E-Commerce: Security Challenges and Solutions

Mohammed Ghouseuddin
College of Computer Sciences & Engg.
KFUPM

Presentation Outline

- Internet Security
- E-Commerce Challenges
- E-Commerce Security
- E-Commerce Architecture

Challenges to Security

- Internet was never designed with security in mind
- Many companies fail to take adequate measures to protect their internal systems from attacks
- Security precautions are expensive {firewalls, secure web servers, encryption mechanisms}
- Security is difficult to achieve

Introduction

- Wide spread networking
- Need for Automated Tools for Protecting files and Other Information

- Network and Internet Security refer to measures needed to protect data during its transmission from one computer to another in a network or from one network to another in an network

…Continue

Network security is complex. Some reasons are:

- Requirements for security services are:
  - » Confidentiality
  - » Authentication
  - » Integrity
- Key Management is difficult

  Creation, Distribution, and Protection of Key information calls for the need for secure services, the same services that they are trying to provide

Cyber Felony

- In 1996 the Pentagon revealed that in the previous year it had suffered some two hundred fifty thousand attempted intrusions into its computers by hackers on the Internet
- Nearly a hundred sixty of the break-ins were successful

…Continue

- Security Attacks:
  - Interruption
  - Interceptor
  - Modification
  - Fabrication
  - Viruses
- Passive Attacks: Interception(confidentiality)
  - Release of message contents
  - Traffic Analysis

…Continue

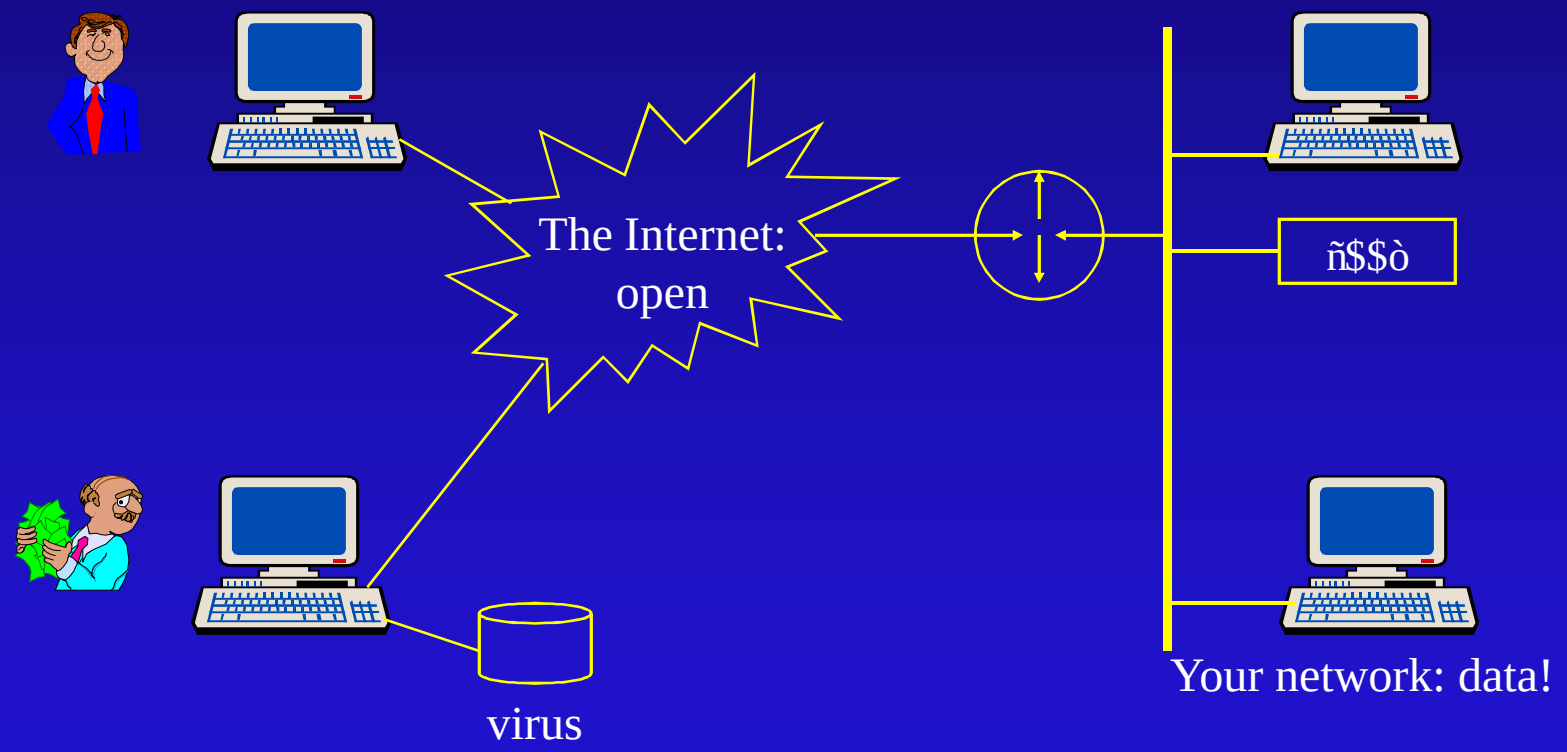
- Active Attacks:
  - » Interruption (availability)
  - » Modification (integrity)
  - » Fabrication (integrity)

Security Threats

- Unauthorized access
- Loss of message confidentiality or integrity
- User Identification
- Access Control
- Players:
  - User community
  - Network Administration
  - Introducers/Hackers

