was much easier to meet.

- Worldwide web (HTTP protocol) gave boost to the internet-based systems
  - Security provisioning became a crucial factor for the success of this endeavour;
  - Meeting the Internet security requirement started becoming a nontrivial task.

Security Requirements

Confidentiality

Integrity

Availability

Physical Security

Access Control

Traceability

Trust

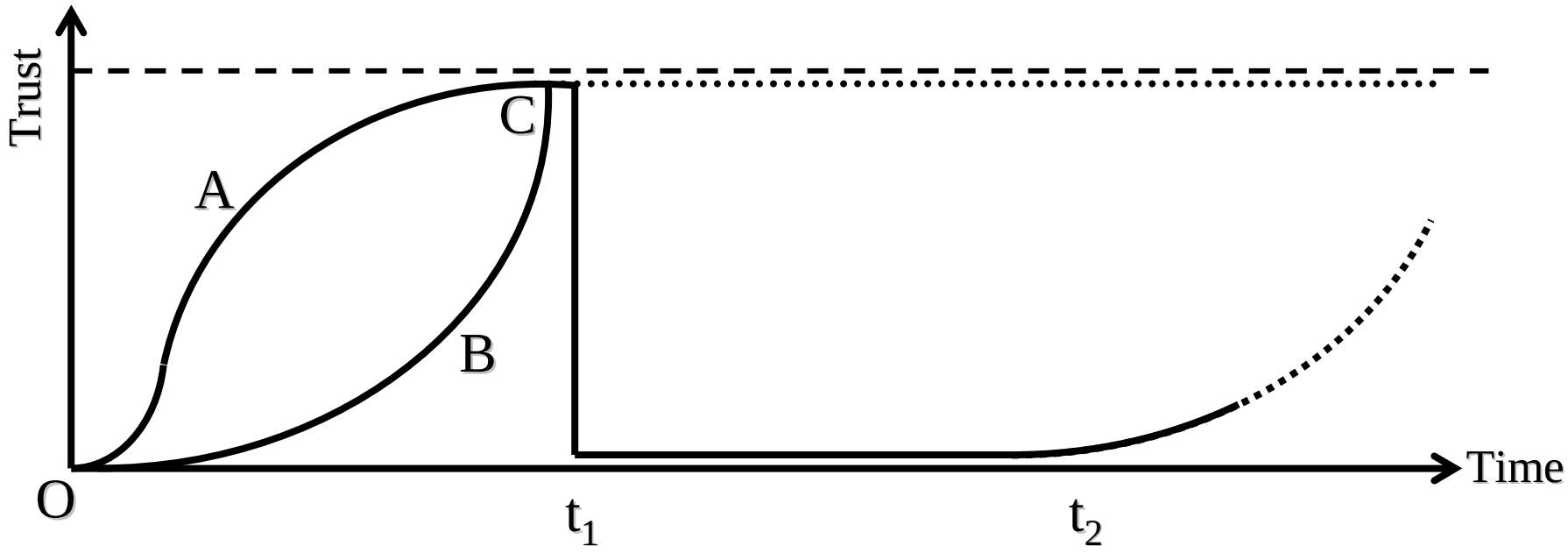
The reliance on a property or a virtue of a person, or the conviction that a given premise is true.

Oxford Dictionary

An entity **A** is considered to trust another entity **B** when entity **A** believes that entity **B** will behave exactly as expected and required.

International Telecommunication Union

Establishing Trust



Security & Trust

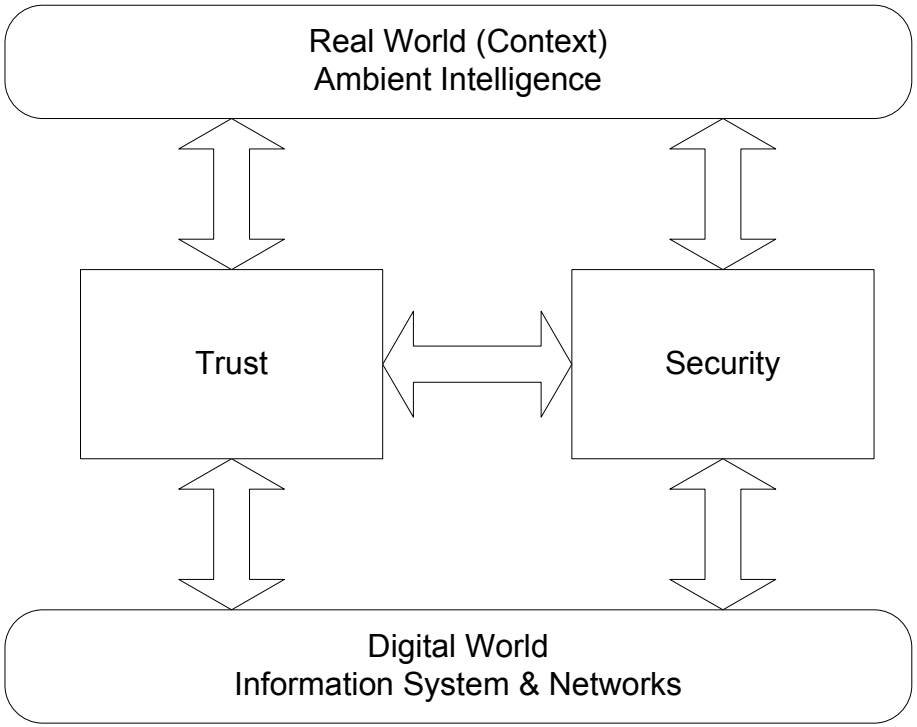


Image source: Michel Riguidel

IDG.net Search All IDG for GO! See More Breaking News

BREAKIN

FTC, hacl

by James
December

A Europea
potential
Netscape
online hor

The spec
Informati
access to
http://ww
similar pa

Although
apparent
the FBI's
of the FB

Security
sites a ta

CNN.com technology > computing

CNN.com EUROPE:
MAINPAGE
EUROPE
WORLD
WEATHER
BUSINESS
SPORTS
TECHNOLOGY
ENTERTAINMENT
IN-DEPTH
NEWS BRIEF

CNN.com:
Sections
change default edition

LOCAL LANGUAGES:
German
Italian
Swedish
Norwegian
Danish
Spanish
Portuguese
Japanese
Chinese Headlines
Korean Headlines

DISCUSSION:
message boards

Editions | myCNN | Video | Audio | News Brief | Fr

Hospital confirms copyin hacker

From...
COMPUTERWORLD
AN IDG.net SITE

December 15, 2000
Web posted at: 2:34 p.m. EST (1934 GMT)

by Marc L. Songini

(IDG) -- A major university hospital in Seattle Thursday confirmed that a hacker penetrated its computer network last summer and made off with files containing information about 5,000 patients

Officials at the University of Washington M
who calls himself "Kane" -- stole user pass
while he had access to the hospital's syster
network through a server in the hospital's p
center CIO Tom Martin.

"The less you give out to the public the better," said Richard Smith, an Internet security consultant based in Brookline, Massachusetts.
"You really don't want these pages to be visible outside the

BBC News in video and audio

Last Updated: Tuesday, 18 February, 2003, 19:30 GMT

Email this to a friend Printable version

Credit card database hacked

A computer hacker has gained access to more than 5 million Visa and Mastercard credit card accounts in the US.


The companies say no actual fraud was committed

The two companies said on Tuesday that none of the information obtained, which would include credit card numbers, was used in a fraudulent way.

But a UK-based business crime expert warned account holders could still be at risk if their cards were not reissued.

Visa and Mastercard said the hacker breached the security system of a company that processes credit card transactions on behalf of merchants.

Numbers of credit cards can be used to make payments, such as buying plane tickets or hiring cars.

> **"The only way to eradicate the risks would be to reissue all 5 million... cards"**
>
> Peter Lilley, business crime expert

Both Visa and Mastercard operate zero liability policies, which protect card holders from having to pay for any unauthorised or fraudulent charges.

Card holders at risk?

Peter Lilley, a fellow of the UK Chartered Institute of Banking and author of various books on hacking and business crime, said some hackers attack computer systems just to prove the point that the system is insecure.

But he told BBC News Online that account holders of the hacked credit cards could still be at risk.

"To gain access to 5 million different accounts is a lot.

defence news

Defence Policy and Business

MOD confirms loss of recruitment data

18 Jan 08

The Ministry of Defence can confirm that a laptop was stolen from a Royal Navy officer in Birmingham last week, on the night of 9/10 January, and as a result, a large quantity of personal data has been lost.

After consultation with West Midlands Police about the impact on the investigation were the theft to become public knowledge, we did not immediately make public the loss of this data. In view of today's media reports, we have, however, decided that it would now be right to do so.

MOD Announcement

The stolen laptop contained personal information relating to some 600,000 people who have either expressed an interest in, or have joined, the Royal Navy, Royal Marines and the Roy Air Force.

The information held is not the same for every individual. In some cases, for casual enquiries, the record is no more than a name. But, fo those who progressed as far as submitting an application to join the Forces, extensive personal data may be held, including passport detai National Insurance numbers, drivers' licence details, family details, doctors' addresses and National Health Service numbers.

The Ministry of Defence is treating the loss of this data with the utmos seriousness. We are writing to some 3,500 people whose bank detail were included on the database. Action has already been taken with th assistance of APACS [Association for Payment Clearing Services] to inform the relevant banks so that the relevant accounts can be flagge for scrutiny against unauthorised access.

The Secretary of State will make a statement to Parliament at the earliest opportunity.

Advice can be sought by emailing 'recruitdata@check.mod.uk'

Man 'finds US troop data' on MP3

A New Zealand man says he found confidential data about US military personnel on an MP3 player he bought from a thrift shop in Oklahoma.

Chris Ogle says he found the files when he went to download music

Chris Ogle, 29, said: "The more I look at it, the more I see and the less I think I should be looking."

The files included names and telephone numbers of American soldiers, according to reports by TV New Zealand.

One expert says the files are unlikely to compromise security, as most of them are from 2005.

Some included a warning that the release of its contents is "prohibited by federal law".

Embarrassment

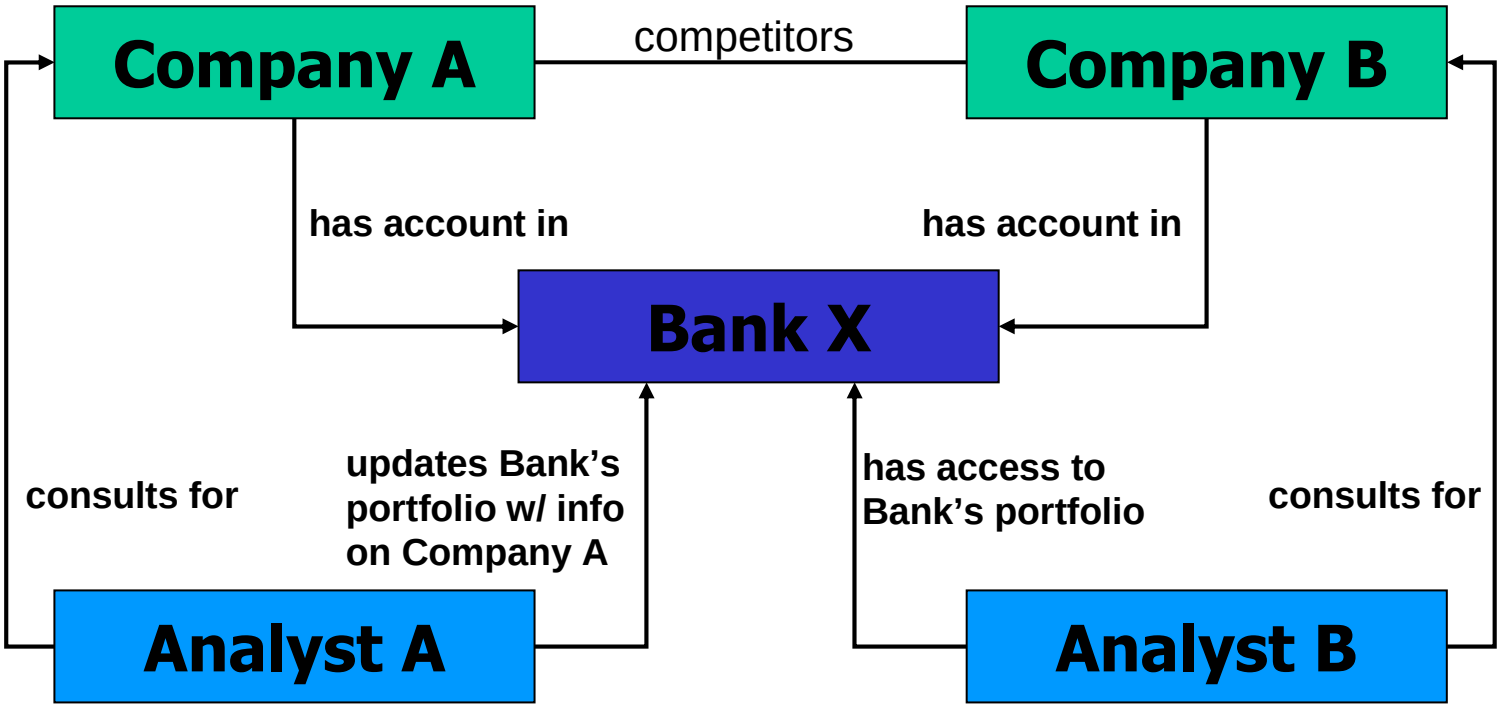
As well as personal details of US soldiers, such as social security numbers, the files also listed pregnant female troops and apparent mission briefings in Afghanistan.

