



IBM eServerJ iSeriesJ

Session:

OS/400 Security and the Internet

Patrick Botz
Lead iSeries Security Architect
eServer Security Architect

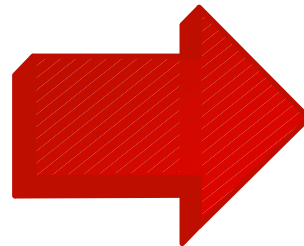
© Copyright IBM Corporation, 2003. All Rights Reserved.
This publication may refer to products that are not currently available in your country. IBM makes no commitment to make available any products referred to herein.

Agenda

- The Internet Security Threat
- Protecting the Back Door
- Protecting the Front Door
 - ◆ Establishing a Security Policy
 - ◆ Protecting a Public Server

Internet Security Threat

Internet Is a Desirable Place to Do Business



Makes it Attractive Place to Steal From Business

2002 CSI/FBI Survey: 41 companies said they lost \$170.8M from theft of proprietary information.

Forrester survey - type of IT security incidents that possess most threat:
30% Intellectual property theft, 30% Malicious code, 22% Financial fraud,
8% Denial of service attacks, 5% Unauthorized access, 2% Human error

Internet Fraud Complaint Center; rose from 48,252 reported in 2001 to 75,063 in 2002.
Monetary loss associated with fraud more than tripled, to \$54M from \$17M in same period.

Internet Security Issues

How do we make the Internet a safe place to do business ?

