IBM i TCP/IP Security

Stuart Stebbings
Power Technical Account Mgr
Arrow UK

Power^{tm} with IBM i

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

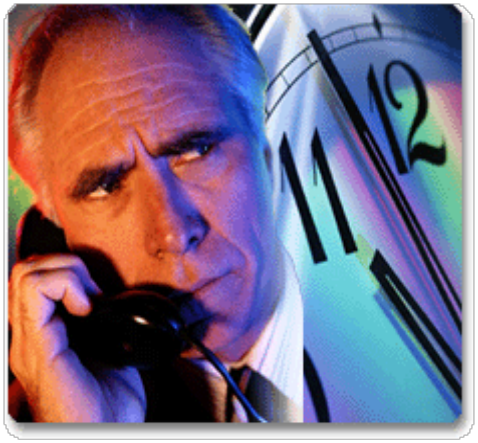
The threats

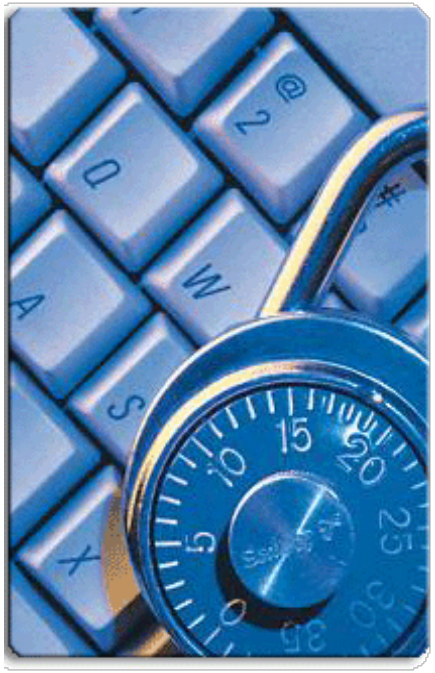
- Unauthorized access
- Theft of information
- Alteration of information
- Denial of service
- Impersonation
- Viruses
- As yet undiscovered
- Ethical hack

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Who would do you harm?

- Hackers
- Industrial espionage
- A thief
- Curious or disgruntled employees
- Unintentional user actions

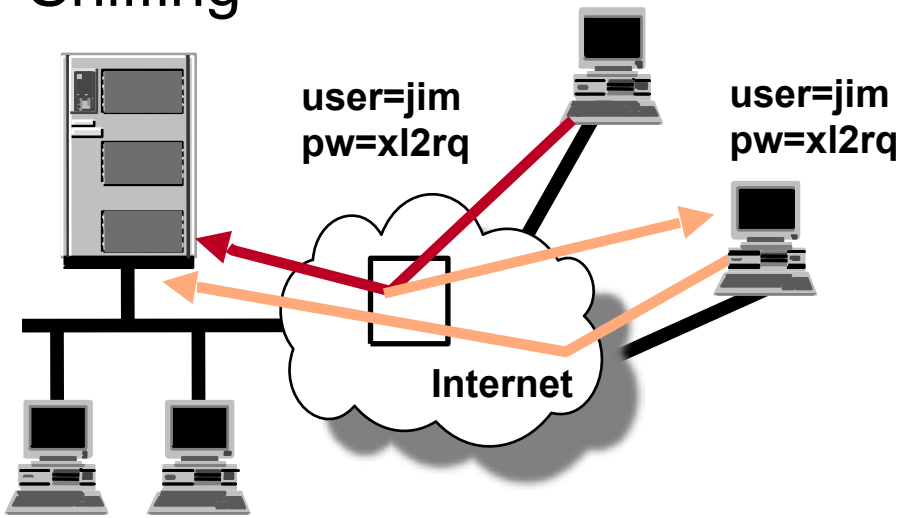




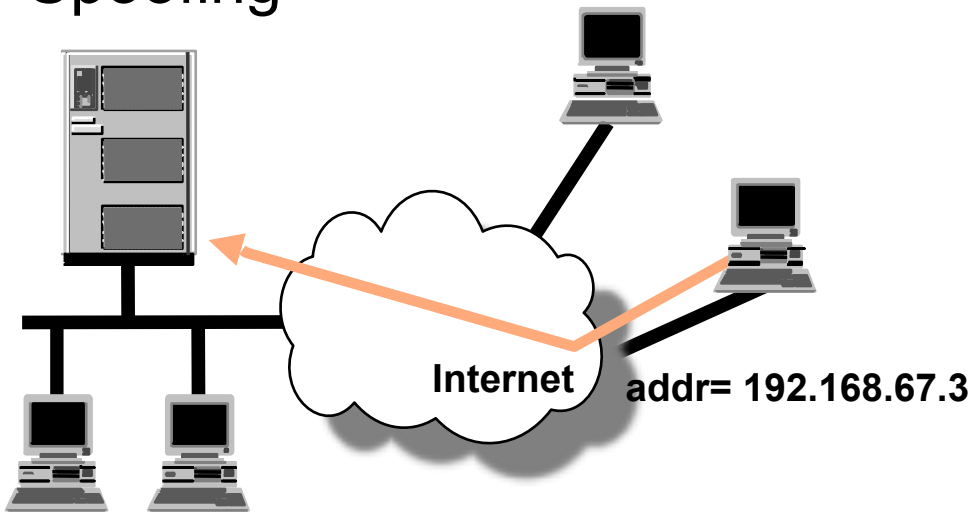
© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