Peter Cozens, director of the Centre for Strategic Studies, New Zealand, said the information should not be in the public domain but it did not appear likely to affect US national security, according to the Associated Press news agency.

"This is just slack administrative procedures which are indeed a cause of embarrassment," he said.

Data Isolation – Multitenancy

Chinese-Wall Model



Cost of Security Lapses

Losses Mount as Security Risks Rise and IT Struggles

A new survey by Symantec of 1000 organizations in the U.S. and Europe highlights the rise in security risks and actual damage done

By James Powell
03/23/2009

Security risks are real and growing, and they'll continue rising for at least the next two years, according to IT security professionals interviewed for Symantec's recent report, *Managed Security in the Enterprise*. Other key findings of the survey of IT security risks, challenges, and strategies: managers say it's getting harder for them to provide effective IT security because of increased regulatory pressures, a smaller budget, and problems finding and hiring qualified staff.

Organizations reported increased threats (a theoretical risk) and a rise in *actual attacks* in the last two years; respondents expect the trend to continue in the next two. Actual losses (including lost revenue and lost staff productivity) were reported by virtually all (98 percent) enterprises surveyed. In fact, 88 percent of U.S. organizations reported being attacked in the last two years, of which 42 percent saw attacks on a regular basis.

That validates other Symantec findings according to Grant Geyer, vice president of managed services at the firm. Geyer told *Enterprise Strategies* that the company's Internet Security Threat Report showed a significant rise is malicious code, especially in bot networks. "That 72 percent said malicious code events were increasing is no surprise. The problem is that IT is finding that anti-virus programs alone aren't enough to combat the problem. Today's malware works in difficult-to-detect stealth mode, attacking in a number of vectors, from e-mail and unpatched systems to the USB drive you plug into your system."

Geyer fears that when one-third (33 percent) of respondents say they have experienced internal malicious attacks when data leaves the network, these experts are seriously underestimating the problem. "From our customer profiles, we know that there is a

Related Articles

- IT Budget Strategies: Doing More with Less
- Best Practices for Data Governance in SharePoint Environments
- System Failure Case Study: Replicating the Old in New Systems
- Q&A: Squeezing More Out of Your IT Environment
- Five Virtualization Best Practices That Can Transform Enterprise IT

Measuring Loss

Estimating Potentia IT Security Losses

An Alternative Quantitative Approach

In a highly network-centric open economy, network-based information plays a pivotal role in all business firms and institutional organizations. The authors have developed a novel model for implementing quantitative measurement of possible IT security losses by mining records of port-scan data.

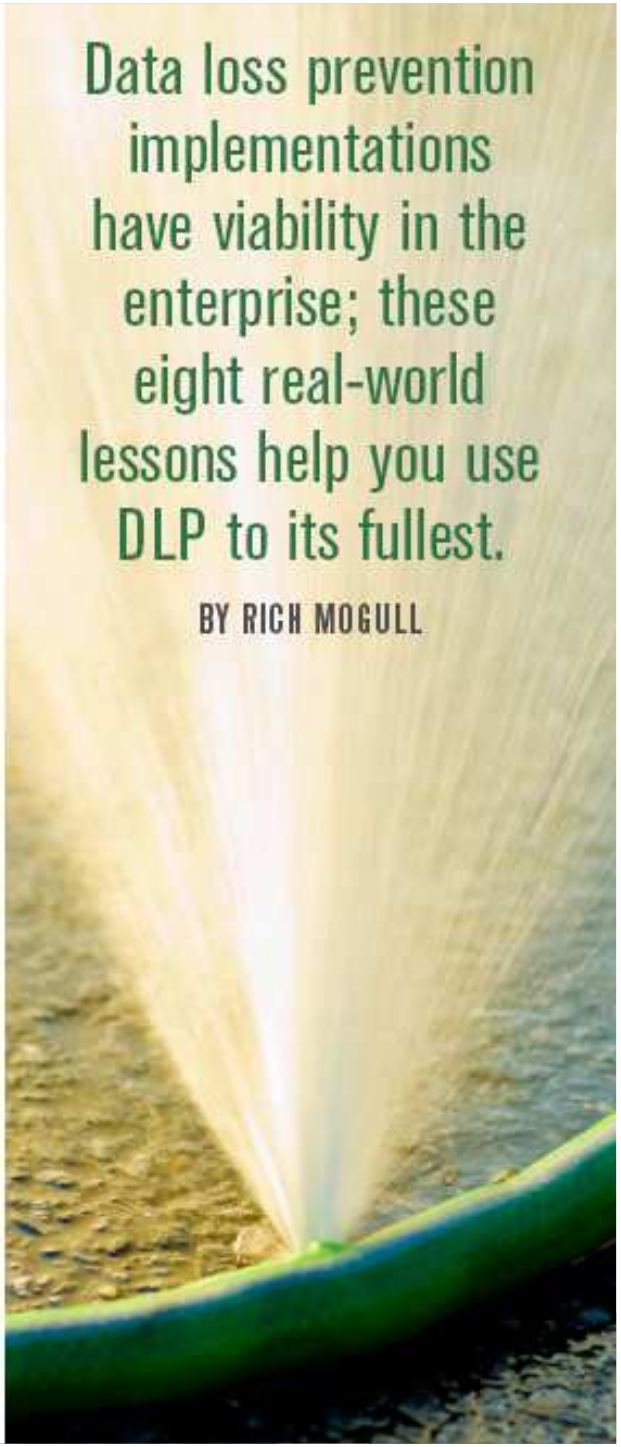
VINCENT C.S. LEE AND LINYI SHAO
Monash University

In today's competitive market environment, the effective use of business information systems is becoming a key success factor for most organizations. Although effective use of such systems brings great benefits, it also creates operational challenges, such as in-

breaches. IT lite
ature posits tha
security project
should be evalu
"investment" cr

Data loss prevention implementations have viability in the enterprise; these eight real-world lessons help you use DLP to its fullest.

BY RICH MOGULL



Crime Costs Business

2nd July 2009

Following last year's British survey and considering the soars, Chambers of Comme further research into the in surveying almost 500 busin

Almost half of the business centred on physical damag demonstrably less common

The findings demonstrate England is burglary (33%),

The most commonly report crime to business in the pa

The survey also demonstra of crime against businesses particularly high levels of cr 45 per cent of incidents.

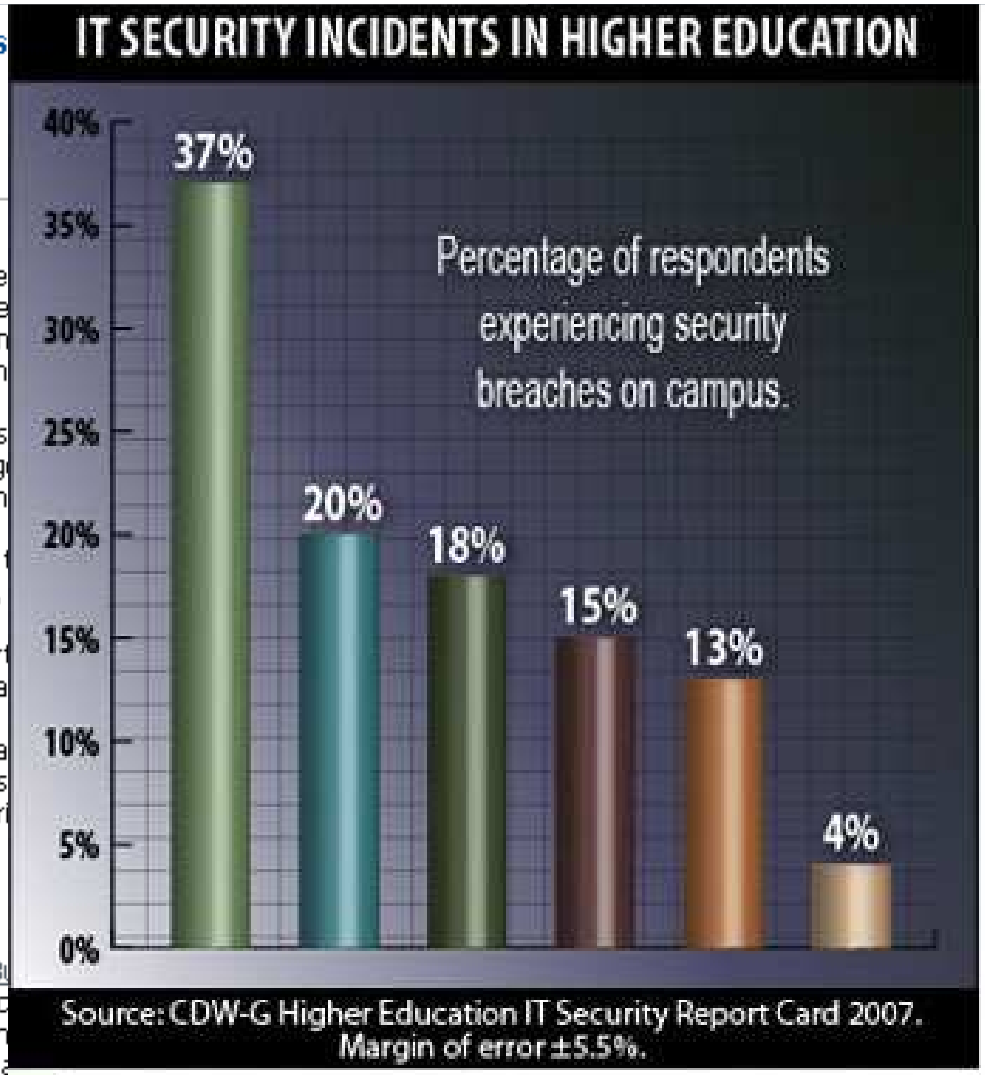
Almost 20% of businesses

Peter Jones, Manager of Bu understand the nature and crime-specific actions are in monitoring business crime a

"Business areas should be p with local businesses and t on business crime. They sh likely to occur."

Businesses are investing he security annually. Over 30%

Peter continued: "Business neighbours. Innovative way



osts $67 billion, FBI says

-MAIL WORTHWHILE? 0 VOTES 0

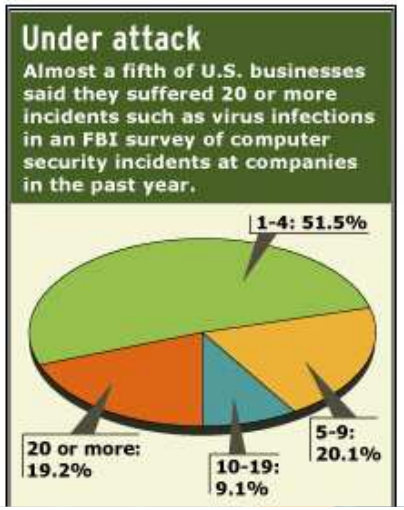
:00 PM

eft and other computer-related ering $67.2 billion a year,

apolating results from a survey of sed Thursday, found that 1,324 financial loss from computer security

re than $24,000, with the total cost l.

ecause poll respondents are more ienced a problem. So, when mate the national cost, the FBI ted organizations from 64 percent to



E-mail this to a friend Printable version

US energy sites tighten security

By Barnie Choudhury
BBC correspondent in Washington

Energy facilities in the US have been told to halt operations that use the type of computer discs missing from the Los Alamos nuclear weapons laboratory.

Los Alamos has suffered other security lapses

Nineteen employees of the New Mexico centre have been suspended while the FBI probes a security breach there.

They were called in after two storage devices disappeared from the top secret laboratory jus over two weeks ago.

The discs are thought to hold classified information, possibly containing nuclear secrets.

An investigation and comprehensive review of security is currently taking place and has shut down all work at the key installation.

Embarrassment

The US Energy Secretary, Spencer Abraham, has ordered work to be stopped at all departments that use the of kind of devices that are missing.

Almost 8,000 people are employed at the lab and managers are having face-to-face meetin with them to make sure their security and safety training are up-to-date.