- Confidentiality/privacy
- Integrity
- Authentication
- Non-repudiation

Resources to Protect

f **There are many things that must be protected**

f *Public systems*

f *Private systems*

f *Network*

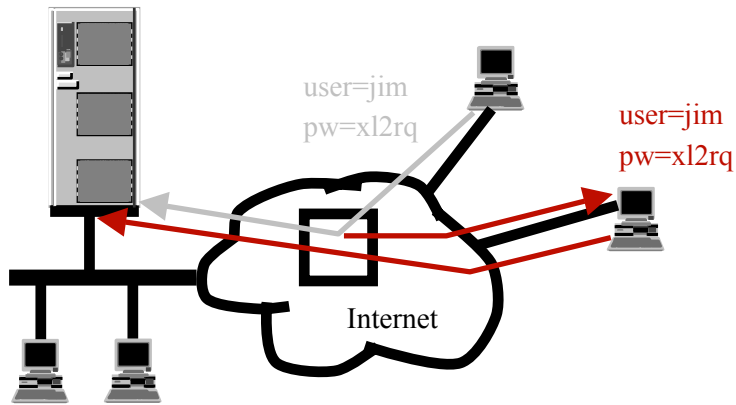
f *Data*

f *Transactions*

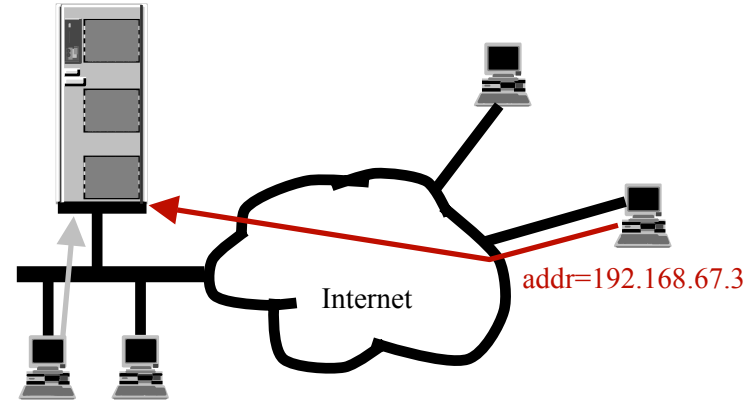
f *Reputation*

Example Internet Security Exposures

Sniffing



Spoofing



Worms

Worms

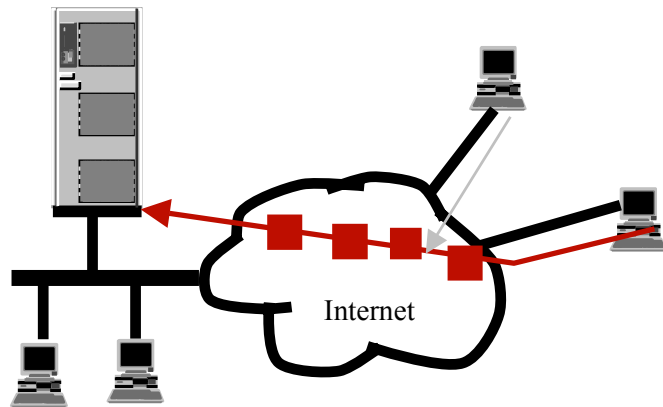
Buffer Overflows

Trojan Horses

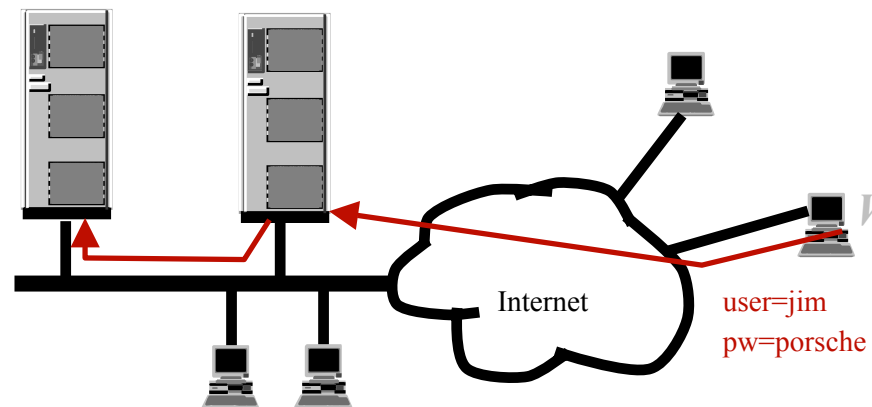
Buffer Overflows

Buffer Overflows

Denial of service



Trusted hosts

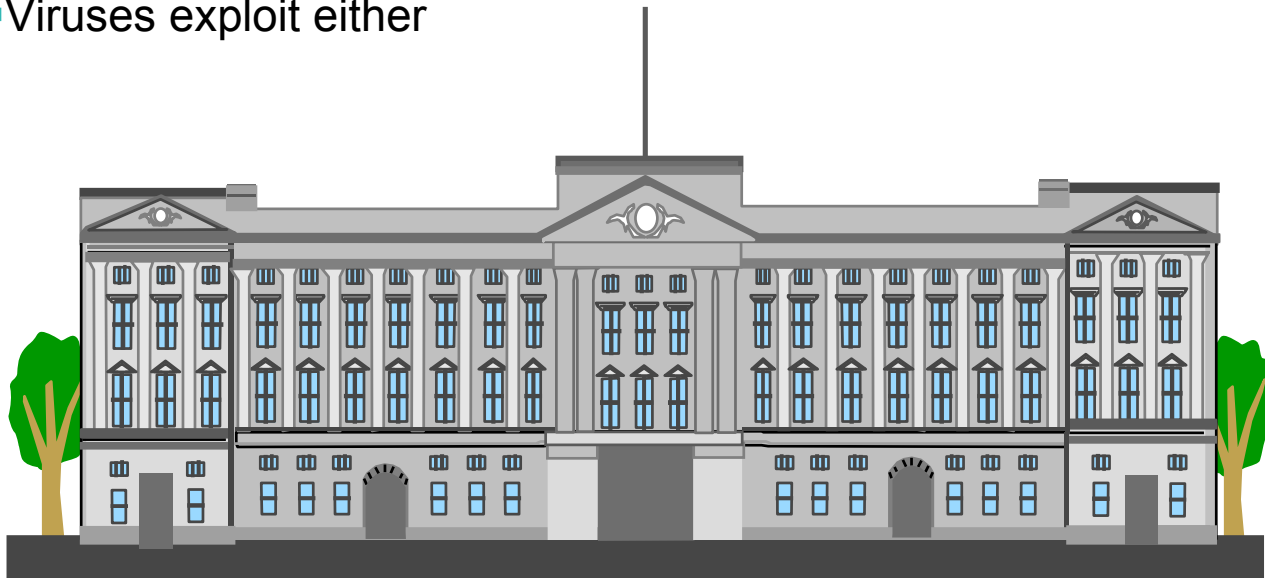


Worms

Worms

Protecting Front Doors and Back Doors

- Back door attacks "sneak" into your system
 - f* poorly architected OS and application interfaces
 - f* e.g. worms, buffer overflow attacks
- Front doors necessary to conduct business
 - f* usually exploited by fraudulent claims
- Viruses exploit either



Protecting the Back Door

OS/400 -- Architected Virus Resistance

- Object based architecture
- Dual Stack -- buffer overflow cannot take over system
- Only OS can manufacture pointers
- Detect programs "claiming" to be OS programs
 - f* Digitally signed OS

OS/400 protects the back door so you can concentrate on the front door!