Introduction to Security Risks

Hackers and crackers



The Main Security Risks

- Data being stolen
  - » Electronic mail can be intercepted and read
  - » Customerôs credit card numbers may be read
- Login/password and other access information stolen
- Operating system shutdown
- File system corruption

Viruses

- Unauthorized software being run
  - » Games
- Widely distributed software
  - » Shareware
  - » Freeware
  - » Distributed software

Possible Security "Holes"

- Passwords
  - » Transmitted in plain text
  - » Could be temporarily stored in unsafe files
  - » Could be easy to guess
- Directory structure
  - » Access to system directories could be a threat
- In the operating system software
  - » Some operating system software is not designed for secure operation
  - » Security system manager should subscribe to
    - ï comp.security.unix
    - ï comp.security.misc
    - ï alt.security

Easy Security

- Use a separate host
  - » Permanently connected to the Internet, not to your network
  - » Users dial in to a separate host and get onto the Internet through it
- Passwords
  - » Most important protection
  - » Should be at least eight characters long
  - » Use a mixture of alpha and numeric
  - » Should not be able to be found in dictionary
    - ï should not be associated with you!
  - » Change regularly

…Continue

- Every transaction generates record in a security log file
  - » Might slow traffic and host computer
  - » Keeps a permanent record on how your machine is accessed
- Tracks
  - » Generates alarms when someone attempts to access secure area
  - » Separate the directories that anonymous users can access
  - » Enforce user account logon for internal users
  - » Read web server logs regularly

E-Commerce: Challenges

- Trusting others electronically
  - » Authentication
  - » Handling of private information
  - » Message integrity
  - » Digital signatures and non-repudiation
  - » Access to timely information

E-Commerce: Challenges

- Trusting others electronically
  - » E-Commerce infrastructure
- Security threats ï the real threats and the perceptions
- Network connectivity and availability issues
  - » Better architecture and planning
- Global economy issues
  - » Flexible solutions

nmerce: Challenges Trusting Others

- Trusting the medium
  - » Am I connected to the correct web site?
  - » Is the right person using the other computer?
  - » Did the appropriate party send the last email?
  - » Did the last message get there in time, correctly?

mmerce: Solutions Trusting Others

- Public-Key Infrastructure (PKI)
  - » Distribute key pairs to all interested entities
  - » Certify public keys in a ñtrustedòfashion
    - ï The Certificate Authority
  - » Secure protocols between entities
  - » Digital Signatures, trusted records and non-repudiation

nmerce: Challenges Security Threats

- Authentication problems
  - » Impersonation attacks
- Privacy problems
  - » Hacking and similar attacks
- Integrity problems
- Repudiation problems

nmerce: Challenges Connectivity and availability

- Issues with variable response during peak time
- Guaranteed delivery, response and receipts
- Spoofing attacks
  - » Attract users to other sites
- Denial of service attacks
  - » Prevent users from accessing the site
- Tracking and monitoring networks

E-Commerce Security

- Security Strategies
  - » Encryption Technology
  - » Firewalls
  - » E-Mail Security
  - » Web Security
- Security Tools

Security Strategies

- Cryptography
  - » Private key
  - » Public Key
- Firewalls
  - » Router Based
  - » Host Based
- E-Mail Security
  - » PGP
  - » PEM
- Secure Protocols
  - » SSL, HTTPS
- VPN

ting Technologies Overview

- Networking Products
- Firewalls
- Remote access and Virtual Private Networks (VPNs)
- Encryption technologies
- Public Key Infrastructure
- Scanners, monitors and filters
- Web products and applications

Cryptography

- The Science of Secret writing
- Encryption: Data is transformed into unreadable form
- Decryption: Transforming the encrypted data back into its original form

- Types of Cipher
  - » Transposition
  - » Substitution

Types of Cryptosystems

- Conventional Cryptosystems
  - » Secret key Cryptosystems
  - » One secret key for Encryption and Decryption
  - » Example: DES
- Public key cryptosystems
  - » Two Keys for each user
    - ï Public key (encryptions)
    - ï Private key (decryptions)
  - » Example: RSA

s of Cryptosystems
(S

- Both the encryption and decryption keys are kept secret

  Example:

  - To encrypt, map each letter into the third letter forward in the alphabet order;
  - To decrypt, map each letter into the third letter back
- Problems with Secret Key Cryptosystems:
  - Key transfer
  - Too many keys