This is the latest in a long line of security breaches at the installation, that have include

Los Alamos hea amid allegation


Los Alamos: Centre of US nuclea

The head of the Los Alamos Laboratory has resigned, fo of theft and fraud at the la first atomic bomb was deve

John Browne, a physicist who became the laboratory's director in 1997, will step down on Monday.

The Federal Bureau of Investigation and the Department of Energy are looking into allegedly questionable purchases and the disappearance of computers and other equipment from the complex in the state of New Mexico.

A spokesman for the University of California – wh laboratory – said the resign decision" by Mr Browne and gave no further details.

E-mail this to a friend Printable version

US nuclear chief forced to quit

US nuclear weapons agency chief Linton Brooks has been made to resign following a number of security breaches at Los Alamos Laboratory.


Linton Brooks became head of the agency in 2003

US Energy Secretary Samuel Bodman said new leadership at the National Nuclear Security Administration was needed.

"These management and security issues can have serious implications for the security of the US," Mr Bodman added.

The NNSA is in charge of maintaining the country's nuclear weapons stockpile and reducing the threat posed by WMDs.

The agency was created in 2000 after an espionage scandal at Los Alamos, site of US nuclear weapons research.

Mr Brooks became head of the agency in 2003 – two security lapses are known to have happened during his leadership.

In June last year, it emerged that a security breach which led to the theft of files containing information on more than 1,000 workers, had gone unreported for months.

Four months later, classified documents were found during a drugs raid on the home of a former Los Alamos employee.

Mr Brooks said in a statement he accepted the decision to remove him although "it was not a decision that I would have preferred".

"Our task is now to minimise the inevitable disruption of such a transition and to continue the vital national security work on which we are engaged," his statement added.

Mr Brooks is expected to leave the agency by the end of the month.

So what is the state of Internet security today ?


TOYOTA
KOMATSU

Future Internet
Security and Dependability

Dependability Metrics

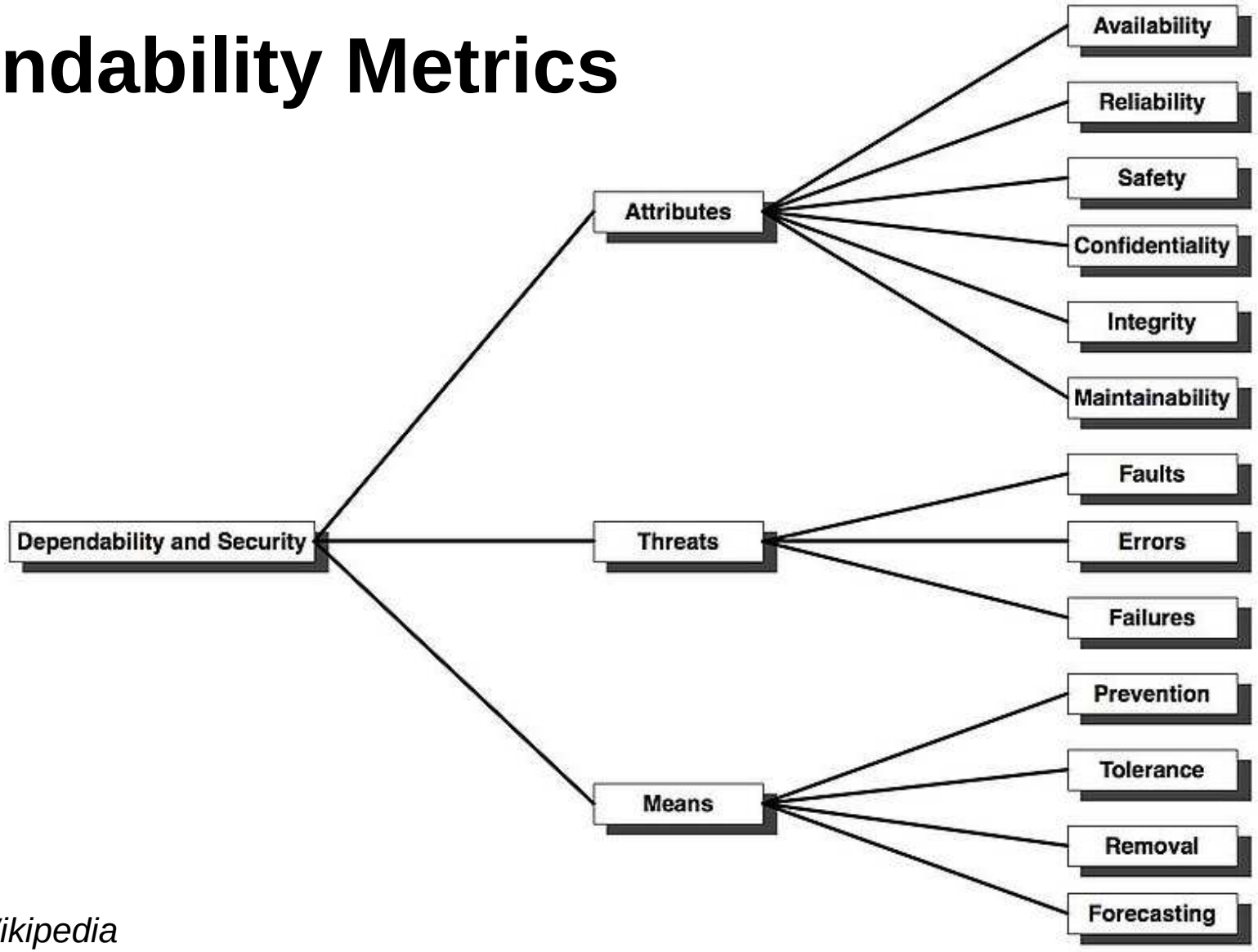


Image source: Wikipedia

E-mail this to a friend Printable

Criminals 'may overwhelm t

By Tim Weber
Business editor, BBC News website, Davos

Criminals controlling millions of personal computers are threatening the internet's future, experts have warned.

Do you know
taken over b

Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets, said Vint Cerf, one of the fathers of the internet.

Technology writer John Markoff said: "It's as bad as you can imagine, it pu
internet at risk."

The panel of leading experts was discussin
internet at the World Economic Forum in D

Internet pandemic

Mr Cerf, who is one of the co-developers c
standard that underlies all internet traffic a
Google, likened the spread of botnets to a

Of the 600 million computers currently on t
between 100 and 150 million were already
botnets, Mr Cerf said.

Botnets are made up of large numbers of computers that malicious hackers have brought under their control after infecting them with so-called Trojan virus programs.

> **Despit**
> **is still wor**
> **pretty am**
> **resilient**
>
> Vint Cerf

› **Cracking**

While most owners are oblivious to the infection, the networks of
of computers are used to launch spam e-m
denial-of-service attacks or online fraud sc

What will frighten us next year?

Kate Bevan
The Guardian, Thursday 11 December 2008
Article history

Online threats could be as scary as Ben Affleck's experience in the film Paycheck

Apart from terrorism, the growth of our waistlines after Christmas, the credit crunch and its effect on our jobs and wallets, you mean? There are going to be plenty of things online to fret about, say internet security companies.

Top of the list of scary things is cloud computing, claim security providers Websense and Lumension. They reckon that the cloud - where software and data is held on servers owned by a third-party provider such as Microsoft Azure or Amazon Web Services - gives the bad guys more opportunities to steal sensitive data and trade secrets.

A total of 61% of those responding to Lumension's survey said they were

A larger | smaller

Technology
Cloud computing · Microsoft · Amazon.com · Hi-tech crime · Data and computer security · Data protection

Breach of Privacy is irreparable now!

October 19, 2008 -- Updated 1156 GMT (1956 HKT)

Official: Sarkozy's bank account hacked by thieves

STORY HIGHLIGHTS
- French media: Thie
- Media: Sarkozy repo
- French Cabinet spo

Next Article in World

TEXT SIZE

PARIS, France (AP) -- The French Cabinet's spokesman says "swindlers" have broken into the personal bank account of President Nicolas Sarkozy.

French President Nicolas Sarkozy reported the theft from his account last month, say media.

Spokesman Luc Chatel told France's Radio-J an investigation is under way and insists the incident "proves that this system of checking (bank accounts) via the Internet isn't infallible." He did not elaborate.

Weekly Journal du Dimanche reported Sunday that thieves seized Sarkozy's bank account information and swiped small sums of money.

The newspaper said Sarkozy reported the theft last month and that those responsible haven't been found. The report cited an unnamed official close to the investigation for its information.

The press service for Sarkozy's office declined comment. E-mail to a friend | Mixx it | Share

E-mail this to a friend

Holes found in Wolfowit

World Bank President Paul Wolfowitz may be dedicated to freeing the world from poverty - but he seems unable to afford a new pair of socks.

Mr Wolfowitz's sartorial deficiencies were revealed when he took his shoes off while visiting a mosque in Edirne, western Turkey.

Both of the grey socks sported holes with his big toes peeking throu

The last World Bank annual report, f president's salary as of 1 July, 2005

Shelter

Mr Wolfowitz was in Turkey on a tw meeting with Prime Minister Reycep

Mr Wolfowitz strongly backs Turkey' Union.

On his trip he also met homeless me who are being helped by a World Ba

In an earlier sartorial foray in the me film Fahrenheit 9/11, Mr Wolfowitz w comb before running it through his h appearance.

Clean Slate Approach for FI Security

- Identity Management
- Trust and Reputation
- Access Control and Data Protection
- Trusted Computing
- Security Analysis
  - Steganalysis
- Security Audit

Work in Progress

Security Audit Example

- **Payment Card Industry Data Security Standard (PCI DSS)**
- Security Audit Procedures
  - Requires audit of the physical controls

PCI Security Standards Council

Requirement 9: Restrict physical access to cardholder data.

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted.

PCI DSS REQUIREMENTS	TESTING PROCEDURES	IN PLACE	NOT IN PLACE	TARGET DATE/ COMMENTS
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems that store, process, or transmit cardholder data.	**9.1** Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems that contain cardholder data • Verify that access is controlled with badge readers and other devices including authorized badges and lock and key • Observe a system administrator's attempt to log into consoles for three randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use			
9.1.1 Use cameras to monitor sensitive areas. Audit collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	**9.1.1** Verify that video cameras monitor the entry/exit points of data centers where cardholder data is stored or present. Video cameras should be internal to the data center or otherwise protected from tampering or disabling. Verify that cameras are monitored and that data from cameras is stored for at least three months			
9.1.2 Restrict physical access to publicly accessible network jacks	**9.1.2** Verify by interviewing network administrators and by observation that network jacks are enabled only when needed by authorized employees. For example, conference rooms used to host visitors should not have network ports enabled with DHCP. Alternatively, verify that visitors are escorted at all times in areas with active network jacks			
9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices	**9.1.3** Verify that physical access to wireless access points, gateways, and handheld devices is appropriately restricted			
9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. *"Employee" refers to full-time and part-time employees, temporary*	**9.2.a** Review processes and procedures for assigning badges to employees, contractors, and visitors, and verify these processes include the following: • Procedures in place for granting new badges, changing access requirements, and revoking terminated employee and expired visitor badges • Limited access to badge system			

Security Audit Scenario

- **Payment Card Industry Data Security Standard (PCI DSS)**
- Security Audit Procedures
  - Requires audit of the physical controls
  - Generic monitoring tools:
    - Hardware monitoring
      - HP Insight Manager, Dell Open Manage, VMWare Virtual Center, …
    - Performance monitoring
      - VizionCore, Veeam Monitor, Vmtree, Nagios, …
    - Machine state monitoring
      - Virtualshield, Logcheck, …
    - Security monitoring
      - Intrusion detection, honeypots, …

Security Audit Scenario

- These tools may not be suitable for security audit controls of “Virtualization Infrastructures”
  - Physical controls can be distributed
    - Onsite checks by the local controllers
  - There maybe a new set of matrices
    - For the measurement of security strength
  - Set of new regulations/legislations for the cross-border deployment of resources
    - Like trade and commerce agreements
  - New models for checkpointing
    - With more reliable matrices

- **Virtualization is not the antonym of Security Audit!**

Only Technical Approach is not sufficient

- Public awareness is crucial for the success
- Usability and ergonomics is essential
- Legal and judicial issues need to be resolved
- …

Page last updated at 10:34 GMT, Sunday, 5 July 2009 11:34 UK

E-mail this to a friend Printable version

MI6 boss in Facebook entry ro

Personal details about the life of the next head of MI6, Sir John Sawers, have been removed from social networking site Facebook amid security concerns.

The Mail on Sunday said his wife had put details about their children and the location of their flat on the site.