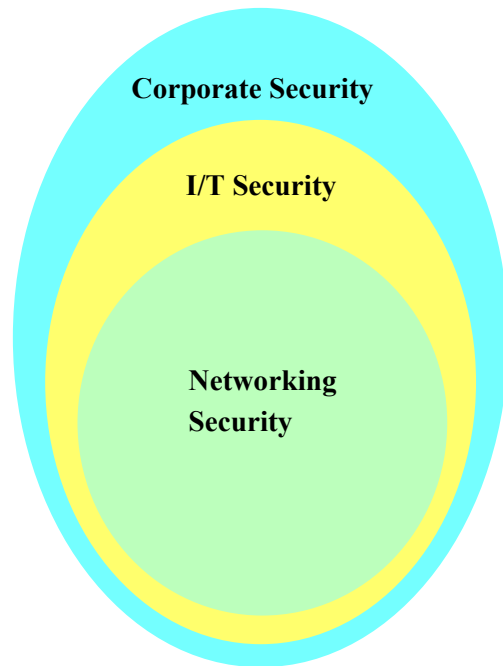
See "Virus Got You Down?" White Paper -- <http://www.skyviewpartners.com>

Protecting the Front Door

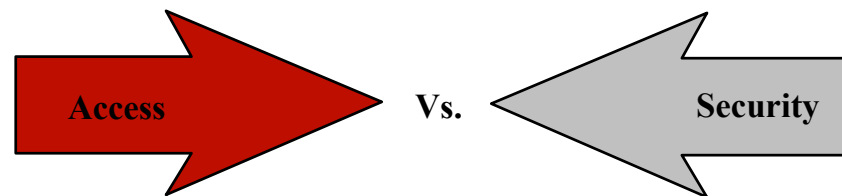
- Your responsibility
- Requirement: Security Policy
- Internet Security Principals

Internet Security Policy

What are your security policies?

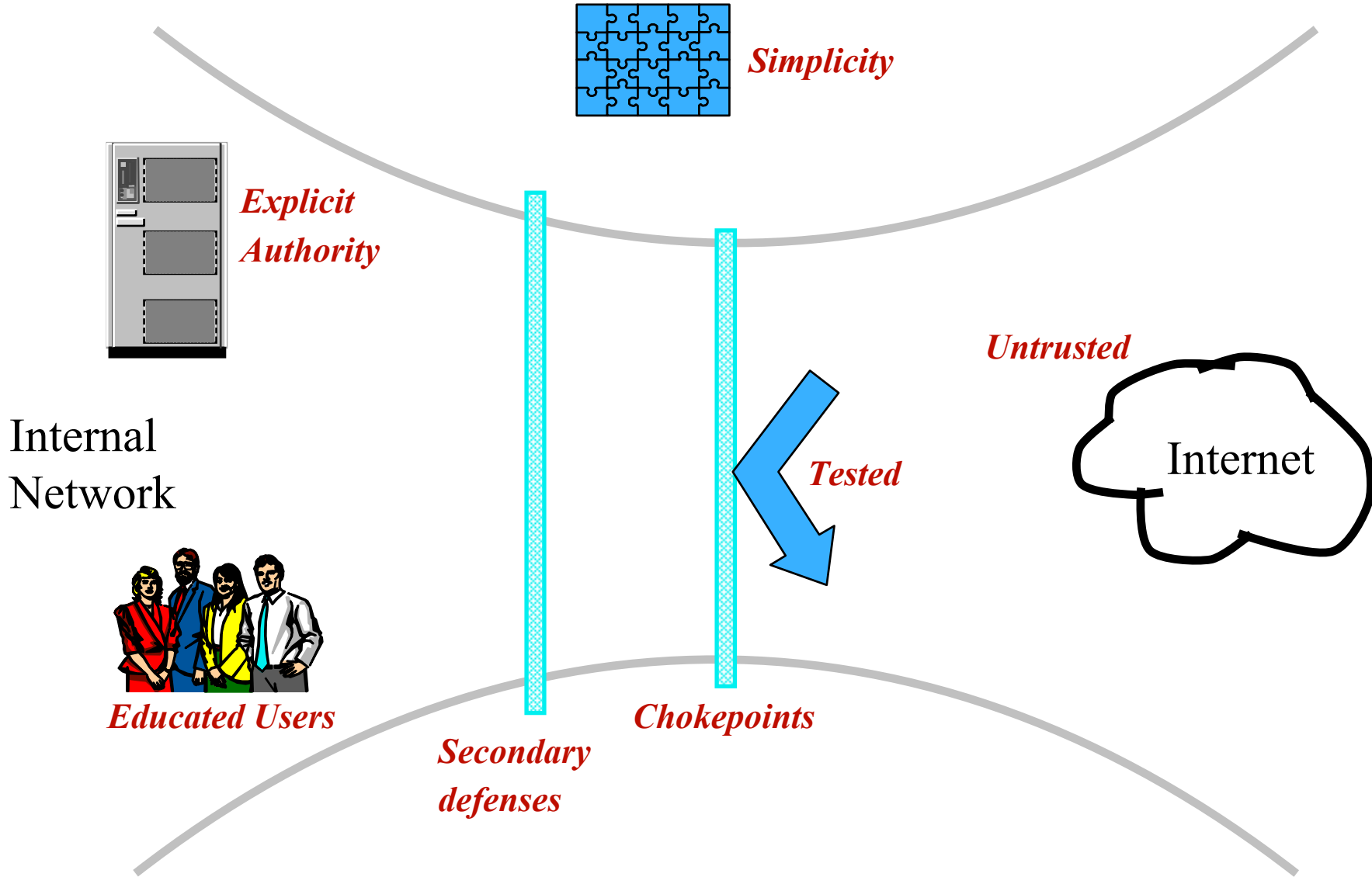


- f* What services are to be permitted (http, ftp, telnet...)?
- f* What Internet sites may be accessed?
- f* What may be accessed from the Internet?