How they do it

Sniffing

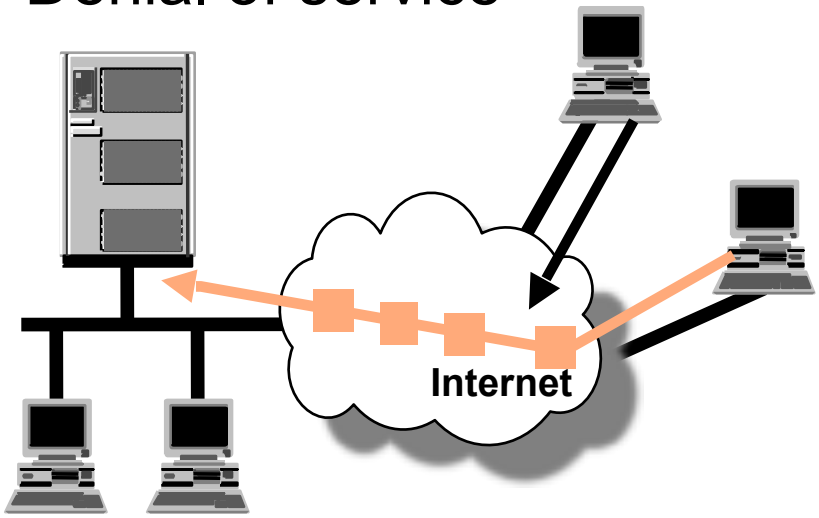


Spoofing

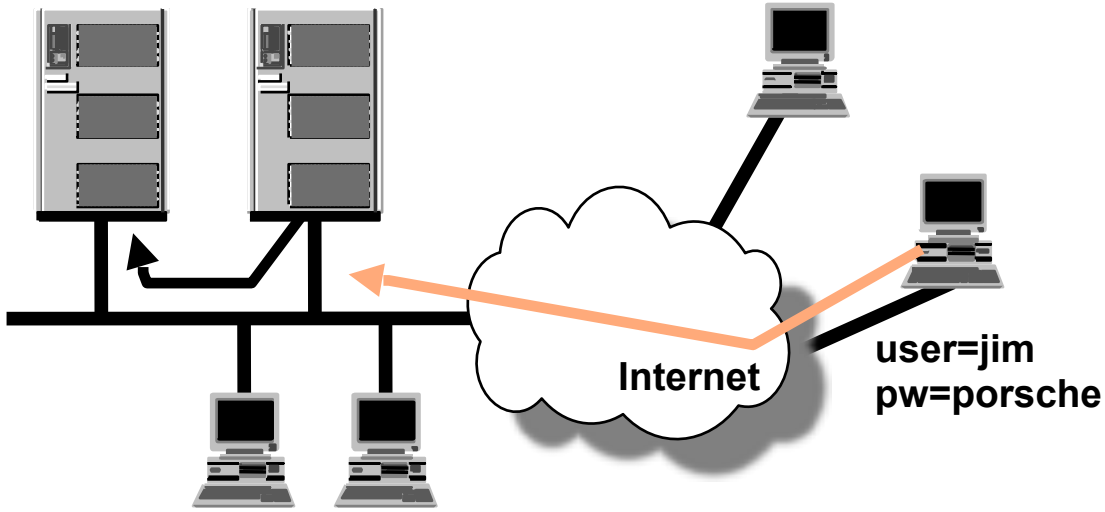


addr= 192.168.67.3

Denial of service



Trusted host



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

A brief word about your organization's Internet security policy

- Inbound access
  - What applications are exposed to the Internet?
  - What are the security threats and vulnerabilities for each application?
  - What security countermeasures can be implemented to reduce or eliminate the risks?
  - Is there still a risk? If yes, do the benefits outweigh the risks?
- Outbound access
  - Who can access the Internet from the secure network?
  - What TCP/IP applications can they use?
  - What are the risks?
  - What security countermeasures can be implemented to reduce or eliminate the risks?