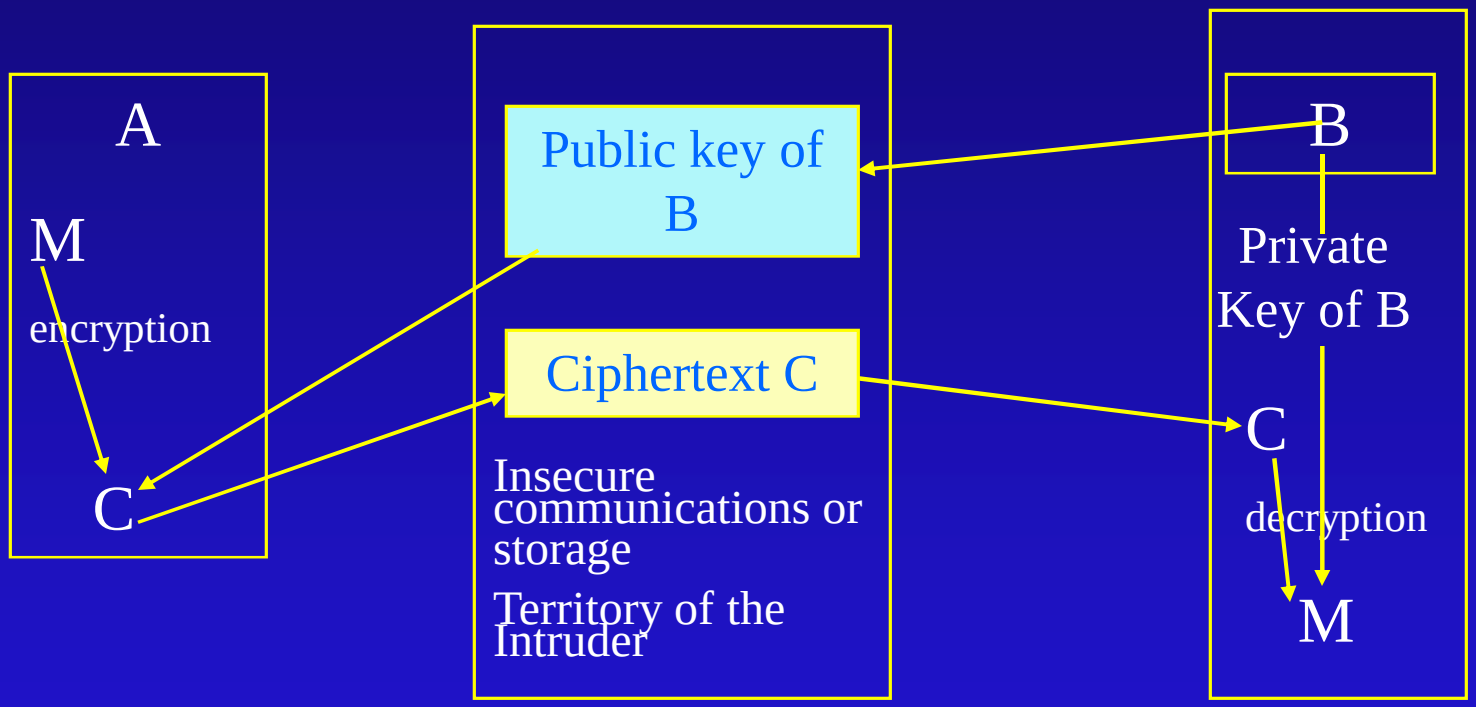
Key Cryptosystems (DES)

- Data Encryption Standard (1977)
- DES key length: 56-bits
- Uses 16 iterations with
  - » Transportation
  - » Substitution
  - » XOR operations
- DES Criticism
  - » Key length
  - » Design of S-Boxes in hidden
- Future
  - » Multiple DES
  - » IDEA (International Data Encryption Algorithm)

s of Cryptosystems (Public Key)

- Only the decryption key is kept secret. The encryption key is made public
- Each user has two keys, one secret and one public
- Public keys are maintained in a public directory
- To send a message M to user B, encrypt using the public key of B
- B decrypts using his secret key
- Signing Messages
- For a user Y to send a signed message M to user X
  - » Y encrypts M using his secret key
  - » X decrypts the message using Yôs public key

Public Key



A wants to send M in a secure manner to B

Encryption Technologies

- Hardware assist to speed up performance
- Encryption at different network layers; Layer2 through application layers
- Provide both public-key systems as well as bulk encryption using symmetric-key methods
- Stored data encryption and recovery

PKI

- A set of technologies and procedures to enable electronic authentication
- Uses public key cryptography and digital certificates
- Certificate life-cycle management

PKI -- the reality

- Many products from many vendors are available for certificate issuance and some management functions
- Interoperability is a big issue -- especially when it comes to policies
- Enabling the use of PKI in applications is limited today
- Building and managing policies is the least understood issue