Sir John Sawers is currently t
the United Nat

She had not imposed privacy protection on her account allowing any of Facebook's 200 million users in the open-access "London" network to see the entries, it added.

had b
imsuit

Unite

ook in
s, incl

Mercer
t possible
risks

00.00 / 01.16 SHA

couple and the whereabouts of their three grown-up children and of Sir John's parents, the paper said.

Page last updated at 08:27 GMT, Wednesday, 3 June 2009 09:27 UK

E-mail this to a friend Printable version

US in nuclear disclosure blunder

A document providing confidential details of US civilian nuclear sites was accidentally posted on the internet, the government has admitted.

The Los Alamos facility in New Mexico was one of those detailed

The 266-page document included the precise location of stockpiles of fuel for nuclear weapons, the Obama administration said.

The Government Printing Office website took down the posting on Tuesday after experts expressed concern.

US officials insisted the information detailed was not a security threat.

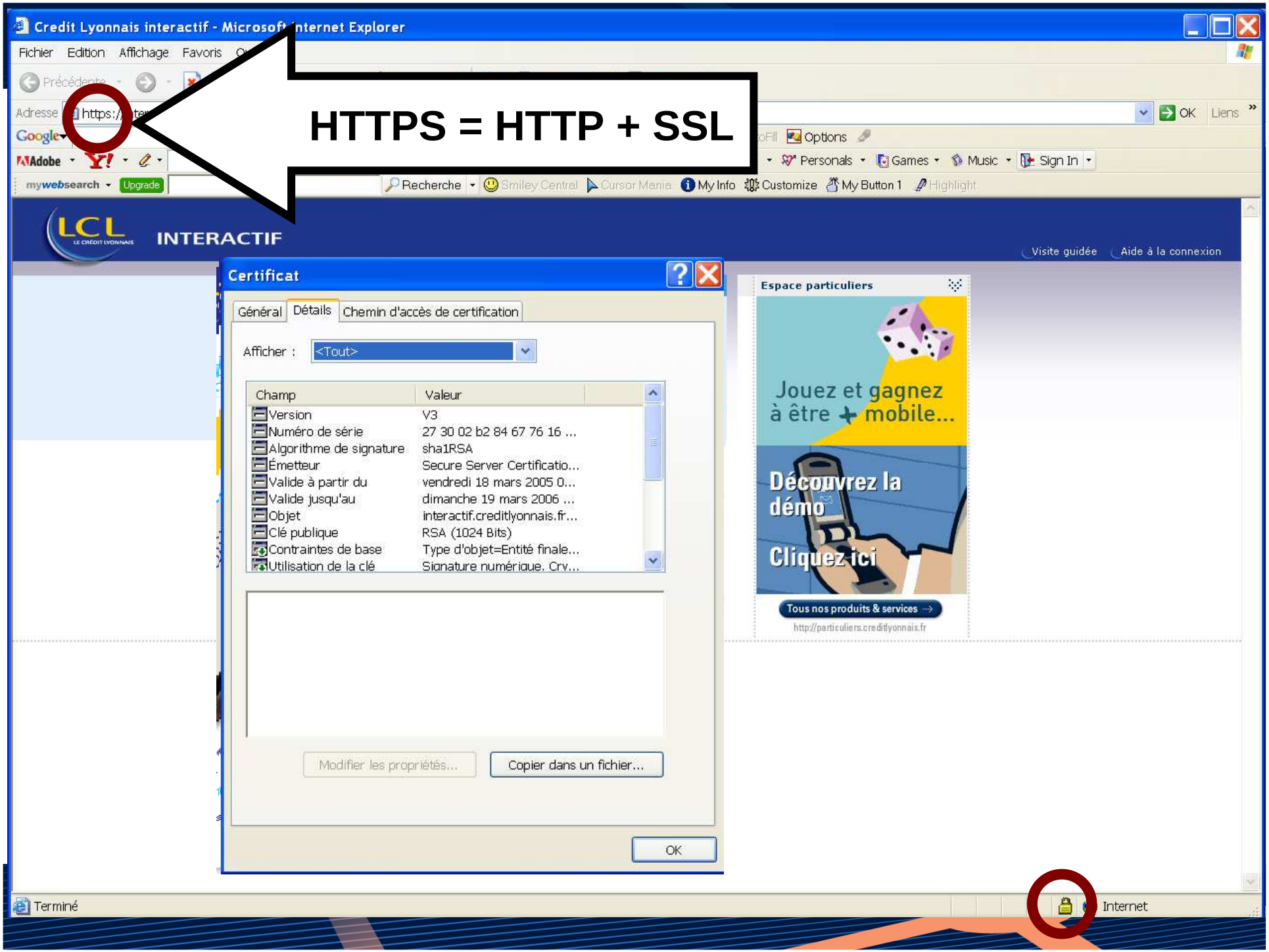
The document, which lists itself as "sensitive but unclassified", contains maps and information on hundreds of US civilian nuclear sites.

No military installations are included but the document does cover the nuclear weapons laboratories at Los Alamos, Livermore and Sandia.

Enriched uranium

An internet site of the Federation of American Scientists in Washington had highlighted the document's existence on Sunday, saying it was "a one-stop shop for information on US nuclear programs".

A spokesman for the printing office told the New York Times the document had been gathered "under normal operating procedures"


Credit Lyonnais interactif - Microsoft Internet Explorer
Fichier Edition Affichage Favoris
HTTPS = HTTP + SSL
LCL
INTERACTIF
Visite guidée
Aide à la connexion
Certificat
Général
Détails
Chemin d'accès de certification
Afficher :
<Tout>
Champ
Valeur
Version
V3
Numéro de série
27 30 02 b2 84 67 76 16 ...
Algorithme de signature
sha1RSA
Émetteur
Secure Server Certificatio...
Valide à partir du
vendredi 18 mars 2005 0...
Valide jusqu'au
dimanche 19 mars 2006 ...
Objet
interactif.creditlyonnais.fr...
Clé publique
RSA (1024 Bits)
Contraintes de base
Type d'objet=Entité finale...
Utilisation de la clé
Signature numérique, Crv...
Modifier les propriétés...
Copier dans un fichier...
OK
Espace particuliers
Jouez et gagnez à être + mobile...
Découvrez la démo
Cliquez ici
Tous nos produits & services
http://particuliers.creditlyonnais.fr
Terminé
Internet

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
In Pictures
Country Profiles
Special Reports

Related BBC sites
Sport
Weather
On This Day
Editors' Blog
BBC World Service

Site Version
UK Version

Page last updated at 02:30 GMT, Thursday, 9 April 2009 03:30 UK

E-mail this to a friend Printable version

Spies 'infiltrate US power grid'

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

The US government has admitted the nation's power grid is vulnerable to cyber attack, following reports it has been infiltrated by foreign spies.

Security experts say the technology protecting the grid has not kept pace

The Wall Street Journal (WSJ) newspaper reported that Chinese and Russian spies were behind this "pervasive" breach.

It said software had been left behind that could shut down the electric grid.

"The vulnerability is something [we] have known about for years," said US Homeland Security Secretary Janet Napolitano.

"We acknowledge that... in this world, in an increasingly cyber world, these are increasing risks," Ms Napolitano added.

She refused to comment on the WSJ story that an intrusion had taken place, but security experts said they were not surprised by the claims.

"There is a pretty strong consensus in the security community that the SCADA equipment, a class of technology that is used to manage critical infrastructure, has not kept pace with the rest of the industry," said Dan Kaminsky, a cyber security analyst and director of penetration testing for IOActive.

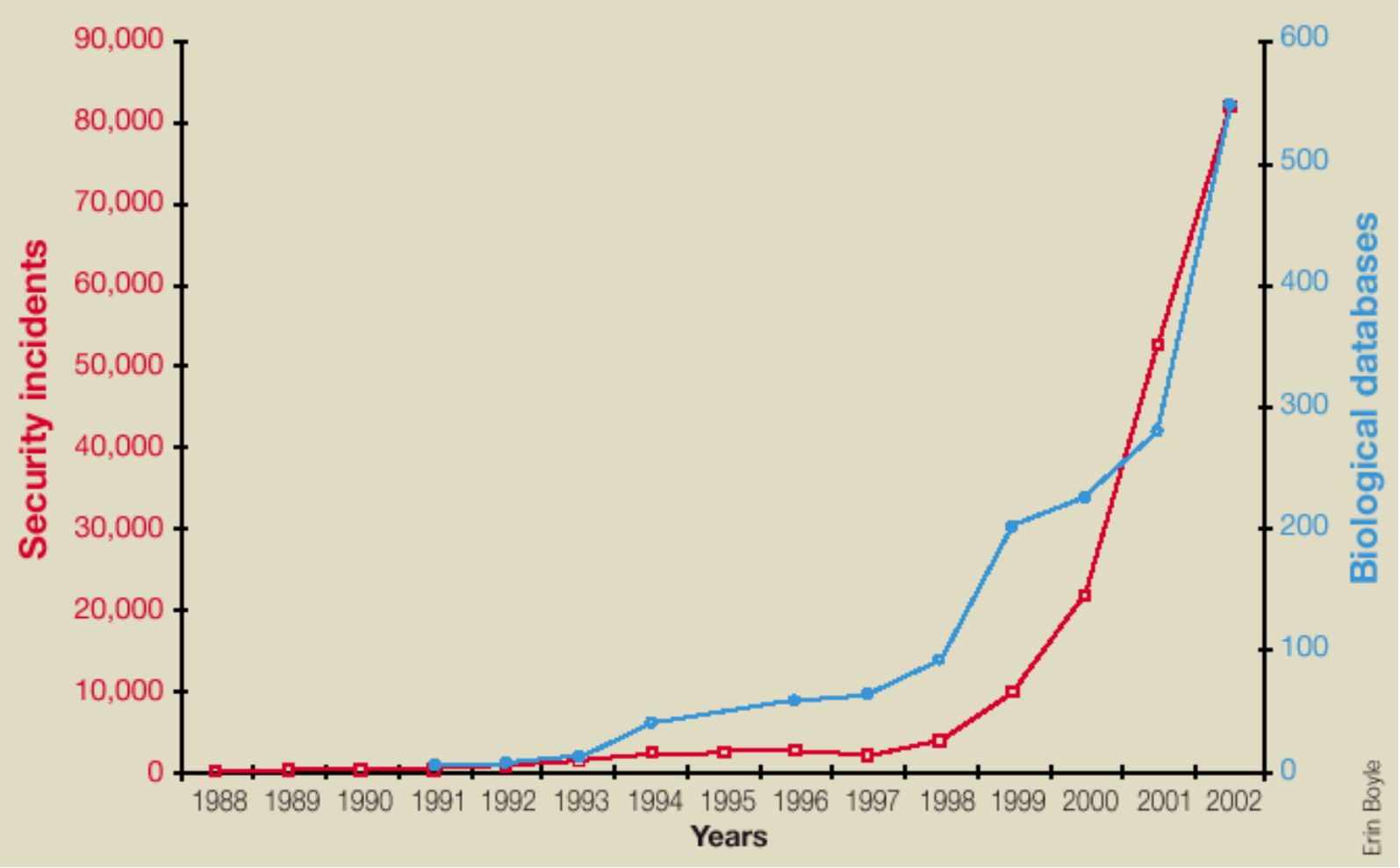
SEE ALSO
- What makes a cyber criminal?
  19 May 08 | Americas
- Obama begins cybersecurity review
  10 Feb 09 | Technology
- Google and GE in energy deal
  18 Sep 08 | Technology
- Cybercrime threat rising sharply
  31 Jan 09 | Davos 2009
- China spying 'biggest US threat'
  15 Nov 07 | Americas
- US warned of China 'cyber-spying'
  20 Nov 08 | Asia-Pacific
- Firms demand aid on hi-tech crime
  03 Nov 08 | Technology
- EU to search out cyber criminals
  01 Dec 08 | Technology

RELATED INTERNET LINKS
- Wall Street Journal
- Dan Kaminsky Blog
- IOActive
- RSA Conference
- Commission on Cybersecurity for the 44th president
- Whitehouse
- Congressional panel on cyber security
- US Government Accountability Office

FI Security – Business Interests

- **Return on Investment (ROI)**
  - Measure of the worth of a project by measuring what benefits (return) accrue from an investment.