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

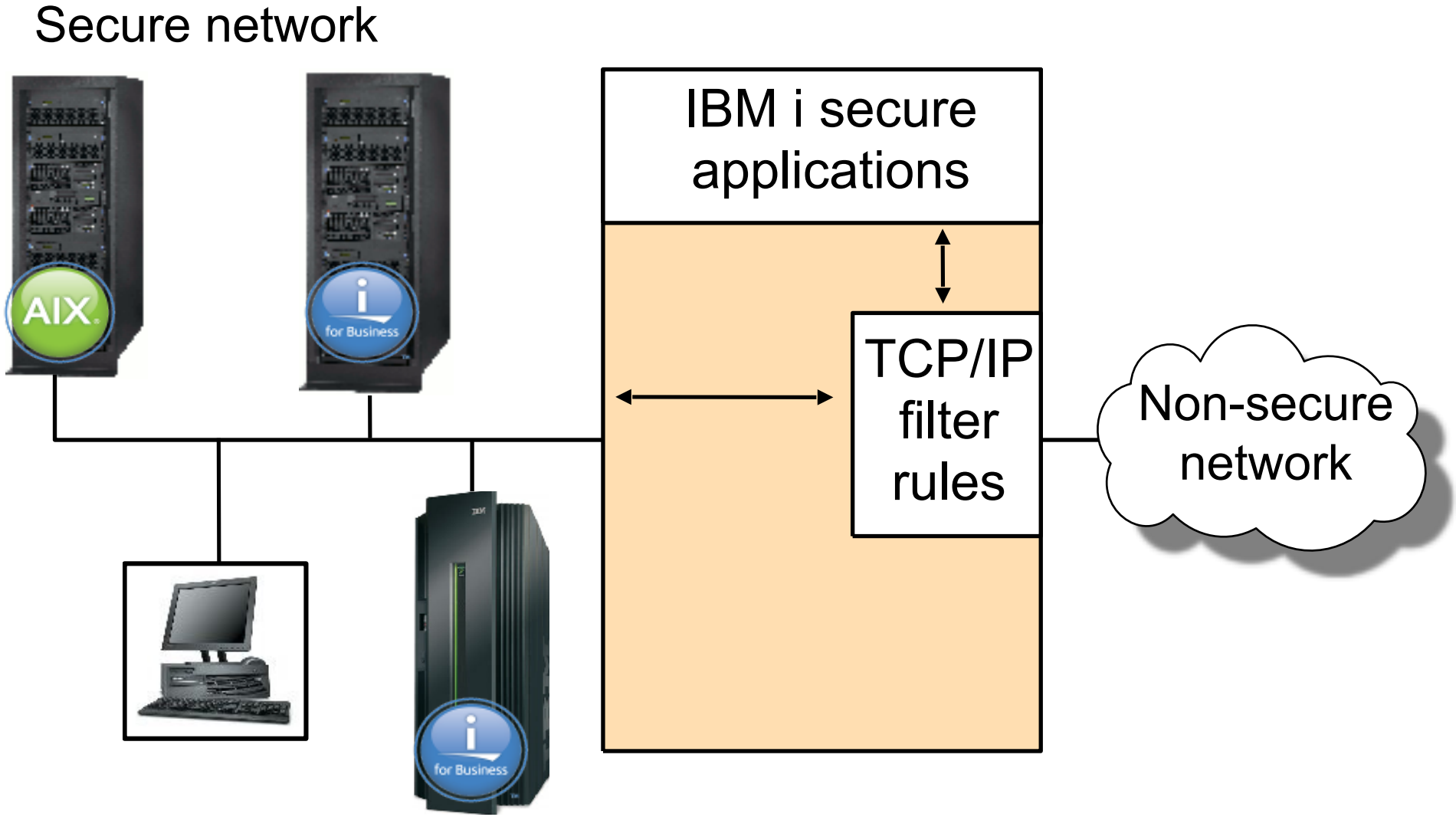
What IBM i V7 can do

- IP packet filter
- Proxy server (for HTTP, using Apache)
- Intrusion Detection System (IDS) / Intrusion Prevention System (IPS)
- Virtual private networking (VPN)
- Digital Certificate Manager (DCM) to manage digital certificates
- Secure Socket Layer (SSL) / Transport Layer Security (TLS) to secure Telnet, FTP, LDAP, IBM System i Access, Management Central, DRDA, DDM, POP, SMTP, WebSphere Application Server, and so forth
- SOCKS
- Cryptographic hardware
- Network authentication service (Kerberos)
- Object signing and signature verification
- Single signon
  - Enterprise Identity Mapping (EIM)
- Anti virus scanning enablement
- Application administration and exit points

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

IP packet filters

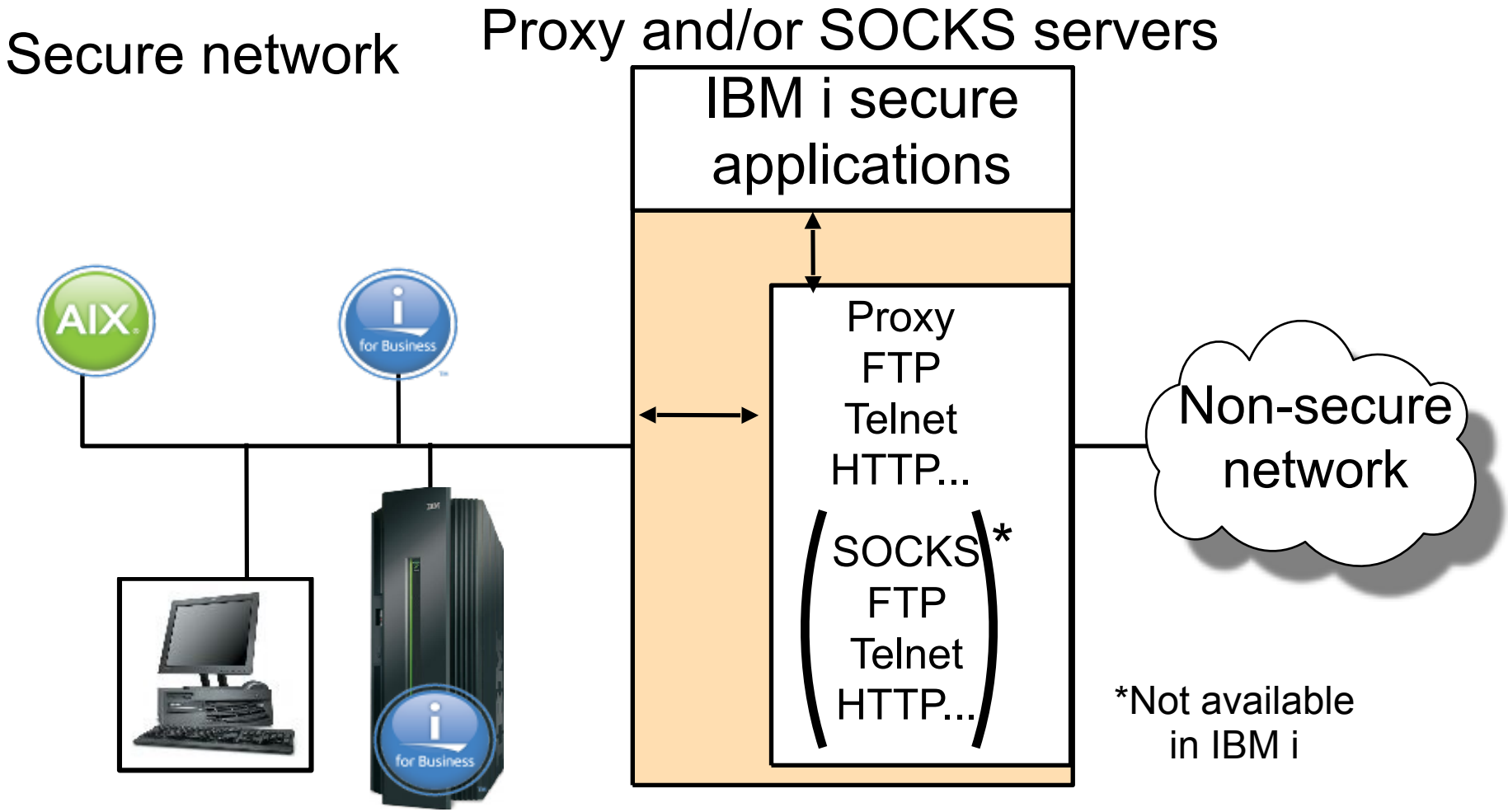
- Inbound and outbound traffic tested against the filter rule
- Either permitted to pass or denied