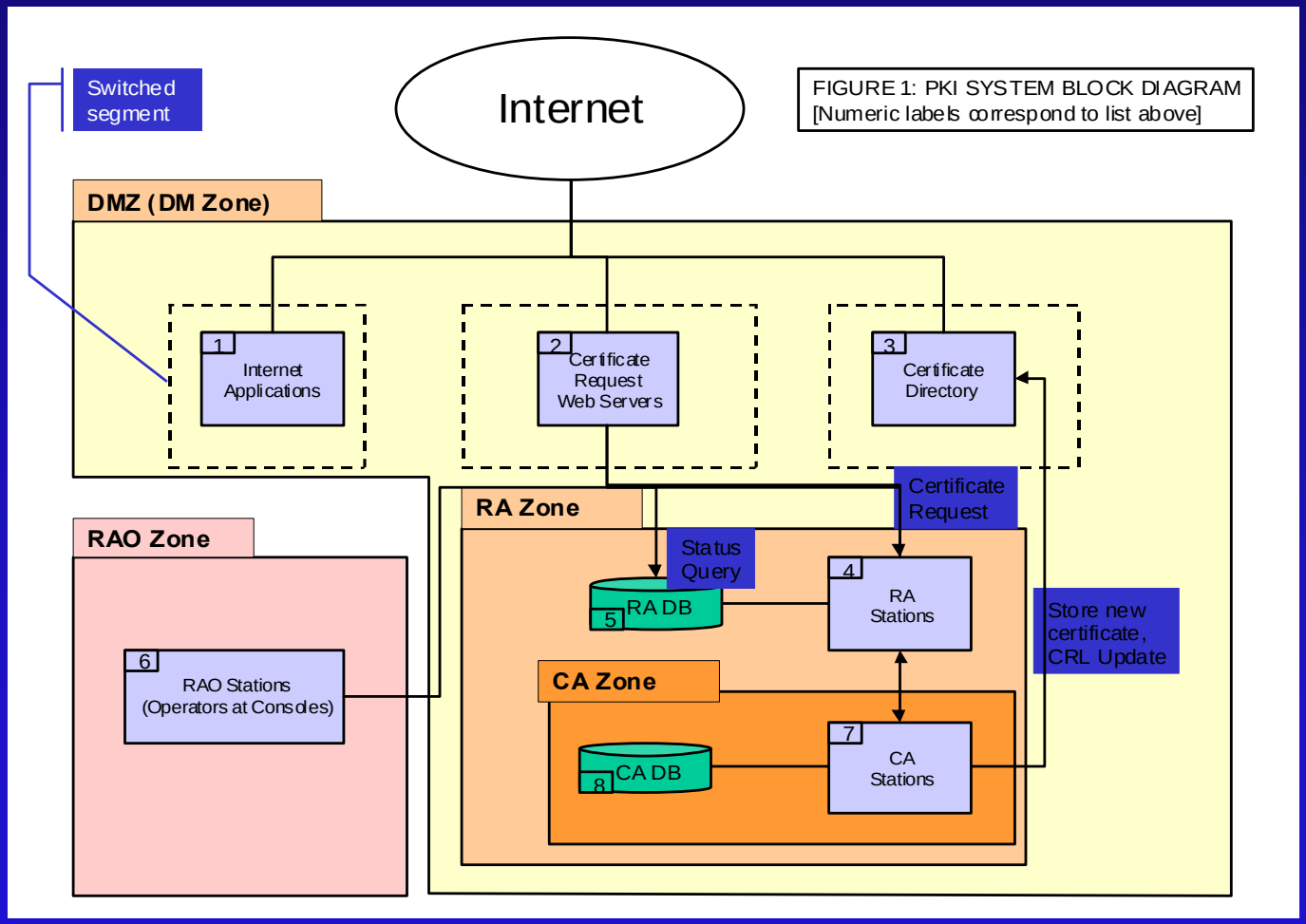
Policies

- Authentication and registration of certificate applicants
- System administration and access to signing keys
- Key ñEscrowò accessibility
- Application use and interfacing
- Trust between hierarchies

…Continue

- Trust decisions to be made at different points within the application need different views
- Certificate fields, authorization and allowed use is really the hardest issue
- Authorization policies for management of CAs and RAs

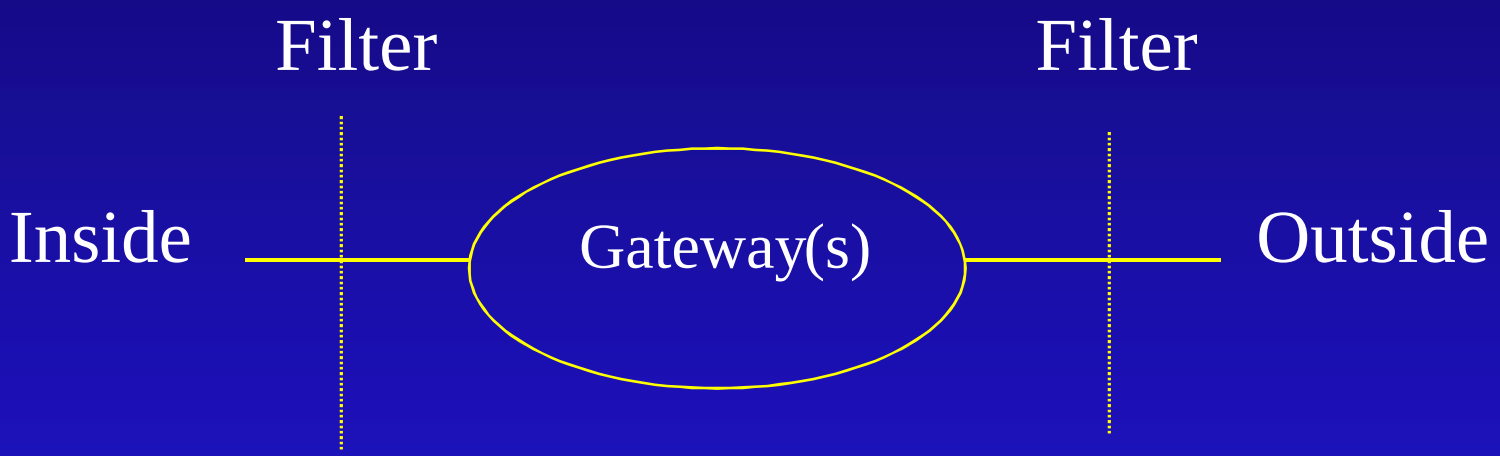
PKI Architecture



Firewalls

- Barrier placed between your private network and the Internet
- All incoming and outgoing traffic must pass through it
- Control flow of data in & out of your org.
- Cost: ranges from no-cost (available on the Internet) to $ 100,000 hardware/software system
- Types:
  - » Router-Based
  - » Host Based
  - » Circuit Gateways

Firewall



Schematic of a firewall

Firewall Types (Router-Based)

- Use programmable routers
- Control traffic based on IP addresses or port information (IP Filtering, Multilayer packet filtering)