- **Return on Security Investment (ROSI)**
  - Budget optimisation for security measures
    how to get maximum security for a given budget
  - Cost vs. Benefit analyses of security measures



Data source: Nature Magazine

FBI says attacks succeeding despite security investments

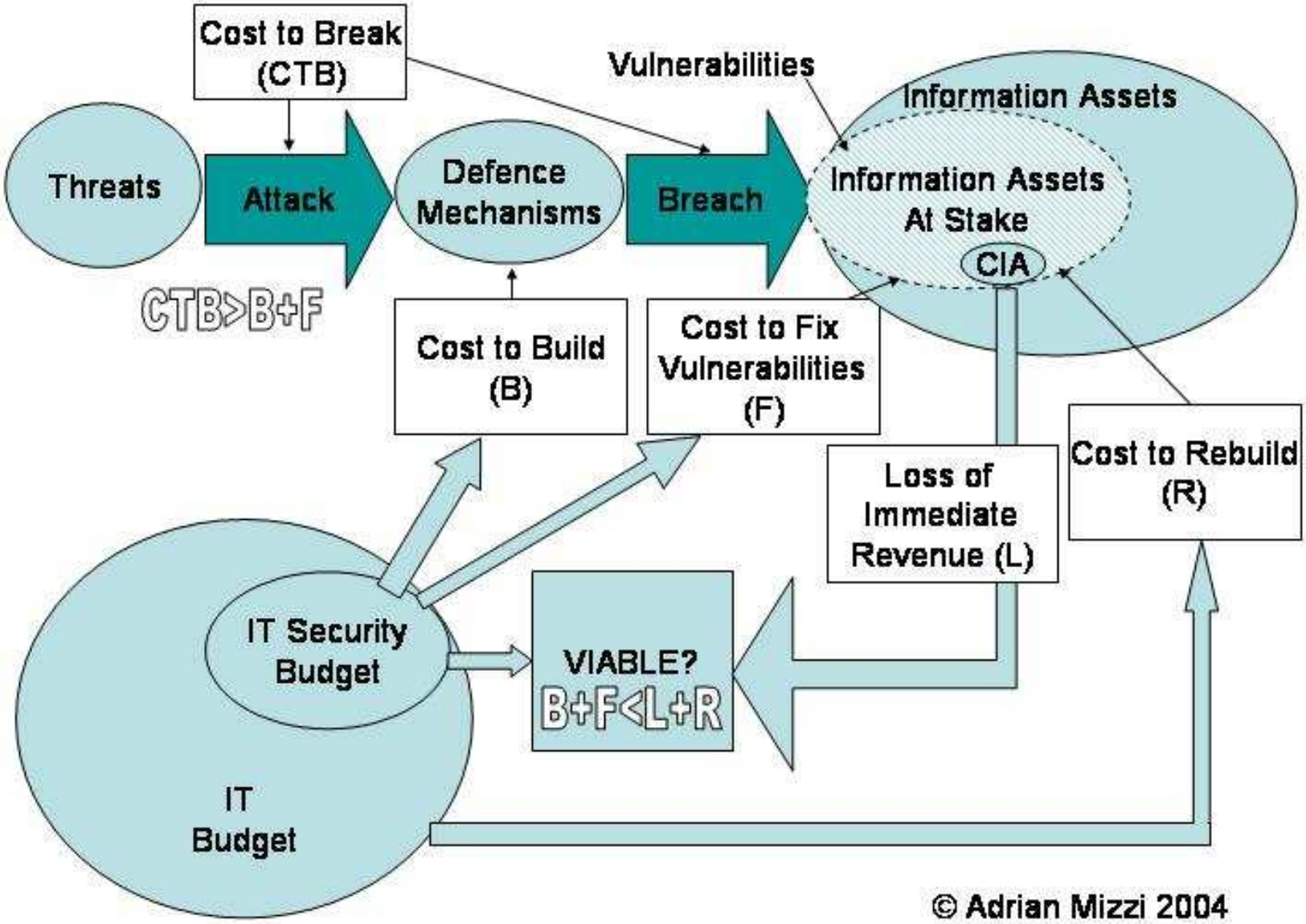
By Bill Brenner, Senior News Writer
11 Jan 2006 | SearchSecurity.com

A correction was made to this story. See below for details.

Despite investing in a variety of security technologies, enterprises continue to suffer network attacks at the hands of malware writers and inside operatives, according to an FBI report released today. Many security incidents continue to go unreported.

The 2005 FBI Computer Crime Survey was taken by 2,066 organizations in Iowa, Nebraska, New York, and Texas late last spring, which survey organizers deemed a good sample of enterprises nationwide. The report is designed to "gain an accurate understanding" of computer security incidents experienced "by the full spectrum of sizes and types of organizations within the United States," the FBI said. The 23-question survey addressed such issues as the computer security technologies enterprises use, what kinds of security incidents they've suffered and what actions they've taken.

The survey is not the same as the CSI/FBI Computer Crime and Security Survey, which has been conducted for several years and has a somewhat different focus, method and restricted number of respondents, the FBI said.


Cost to Break (CTB)
Vulnerabilities
Information Assets
Threats
Attack
Defence Mechanisms
Breach
Information Assets At Stake
CIA
CTB>B+F
Cost to Build (B)
Cost to Fix Vulnerabilities (F)
Loss of Immediate Revenue (L)
Cost to Rebuild (R)
IT Security Budget
VIABLE?
B+F<L+R
IT Budget
© Adrian Mizzi 2004

Conclusions

Predictions are not easy …

- It has always been difficult to predict the future trend of computing. These predictions are not always true:
  - *I think there is a world market for about five computers*
    Thomas J. Watson (IBM Founder) 1943
  - *The number of UNIX installations has grown to 10, with more expected* Dennis Ritchie and Ken Thompson 1972
  - *640k (program memory) ought to be enough for anybody*
    Attributed to Bill Gates (Microsoft Founder) 1981

Technology-based predictions

- However, technology-based predictions are often correct:
  - Moore's law
  - Mark Weiser vision
  - Quantum computers
- We agree that Future Internet has fascinating prospects.
- We need to work on the new paradigms for assuring security requirements of this emerging area.

Growth of Security Services

- **Past:** Security architecture has to thwart attacks
  - Access control, intrusion detection system, ..
- **Present:** Security architecture provides protection even under hostile situations
  - Intrusion tolerance, honeypots, security wrappers, …
- **Future:** Security architecture will have to cover the post-attack situations
  - Ethical hacking, forensics, security bootstrapping, …

Investment in Human Capital

- Security Management is itself becoming a comprehensive domain.

- We need to produce skilled manpower to deal with the complex security and dependability issues.

- This is the obvious way of weaving the security services in the fabric of today's information society

REMEMBER

Security is not a PRODUT

Security is a PROCESS

Thank you

Backup slides

Definitions

- **Authentication**
  - Each party establishes a level of trust in the identity of the other party
  - Authentication protocol sets up a secure communication channel between the authenticated parties

- **Authorization**
  - Provides access controls to desired parties.
  - Allows access to resources based on policies attached to each service.
    - Determines what you are allowed to do when you have been authenticated to the system.

Definitions

- **Availability**
  - Legitimate users have access when they need it
  - Replication: well-known technique for improving availability in distributed systems
    - Total network load is also decreased if replicas & requests are reasonably distributed

- **Confidentiality**
  - Assures that information does not reach unauthorized individuals, entities, or processes.
  - Achievable by a mechanism for ensuring access control
  - Confidentiality requirements include point-to-point transport as well as store-and-forward mechanisms.

Definitions

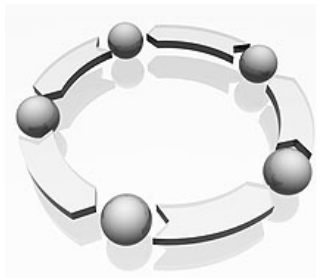
- **Integrity**
  - Assurance that information can only be accessed or modified by those authorized to do so.
  - Nontrivial problem
    - especially when storage hardware and networks are not perfect

- **Traceability**
  - Mechanism of observing the various actions taken by the different actors
  - Used to develop audit trails
  - Events are recorded in log files
  - Can be used to determine the responsibility of incidents

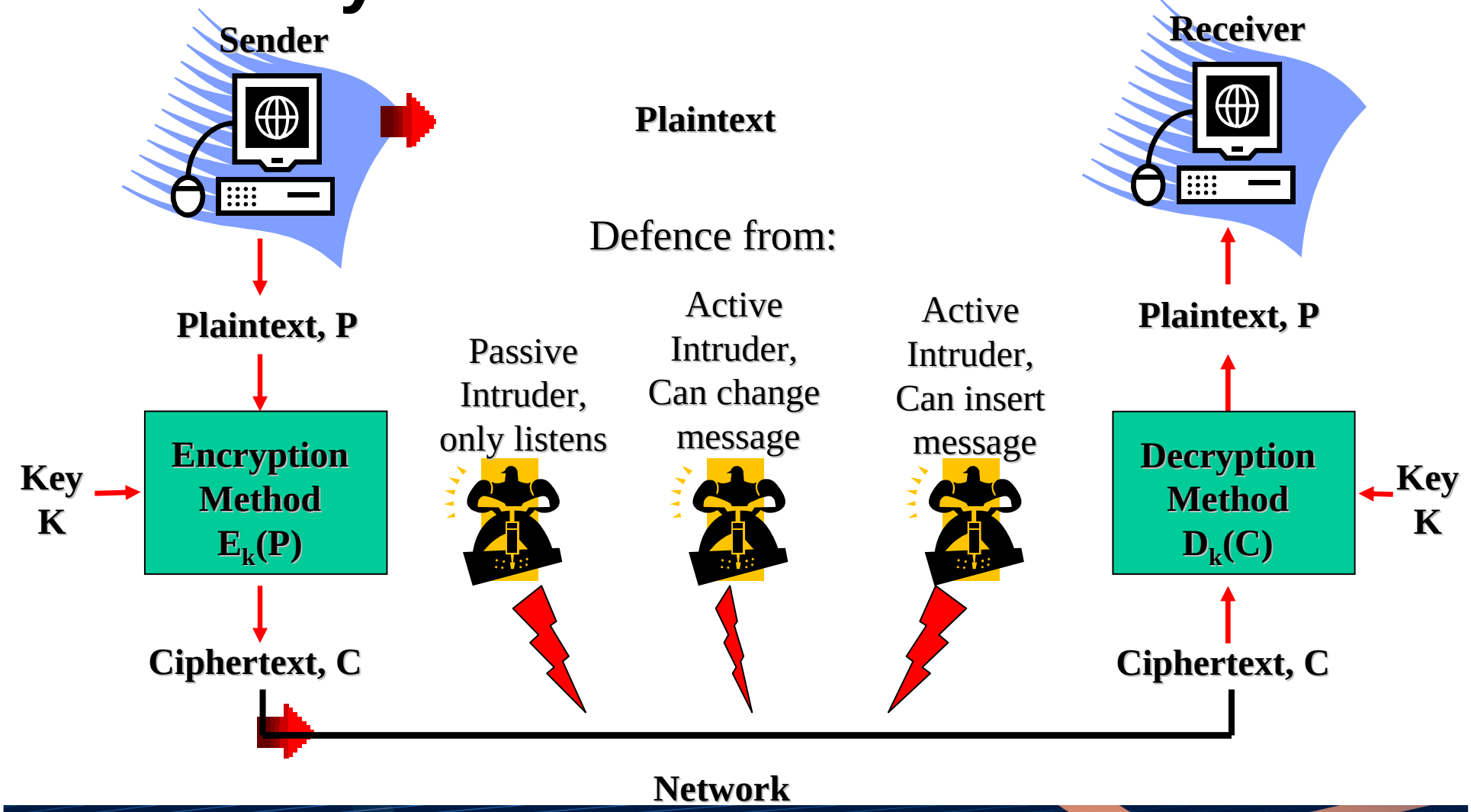
Definitions

- **Resilience**
  - Provides an abstraction layer to hide the architectural changes from the overall security architecture
  - Security architecture should remain intact and should deliver the promised level of security even if its composition changes over time.

- **Data Lifecycle Management (DLM)**
  - Lifecycle is the time from the moment data is created until it is deleted or stored indefinitely.
  - Security assurances require spanning the entire lifecycle of data.