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

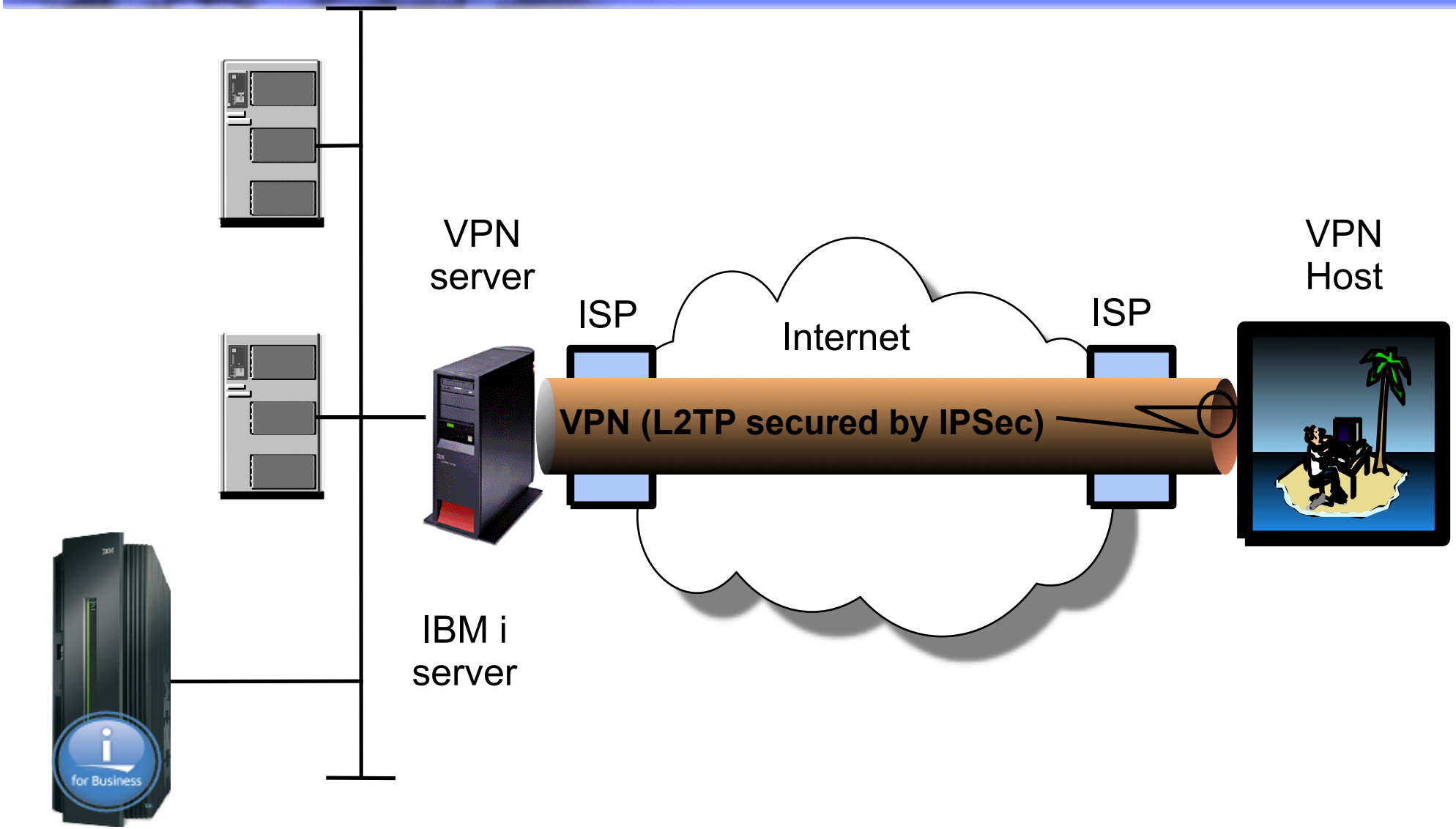
Proxy, SOCKS servers

- Internal user first connects to the proxy or SOCKS.
- Proxy or SOCKS makes connection to target system.
- Only the non-secure attributes of the firewall are exposed to the Internet.
- IBM i HTTP Server can be a forward and reverse proxy server.