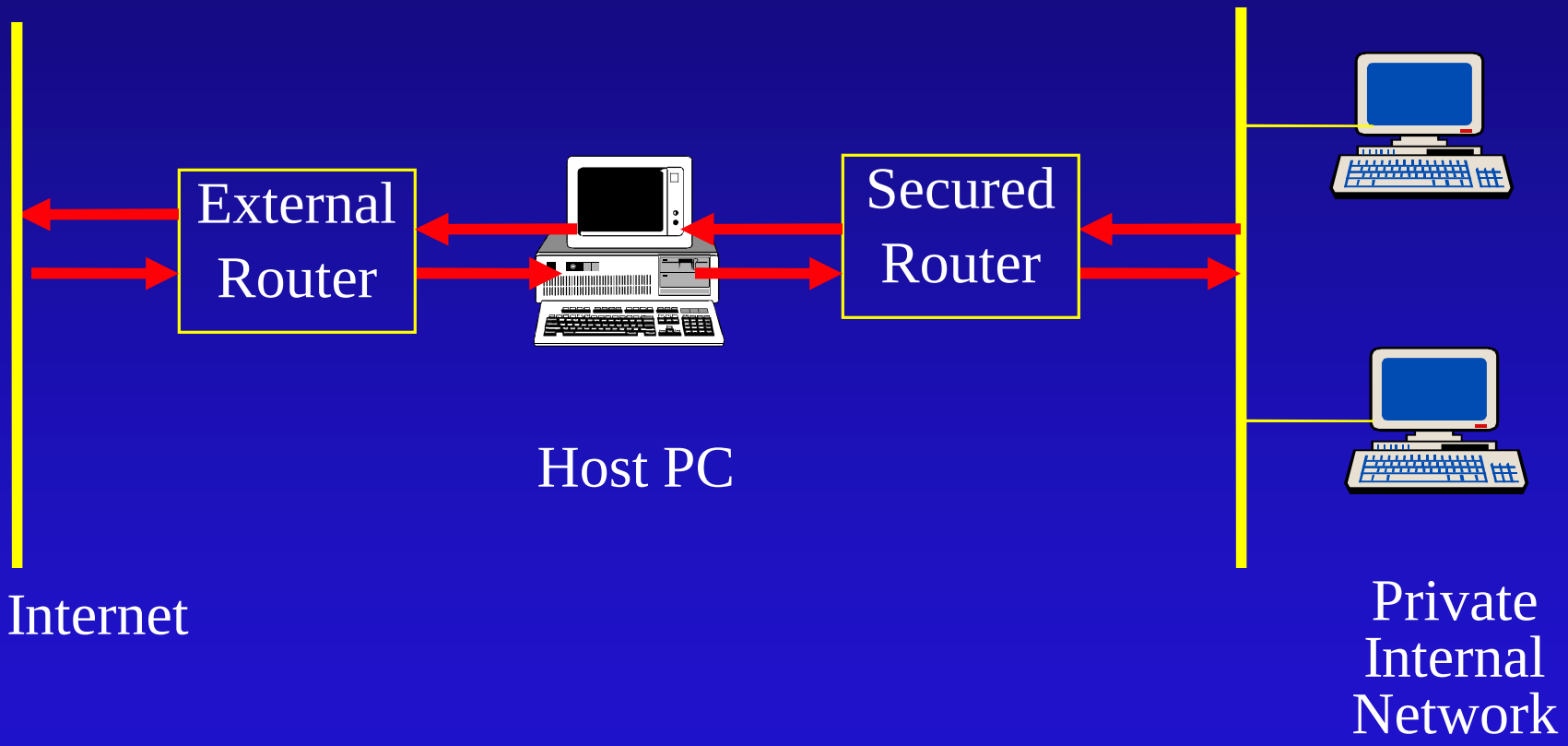
Examples:

- » Bastion Configuration
- » Diode Configuration

To improve security:

- Never allow in-band programming via Telnet to a firewall router
- Firewall routers should never advertise their presence to outside users