Security Solutions – ENCRYPTION



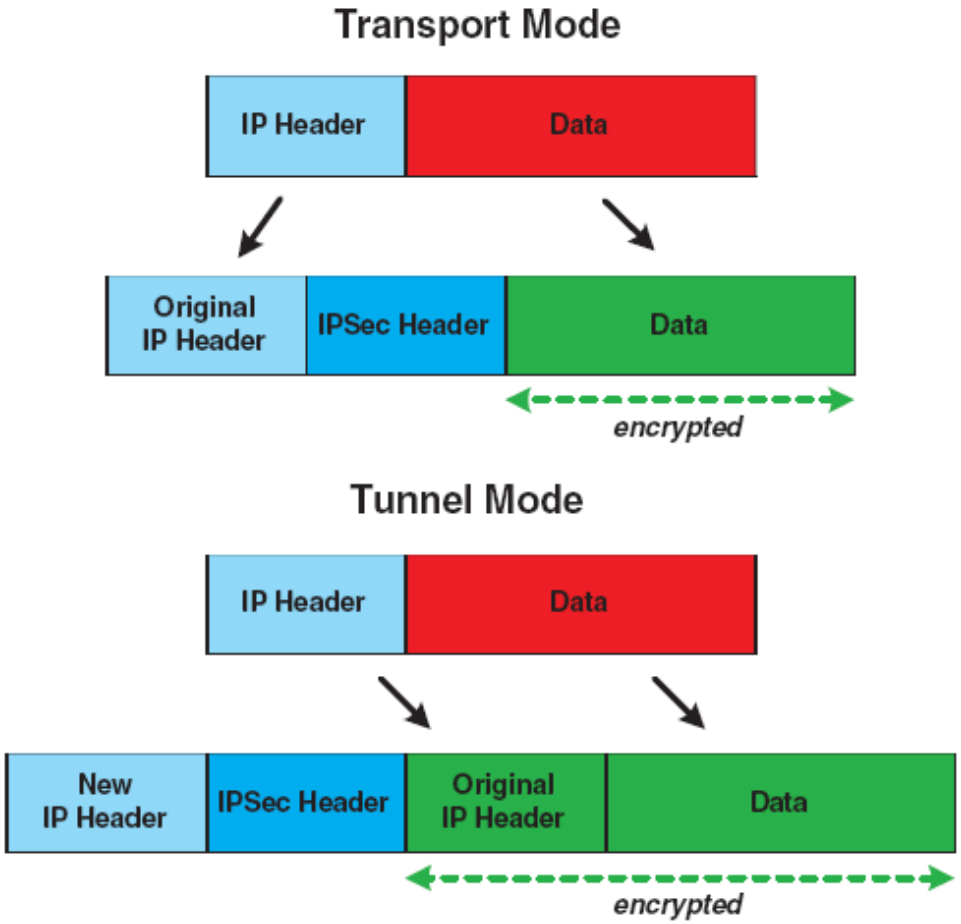
Security Solutions – IP Security (IPSec)

- **IPSec is an Internet standard for network layer security**
- **Components:**
  - an authentication protocol (Authentication Header – AH)
  - a combined encryption and authentication protocol (Encapsulated Security Payload – ESP)
  - key management protocols (the default is ISAKMP/Oakley)

- **Important RFCs**
  - RFC 2401: an overview of the IPSec security architecture
  - RFC 2402: specification of AH
  - RFC 2406: specification of ESP
  - RFC 2408: specification of ISAKMP
  - RFC 2412: specification of Oakley

- **IPSec is mandatory for IPv6 and optional for IPv4**

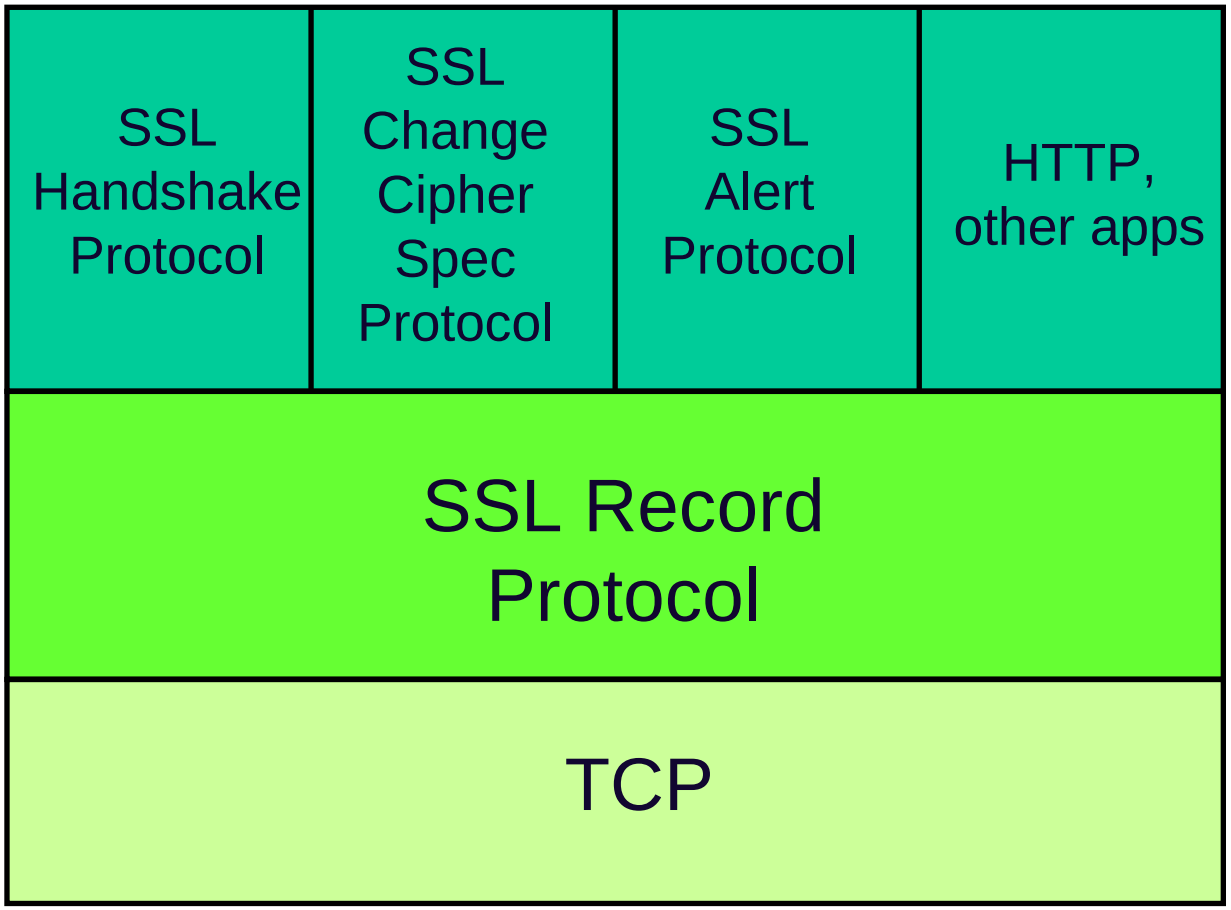
IPSec – Modes of Operation



SSL / TLS

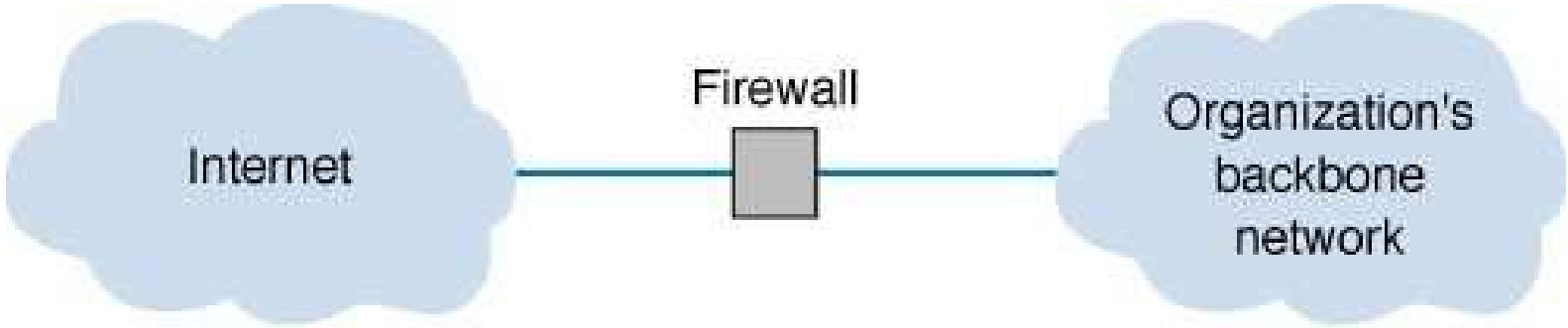
- **SSL = Secure Sockets Layer**
  - unreleased v1, flawed but useful v2, good v3
- **TLS = Transport Layer Security**
  - TLS1.0 = SSL3.0 with minor tweaks (see later)
  - Defined in RFC 2246
  - Open-source implementation at http://www.openssl.org/
- **SSL/TLS provides security ‘at TCP layer’**
  - Uses TCP to provide reliable, end-to-end transport
  - Applications need some modification
  - In fact, usually a thin layer between TCP and HTTP

SSL / TLS


SSL Handshake Protocol
SSL Change Cipher Spec Protocol
SSL Alert Protocol
HTTP, other apps
SSL Record Protocol
TCP

Firewalls

- Firewalls are used to prevent intruders on the Internet from making unauthorized access and denial of service attacks to your network.
- A firewall is a router, gateway, or special purpose computer that examines packets flowing into and out of the organization's network (usually via the Internet or corporate Intranet), restricting access to that network.
- The two main types of firewalls are packet level firewalls and application-level firewalls.



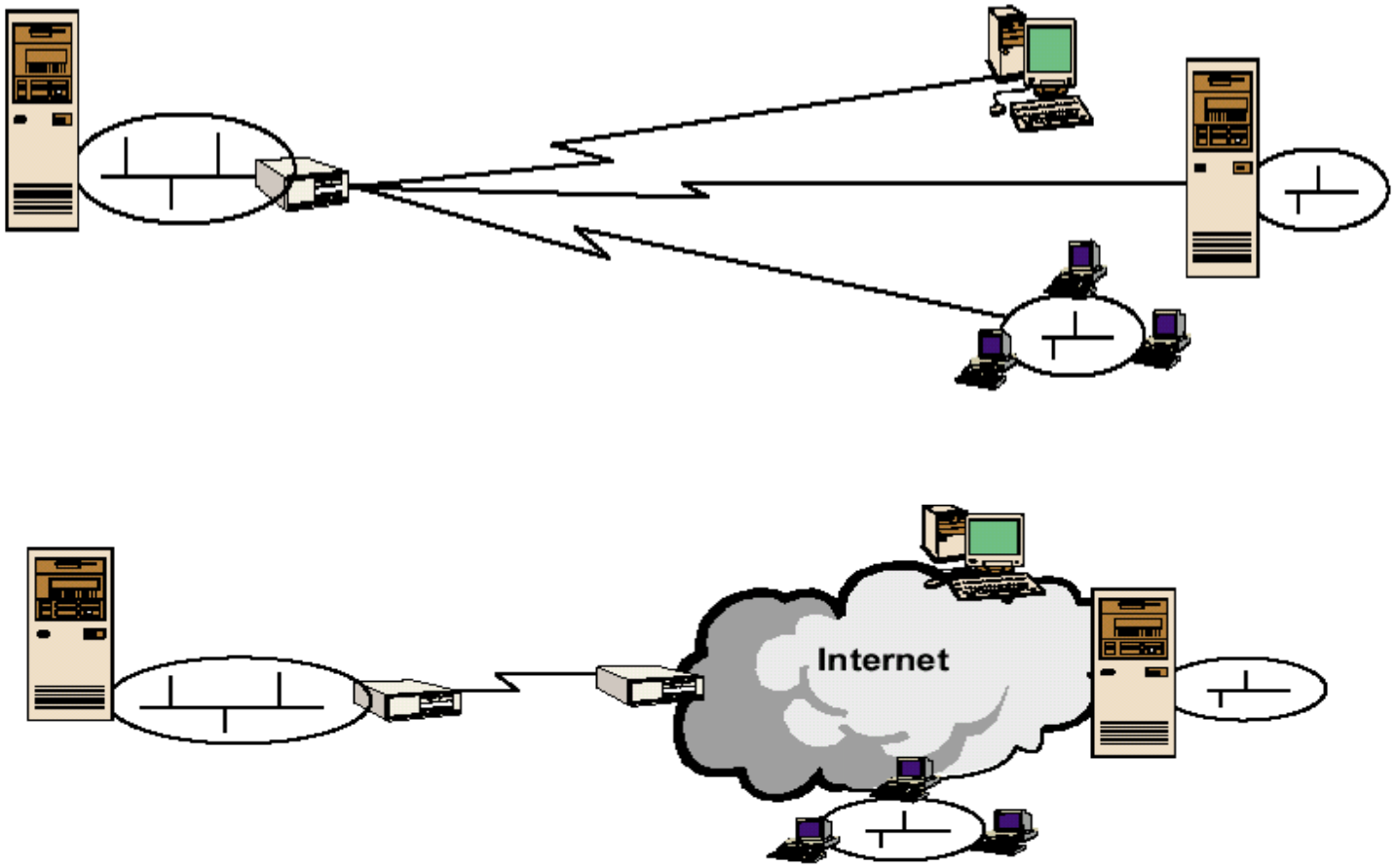
Firewalls

- A packet-level firewall (or packet filter) examines the source and destination address of packets that pass through it, only allowing packets that have acceptable addresses to pass.