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Virtual private networking (VPN)



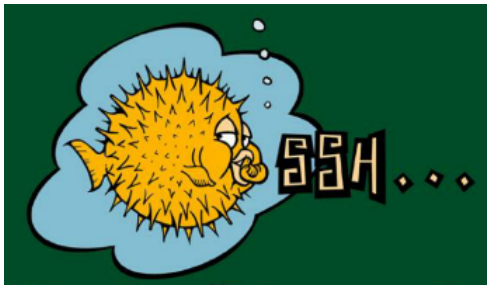
© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Securing IBM i applications with SSL

- IBM HTTP Server for IBM i
- IBM i Access applications, including IBM System i Navigator, and applications that are written to the IBM System i Access set of application programming interfaces (APIs).
- Telnet client and server
- FTP client and server
- Distributed Relational Database Architecture (DRDA) and Distributed Data Management (DDM) / ODBC / JDBC
- Management Central
- Directory Services client and server (LDAP)
- Mail services (SMTP client and server, POP server)
- Programs developed with Developer Kit for Java and client applications that use IBM Toolkit for Java.
- Programs developed with Secure Socket Layer (SSL) application programming interfaces (APIs), which can be used to enable SSL on applications.

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

OpenSSH introduction (1 of 2)



- Secure Shell (SSH) is a program to log into another computer over a network connection to run commands and copy files between computers.
- Entire data traffic is encrypted including user and password information.
- SSH is subject to licensing requirements.
- OpenSSH is the free version of the SSH protocol suite.
  - It does not use any patented components, such as the IDEA encryption algorithm.
- Several utilities are available with OpenSSH, including:
  - ssh: A secure command shell
  - sftp: A secure FTP alternative
  - scp: A secure file copy program
  - ssh-keygen: A public/private key pair generation and management tool
  - ssh-agent: An authentication agent that can store private keys
  - ssh-add: Used to add private keys to a running ssh-agent
  - sshd: A daemon (server) program that handles incoming ssh connections
- Two protocols are available: SSH1 and SSH2

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

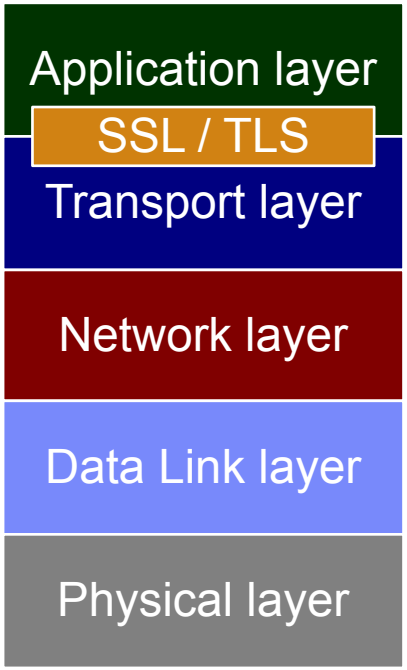
OpenSSH introduction (2 of 2)

- OpenSSH also supports the following services and functions:
  - X11 forwarding
    - X11 forwarding allows the encryption of remote X windows traffic
  - Port forwarding
    - Port forwarding allows forwarding of TCP/IP connections to a remote system over an encrypted channel
  - Data compression
    - Uses zlib for compression
  - Kerberos and AFS ticket passing
    - Passes tickets for Kerberos and AFS on to the remote machine
  - Cryptographic functions
    - Uses the OpenSSL cryptographic library
  - Information can be found at http://www.openssh.org

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

OpenSSL

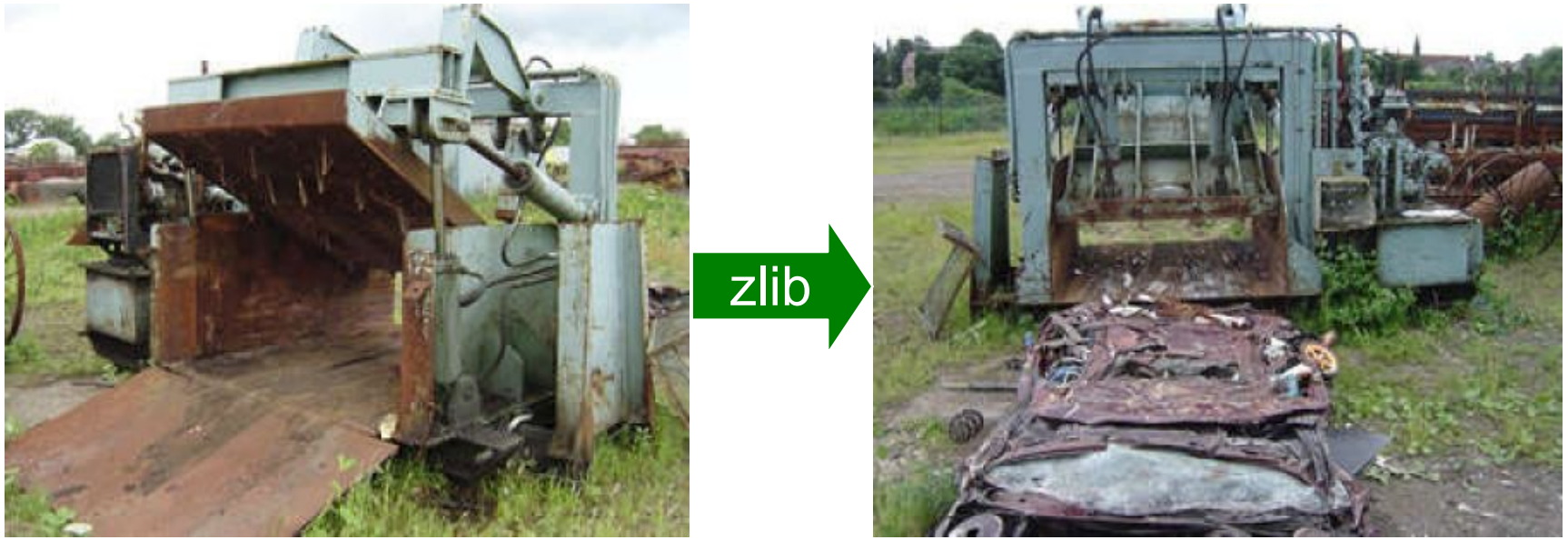
- OpenSSL refers to an open source project that provides a full-featured SSL implementation.
- It supports:
  - Secure Sockets Layer V2 and v3
  - Transport Layer Security V1
  - A general purpose cryptographic library
- Open SSL allows programmers to write SSL/TLS sockets applications that can run on any platform that supports OpenSSL.
- openssl command line tool can be used for:
  - Creation of RSA, DH, and DSA key parameters
  - Creation of X.509 certificates, certificate signing requests (CSRs), and certificate revocation lists (CRLs)
  - Calculation of message digests
  - Encryption and decryption with ciphers
  - SSL/TLS client and server tests
  - Handling of S/MIME signed or encrypted mail
- Information is available from http://www.openssl.org