Bastion Firewalls

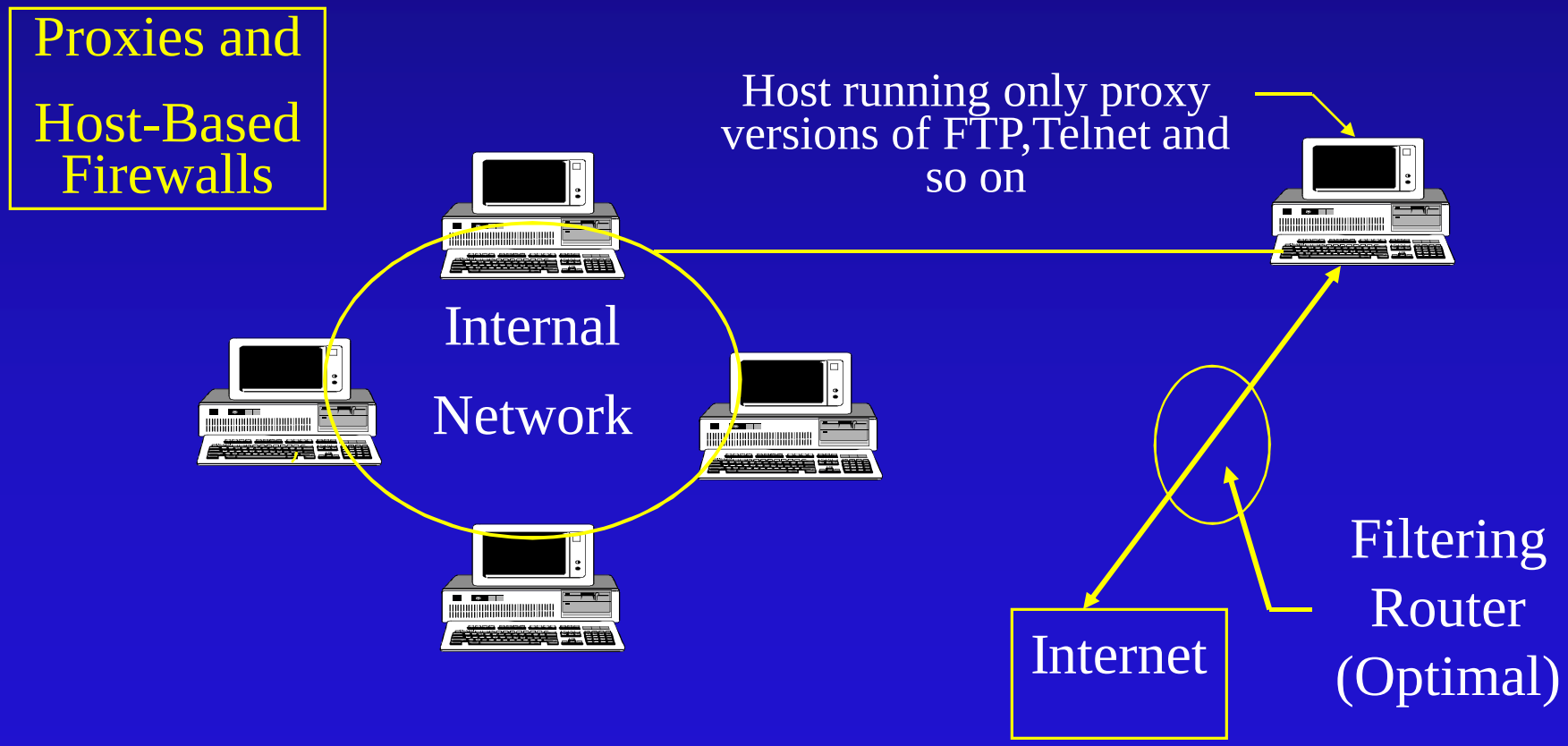


Firewall Types (Host-Based)

- Use a computer instead of router
- More flexible (ability to log all activities)
- Works at application level
- Use specialized software applications and service proxies
- Need specialized programs, only important services will be supported

…Continue

- Example: Proxies and Host-Based Firewalls



Scanners, Monitors and Filters

- Too much network traffic without designed policies
- Scanners understand the network configurations
- Monitors provide intrusion detection based on preset patterns
- Filters prevent unwanted traffic ï based of ñtypeò, for example virus detection

E-Mail Security

- E-mail is the most widely used application in the Internet
- Who wants to read your mail ?
  - » Business competitors
  - » Reporters,Criminals
  - » Friends and Family
- Two approaches are used:
  - » PGP: Pretty Good Privacy
  - » PEM: Privacy-Enhanced Mail

E-mail Security (PGP)

- Available free worldwide in versions running on:
  - » DOS/Windows
  - » Unix
  - » Macintosh
- Based on:
  - » RSA
  - » IDEA
  - » MD5

…Continue

- Where to get PGP
  - » Free from FTP site on the Internet
  - » Licensed version from Thwate.com

Example:

pgp -kg ID-A	→	Signature
pgp esa m.txt ID-B	→	Encryption
pgp message	→	Decryption

E-mail Security (PEM)

- A draft Internet Standard (1993)
- Used with SMTP
- Implemented at application layer
- Provides:
  - » Disclosure protection
  - » Originator authenticity
  - » Message integrity

S u

Function	Algorithms used	Description
Message encryption key	IDEA, RSA	A message is encrypted using IDEA . The session is encrypted using RSA recipientôs public key
Digital signature	RSA, MD5	A hash code of a message is created using MD5. This is encrypted using RSA with the senderôs private key
Compression	ZIP	A message may be compressed using ZIP
E-mail compatibility	Radix 64 conversion	To provide transparency for e-mail applications

Summary of PEM Services

Function	Algorithms used	Description
Message encryption	DES	A message is encrypted using DES-CBC. The session key is encrypted using RSA with the recipient's public key
Authentication and Digital signature(asymmetric encryption)	RSA with MD2 or MD5	A hash code of a message is created using MD2 or MD5. This is encrypted using RSA with the sender's private key
E-mail compatibility	Radix 64 conversion	To provide transparency for e-mail applications

Web Security

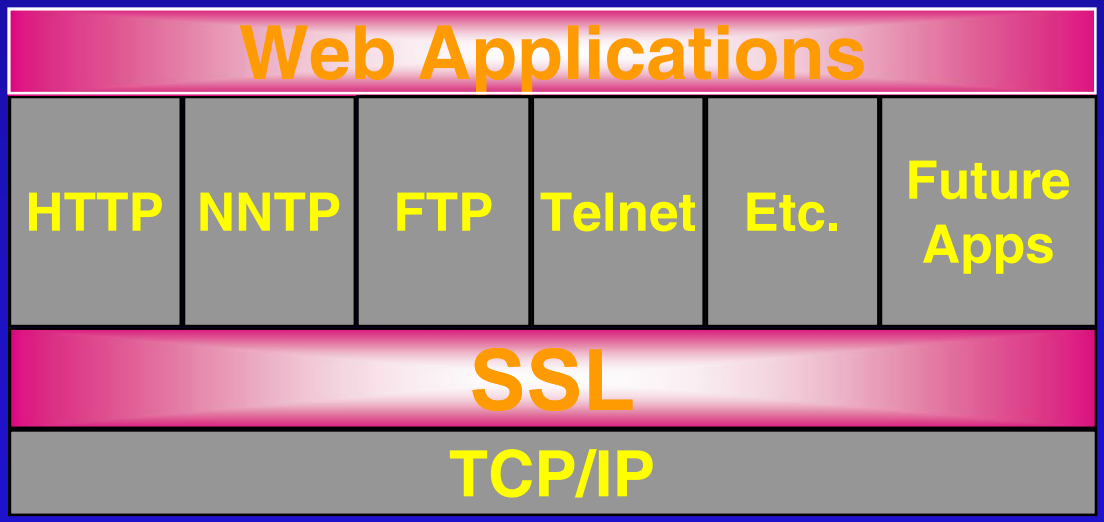
- Secure web servers ï SSL enabled
- Application servers ï generally lacking any security support
- A number of toolkits to enable applications to utilize security functions
- Integration into existing (legacy) infrastructure is difficult