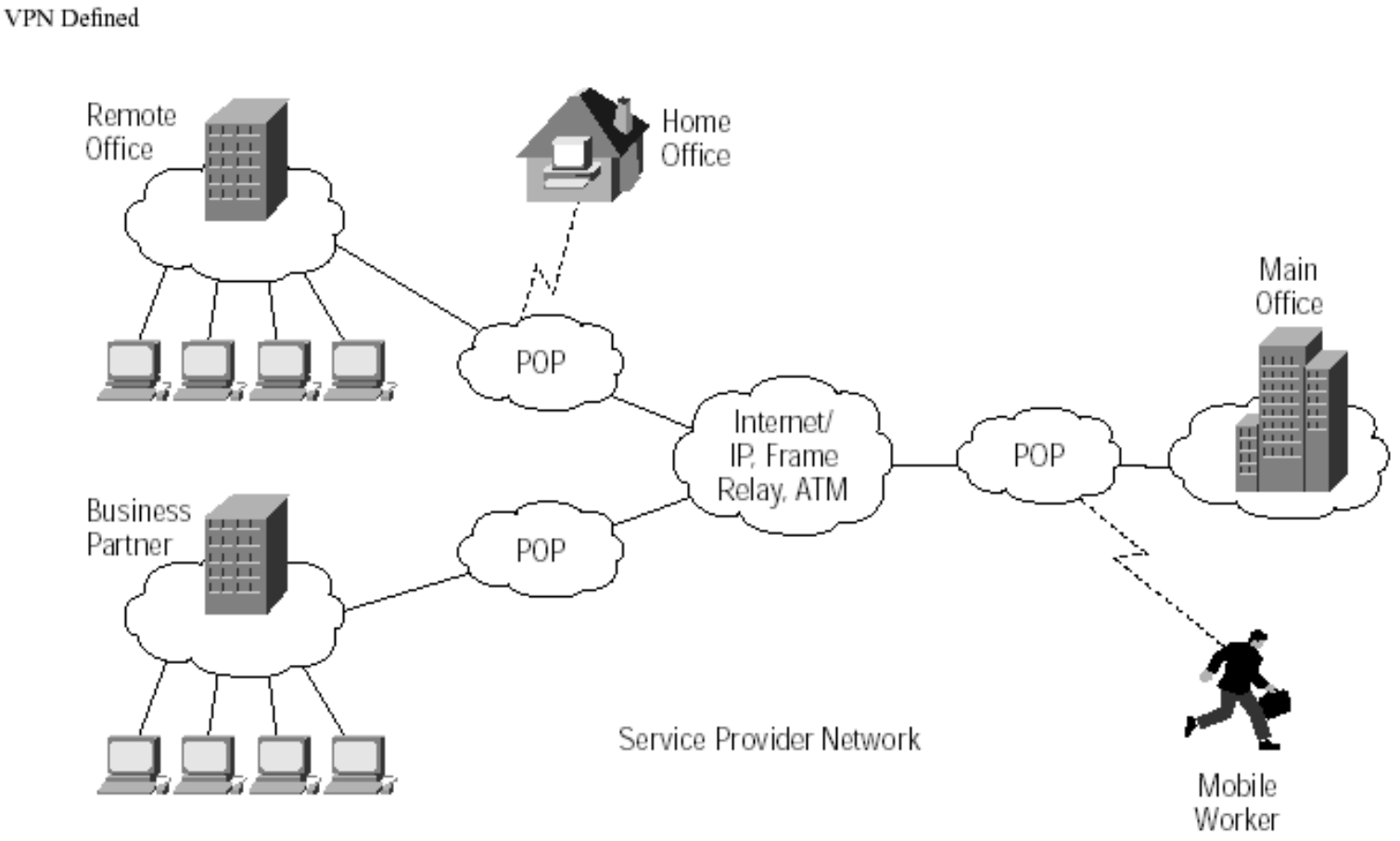
- An application level firewall or application gateway acts as an intermediate host computer, separating a private network from the rest of the Internet, but it works on specific applications, such as Web site access.

- DMZ (demilitarized zone) sits between perimeter network and internal network. It is separated by firewalls on both sides.

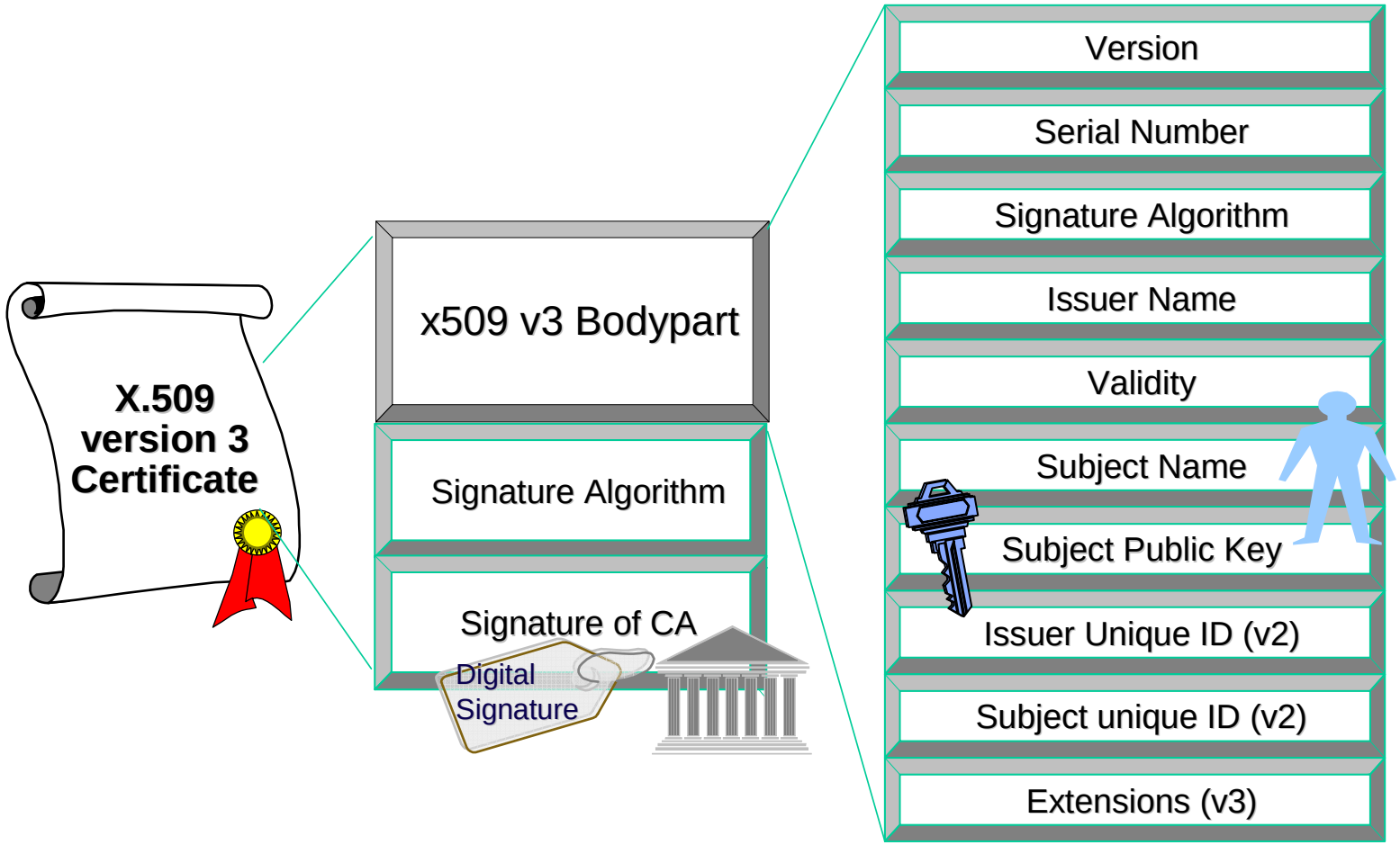
Virtual Private Network (VPN)



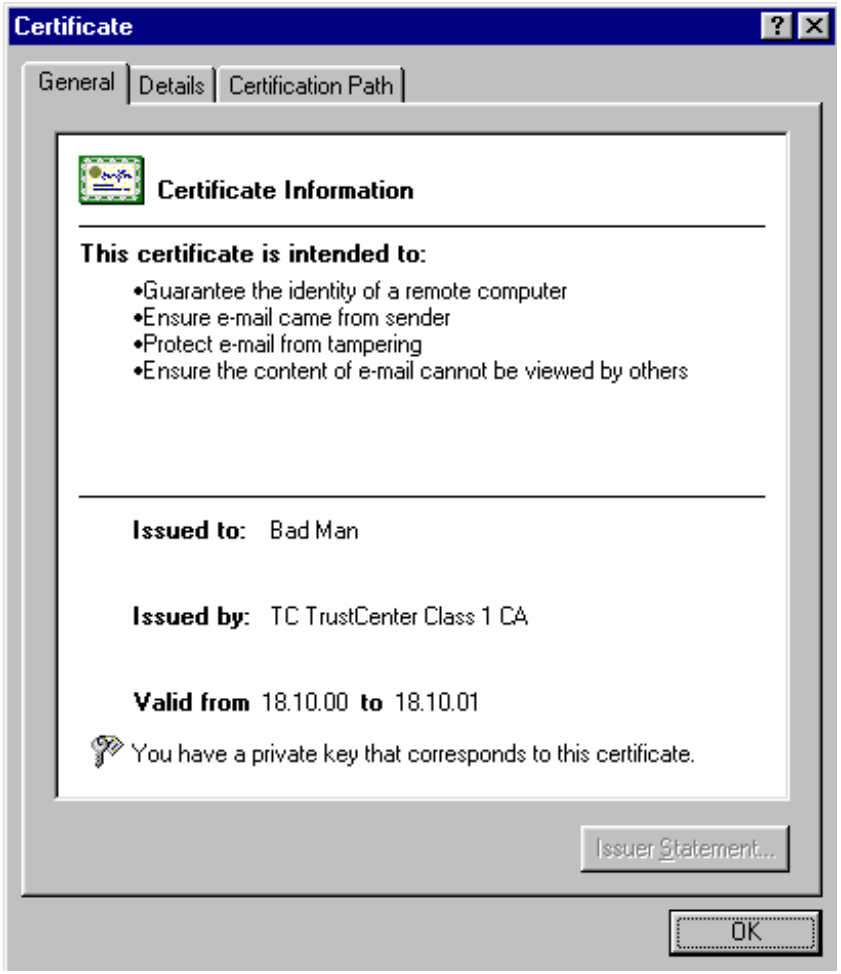
Virtual Private Network (VPN)