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Compression using zlib

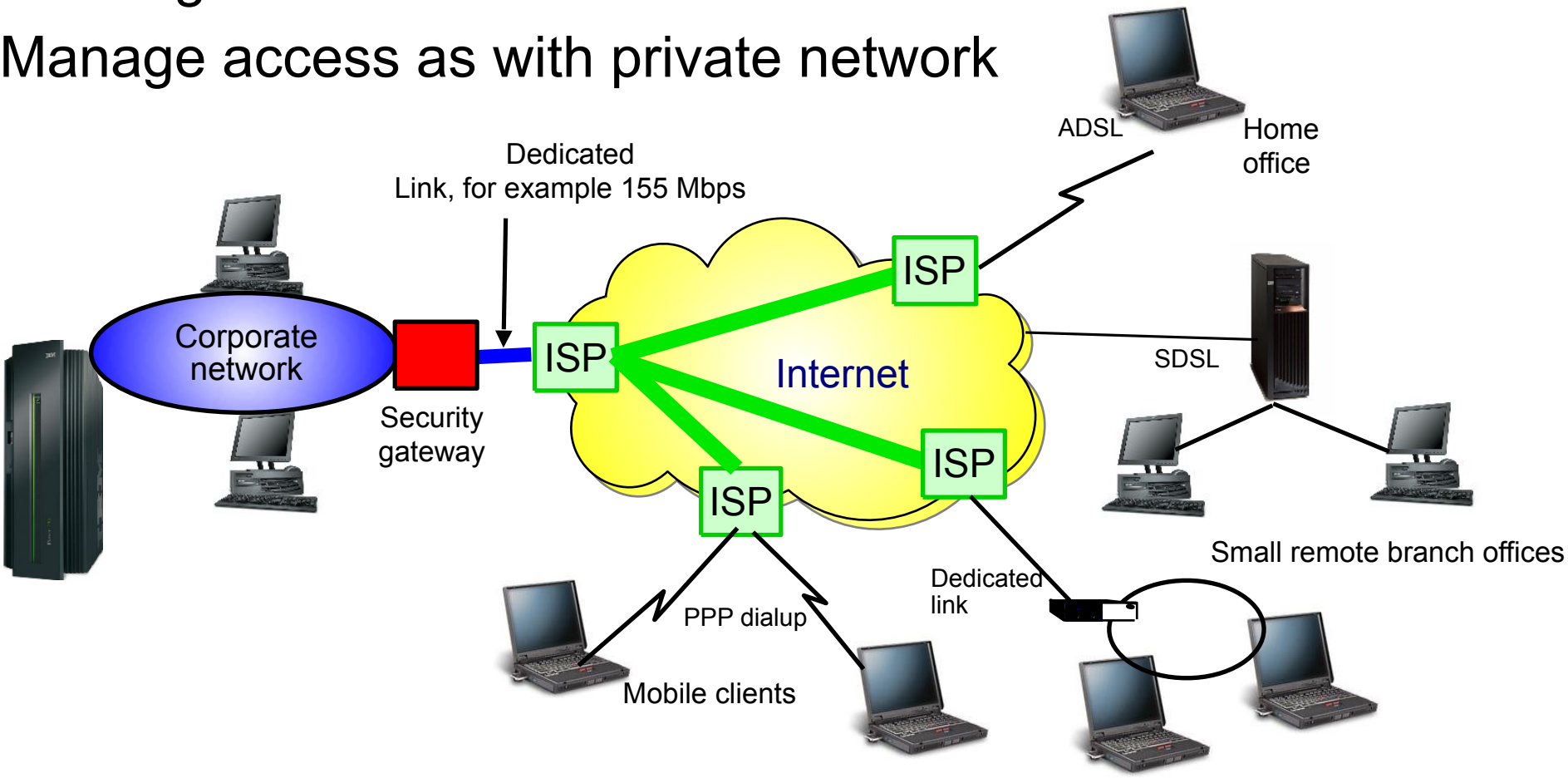
- zlib is a public compression algorithm that:
  - Does not use patented material
  - Is used in many compression products
  - Can be freely downloaded and used for any purpose (personal or commercial)
  - However, is not the fastest algorithm available
- Information is available from http://www.zlib.net