Web Security

- Extensive Logging & Auditing
- Directory traversal protection
- Buffer overflow protection
- SSL enable the web server
- URL filtering (Web Sense)
- Common exploit signatures filter

Secure Sockets Layer (SSL)

- Platform and Application Independent
  - » Operates between application and transport layers



Secure Sockets Layer (SSL)

- Negotiates and employs essential functions for secure transactions
  - » Mutual Authentication
  - » Data Encryption
  - » Data Integrity
- As simple and transparent as possible

SSL 3.0 Layers

- Record Layer
  - » Fragmentation, Compression, Message Authentication (MAC), Encryption
- Alert Layer
  - » close errors, message sequence errors, bad MACs, certificate errors

Why did SSL Succeed

- Simple solution with many applications ï e-business and e-commerce
- No change in operating systems or network stacks ï very low overhead for deployment
- Focuses on the weak link ï the open wire, not trying to do everything to everyone
- Solution to authentication, privacy and integrity problems and avoiding classes of attacks

S-HTTP

- Secured HTTP (S-HTTP)
  - » Security on application layer
  - » Protection mechanism:
    - ï Digital Signature
    - ï Message authentication
    - ï Message encryption
  - » Support private & public key cryptograph
  - » Enhanced HTTP data exchange

S-HTTP vs. SSL

	User Interface		
Application Layer	S-HTTP	HTTP, SMTP, FTP, Telnet, Other Apps.	
	SSL	PCT	SET
Transport Layer	Transport Control Protocol		
Internet Layer	Internet Protocol (IP)		
Network Layer	Network		

SSL

- Operate on transport layer
- Encryption only for integrity and confidentiality
- Support HTTP, Telnet, FTP, Gopher, etc.
- Application independent
- Provide P-to-P protection
- DES, RSA, RC-2 and RC-4 with different size of keys
- One step security

S-HTTP

- Operate on application layer
- Encryption and digital signature
- Work only with (HTTP)
- Application dependant
- More secure than SSL at end point even after data transfer
- No particular cryptographic system
- Multiple times encryption

cured Electronic Transactions (SET)

- Developed by VISA & MasterCard
- SET Specifications:
  - » Digital Certificates (Identification)
  - » Public Key (Privacy)
- On-Line Shopping Steps:
  - » C.H. Obtain Digital Wallets
  - » C.H. Obtain Digital Certificates
  - » C.H. & Merchants conduct Shopping Dialog
  - » Authentication & Settlement Process

Verified by Visa

- Works with few big leaders in e-commerce market
- Secure Transactions (Secure web site to enter Credit card, Personal Information etc.)
- Secure Authentication
- Receipt of transaction payments
- Transaction history for tracking & verification

Existing EPS

- Electronic Cash
  - » Imitates Paper Cash
  - » Examples: CyberCash, DigiCash and Virtual Smart Cards
- Electronic Checking
  - » Same as Paper Checks
  - » Use Automated Clearing House (ACH)
  - » Examples: CheckFree, NetCheque and NetChex
  - » Not well developed as E-Cash or Credit Card

t mechanisms designed for the Internet

- Automated Transaction Services provide real-time credit card processing and electronic checking services (http://www.atsbank.com/)
- BidPay allows person-to-person payments, by accepting a credit card payment from the payer, and sending a money order to the payee (http://www.bidpay.com/)
- CyberCash offer secure credit card transactions, and electronic checks over the Internet (http://www.cybercash.com/)

Remote access and VPNs

- Better control for user access
- VPNs connect offices together using the public network, with authenticated encrypted channels
- IPSEC as a basic security protocol for remote access and VPN products

Security Tools

- Penetration Testing
  - » NESSUS, NMAP, Whisker, Etherreal, TCPDump
- Protocols
  - » SSL ï ñthe web security protocolsò
  - » IPSEC ï ñthe IP layer security protocolò
  - » SMIME ï ñthe email security protocolò
  - » SET ï ñcredit card transaction security protocolò
  - » Smart Cards, Secure VbV
- Website Trust Services
  - » Commerce Site Services
  - » Secure Site Services
  - » Payflow Payment Services
  - » Code Signing Digital IDs

Commerce Site Services

- For E-Merchants & Online stores
  - » 128 bit SSL ids
  - » Site authentication, Encryption
  - » Securely & easily accept credit cards, debit cards, purchase cards, elctronic checks

Pay-Pal

- Payment connectivity thru secure links
- Small scale thru limited & fixed connectivity
- Large scale thru. customizable links
- Dynamic Fraud screening

Code Signing

- For Software developers
- Digitally signed software & macros
- Safe delivery of content
- Trust implemented

What is Missing??