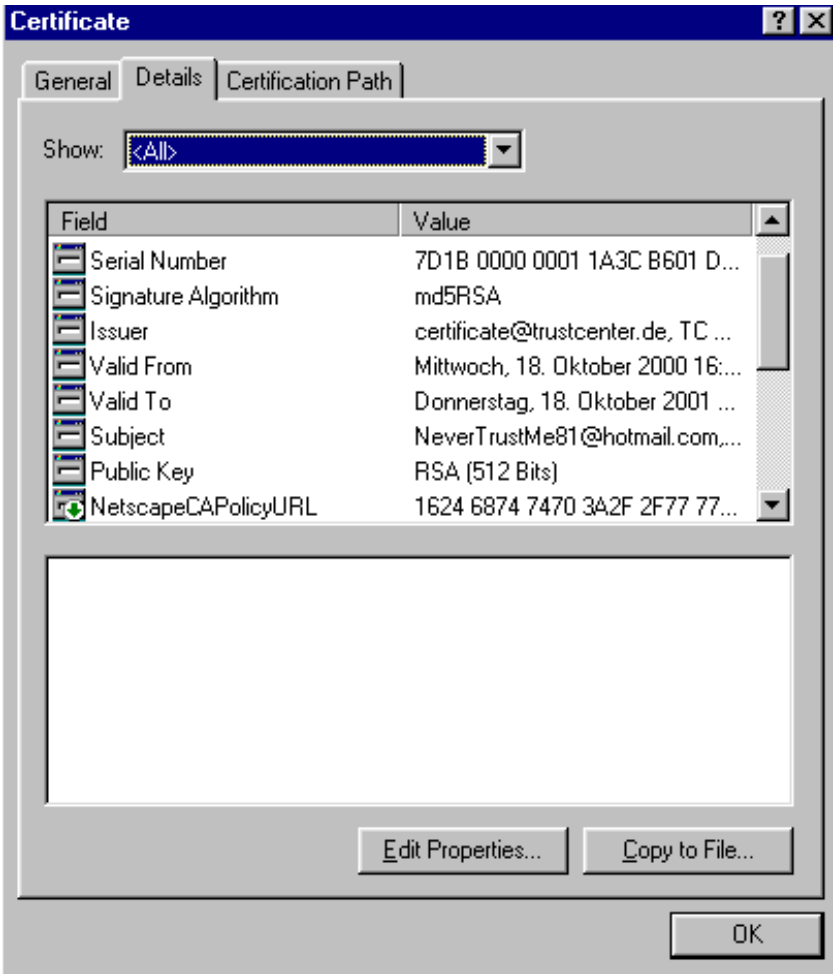


Security Solutions – AUTHENTICATION

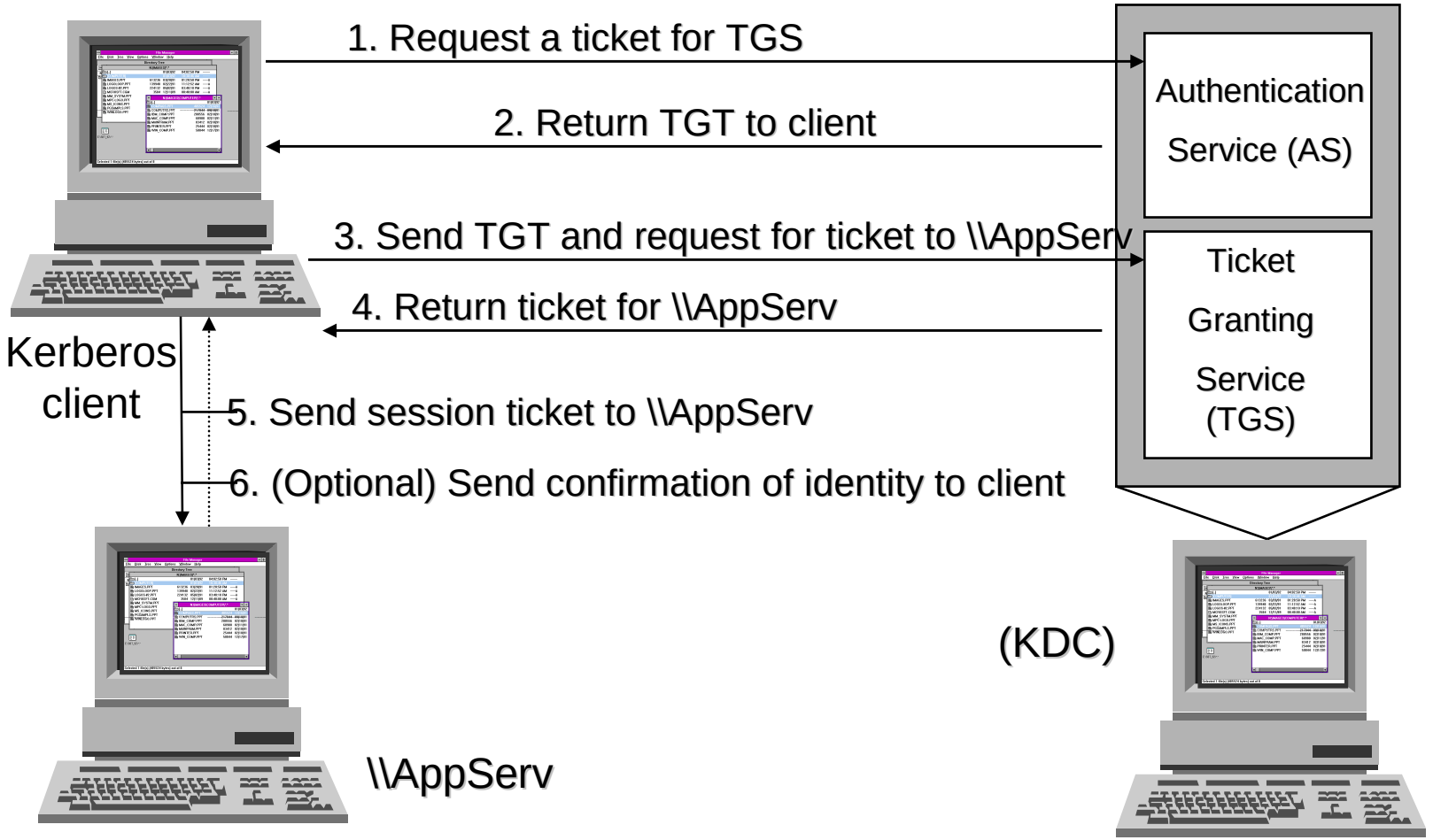


Security Solutions – X.509 Certificates



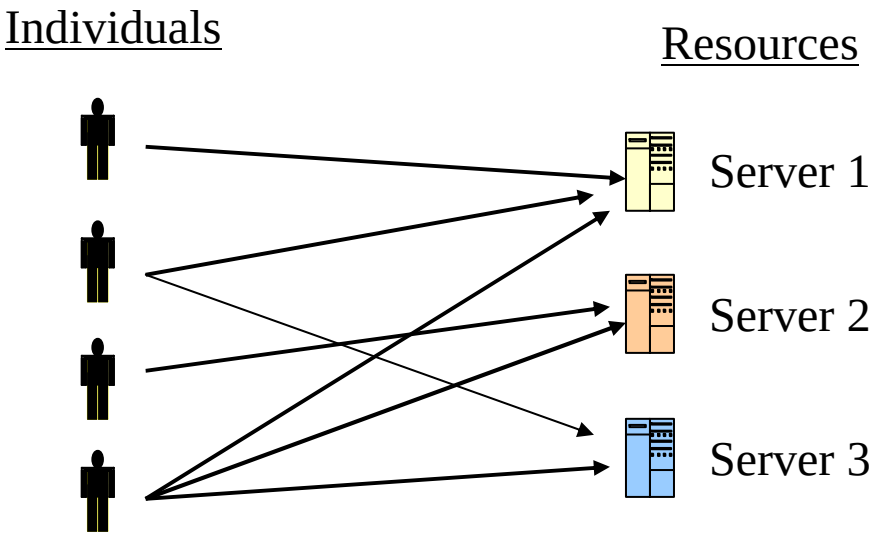


Security Solutions – Kerberos



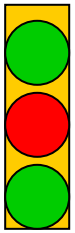
Security Solutions – AUTHORISATION

Discretionary Access Control



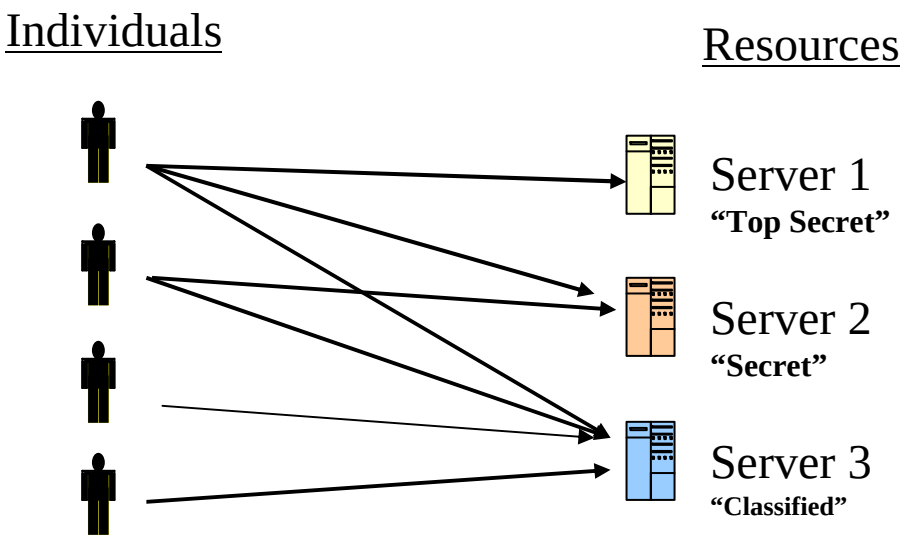
Application
Access List

Name	Access
Tom	Yes
John	No
Cindy	Yes



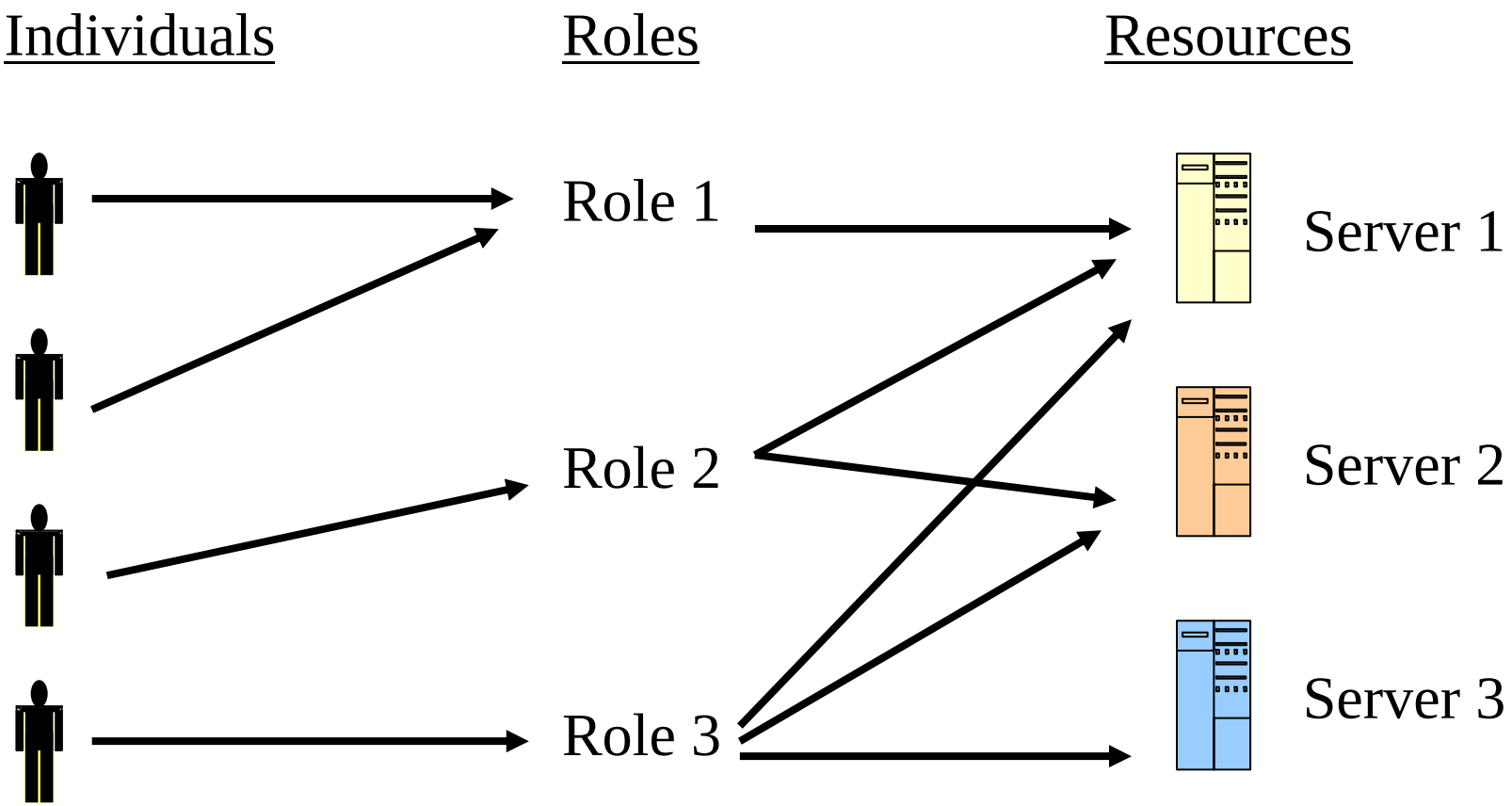
Security Solutions – AUTHORISATION

Mandatory Access Control



Security Solutions – AUTHORISATION

Role-based Access Control



Users change frequently, Roles don’t

Security Solutions – CONFIDENTIALITY

Bell-LaPadula Model

- Let L(S)=ls be the security clearance of subject S.
- Let L(O)=lo be the security classification of object O.
- **Simple Security Condition:** (No Read Up)
  - S can read O if and only if lo<=ls and
  - S has discretionary read access to O.
- ***-Property (Star property):** (No Write Down)
  - S can write O if and only if ls<=lo and
  - S has discretionary write access to O.
- TS personnel can not write documents lower than TS.
  - Prevent classified information leak.

Security Solutions – INTEGRITY

Biba Model

- Based on Bell-LaPadula
  - Subject, Objects
  - Integrity Levels with dominance relation
    - Higher levels
      - more reliable/trustworthy
      - More accurate

Clark-Wilson Model

- Addresses data integrity requirements for commercial applications.
  - E.g. Bank transactions
- Integrity requirements are divided into:
  - internal consistency: properties of the internal state that can be enforced by the computer system.
  - external consistency: the relation of the internal state to the real world: enforced by means outside the system, e.g. auditing.