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Virtual private networking

- Authenticate incoming data traffic
- Maintain data privacy
- Leverage ISP access locations
- Manage access as with private network



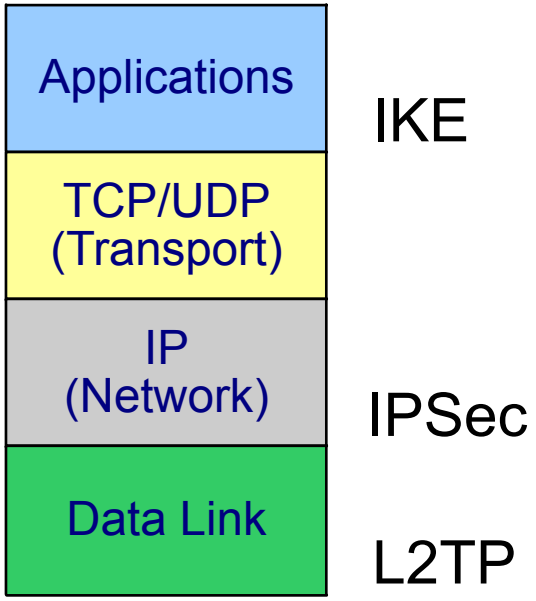
Secure extension of your company's private intranet across a public network

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

VPN protocols

IP Security Architecture Protocols (IPSec)

- Open, standards-based, network layer security technology
- Supports authentication, integrity checking and encryption per packet
- Provides key management solution by using the Internet Key Exchange (IKE) protocols (used to be ISAKMP/Oakley)
- IETF standard in IPv6 (optional in IPv4)
- Used to secure L2TP tunnels



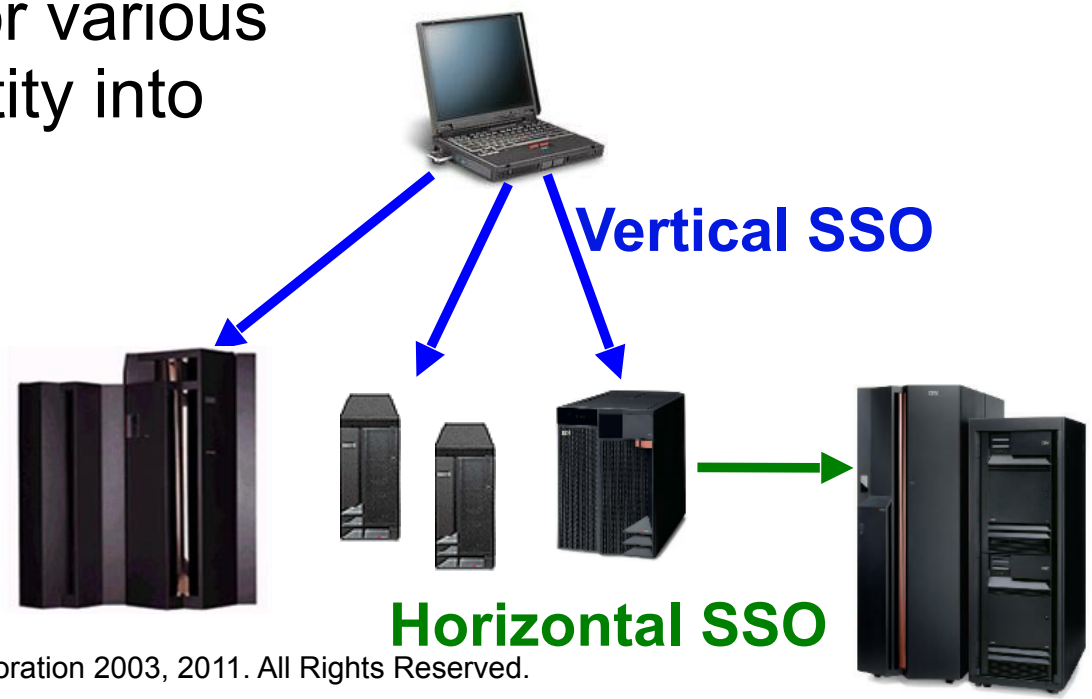
Layer 2 Tunneling Protocol (L2TP)

- Open, standards-based link layer technology
- Transports multiprotocol data over the Internet
- Cost-effective; extends PPP connections to destination network
- IETF Internet draft, but emerging industry standard
- No inherent security features; use IPSec for security

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Single sign on (SSO) characteristics