- Solid architecture practices
- Policy-based proactive security management
- Quantitative risk management measures especially regarding e-commerce or e-business implementations

E-Commerce Architecture

- Support for peak access
- Replication and mirroring, round robin schemes ï avoid denial of service
- Security of web pages throuògh certificates and network architecture to avoid spoofing attacks

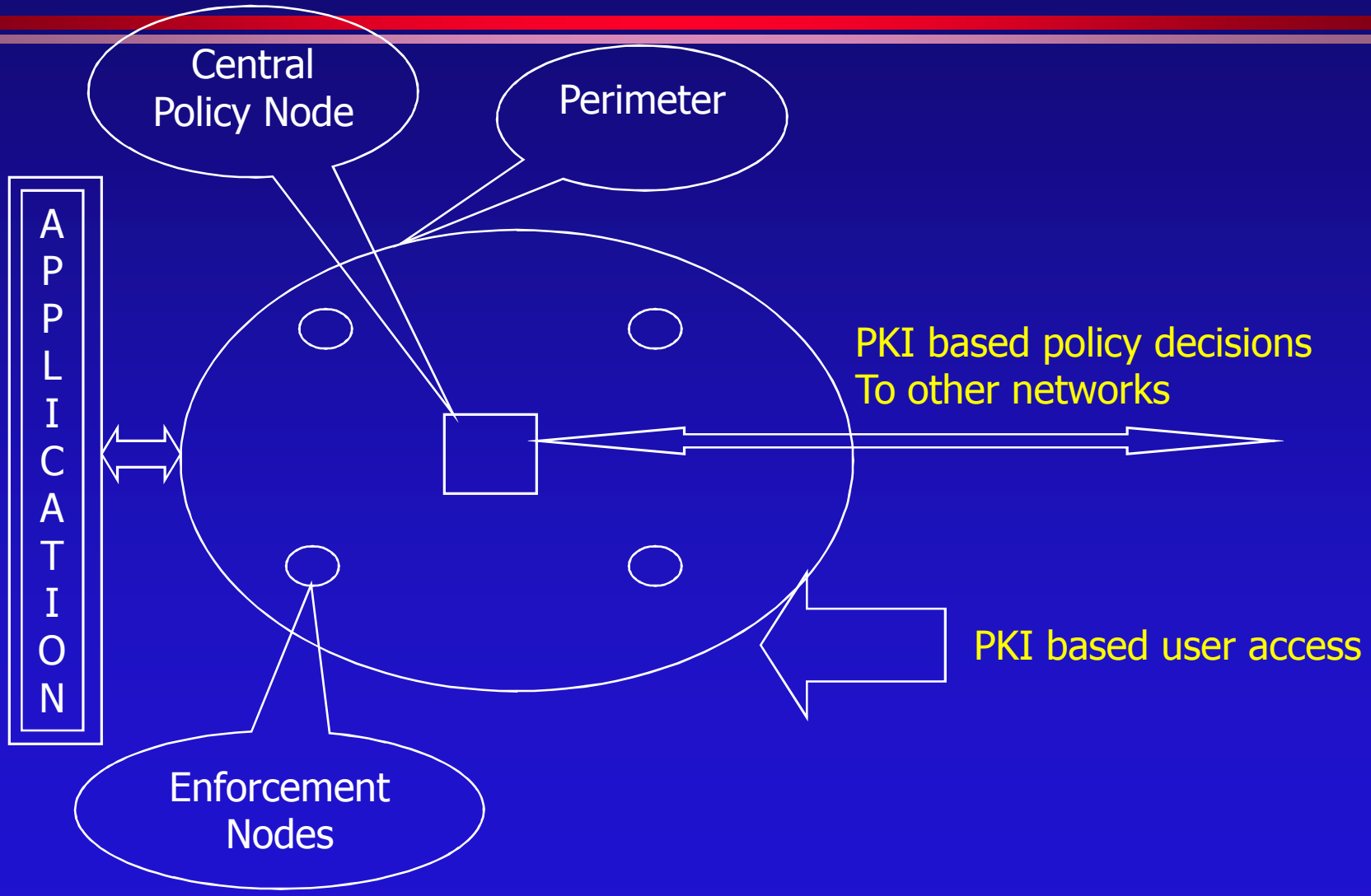
Proactive Security Design

- Decide on what is permissible and what is right
- Design a central policy, and enforce it everywhere
- Enforce user identities and the use of credentials to access resources
- Monitor the network to evaluate the results

PKI and E-Commerce

- Identity-based certificate to identify all users of an application
- Determine rightful users for resources
- ñRole-basedòcertificates to identify the authorization rights for a user

Architectures for E-Commerce



E-Commerce: Are We Ready?

- Infrastructure?
- Security?
- Policies & legal issues?
- Arabic content?

E-Commerce: Future

- Was expected to reach 37,500 (million US $) in 2002. It reached 50,000 (million US $) in 1998
- Expected to reach 8 million company in 2000 (40% of total commerce)
- Arab word, about 100 million US $

…Continue

- B-to-B E-Commerce will grow faster than B-to-C E-Commerce
- E-business is expected to grow faster in:

  Europe 118% Annual growth rate

  worldwide 86% *
- Number of companies is expected to reach 8 million by 2002 **

* Study by Nortel Networks (Financial Times 28/1/2000)

** British Telecom