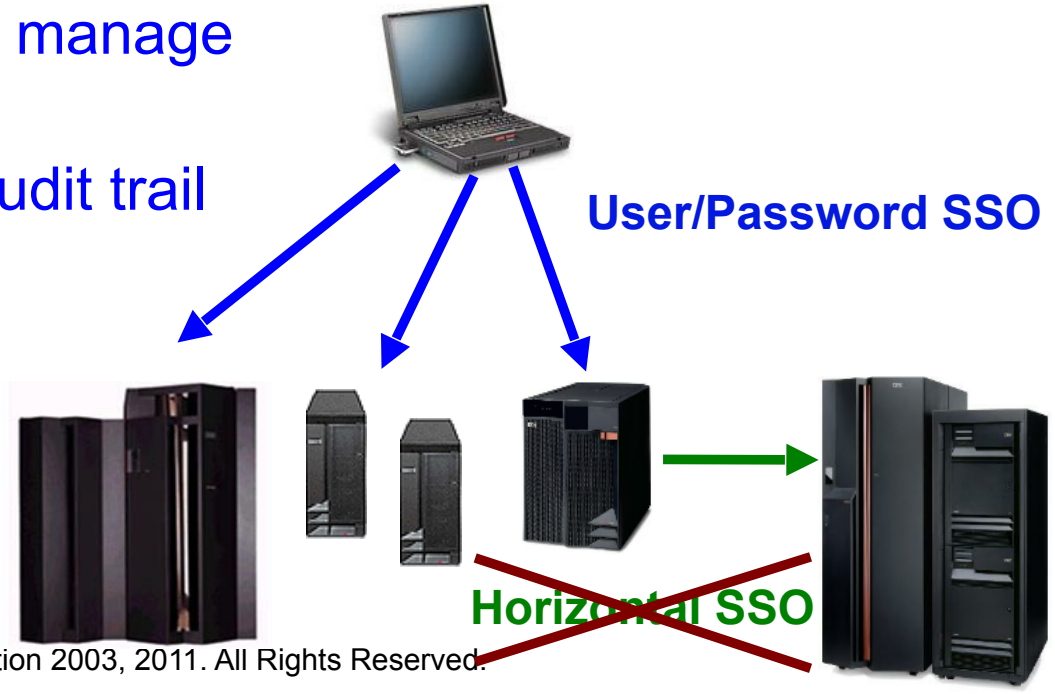
- Sign on once to the network using, for example, user ID and password.
- Subsequent connection requests to application services and resources are authenticated without prompting for the user ID or password.
  - Network authentication protocols, such as Kerberos, are used to perform authentication
- Taking different identities for various applications for a single entity into consideration is desirable.



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Single sign on solution using user/password authentication

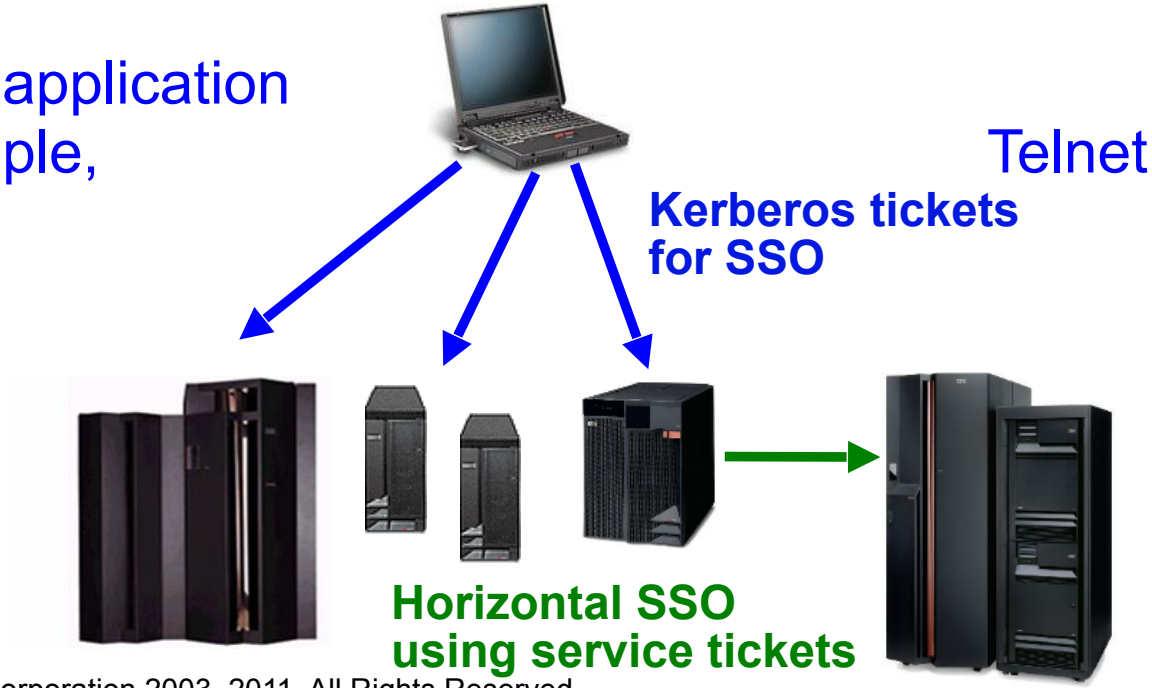
- Pros
  - Relatively simple to implement
  - Covers basically every application signon that requires user and password
- Cons
  - Users and passwords are stored centrally or decentralized
  - Passwords are decryptable!!!
  - Does not eliminate the need to manage passwords on all platforms
  - No multi-tier support, bad for audit trail



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Single sign on solution using network authentication

- Kerberos is an example of a widely used network authentication protocol.
- Pros
  - Eliminates the need to manage passwords on application systems
  - Does not rely on passwords for authentication, it is ticket based
  - No passwords are stored in decryptable form
- Cons
  - Requires support for every application (client and server, for example, client and Telnet server)



© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

Advantages and risks of SSO

- Advantages
  - Reducing the number of calls to the help desk for password resets
  - Simplifying sign-on processes
  - Allows stronger passwords
- Risks
  - If the password for initial authentication is compromised, an intruder has full access to all applications for that user
  - If a workstation is left unlocked and unattended, someone could log in to all SSO-enabled applications
- Recommendations
  - User awareness education
  - Lock the workstations after a certain amount of idle time with a password-protected screen saver
  - Use smart cards/public key authentication for initial login

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.

THANK YOU!

Further IBM Education information

https://edu.arrowecs.eu/ibm/uk/index.html

© Copyright IBM Corporation 2003, 2011. All Rights Reserved.