- f* FTP access<-> PC virus introduction
- f* Mail exchange<-> mail flooding
- f* Web server <-> web graffiti

Internet Security Principles

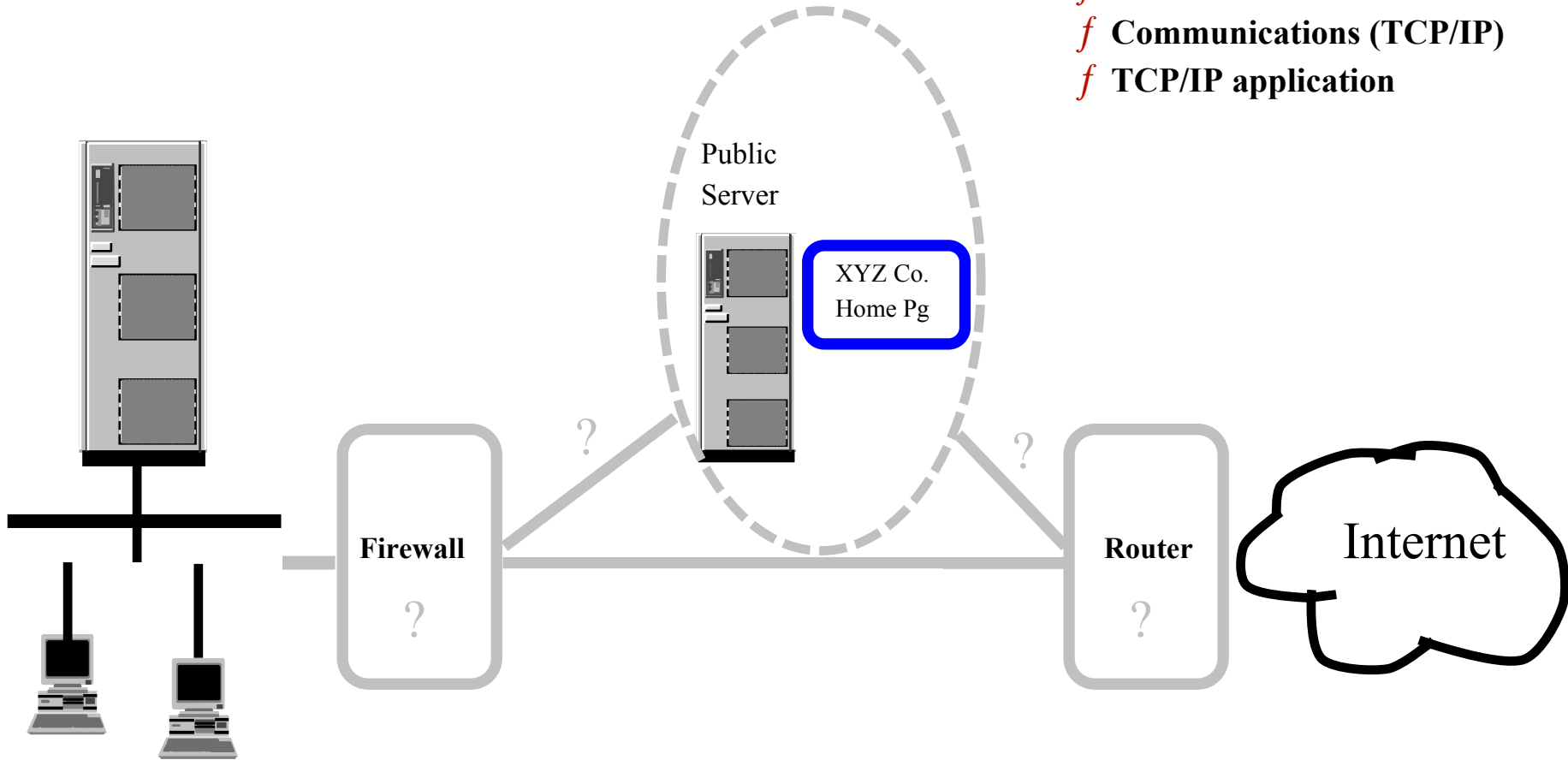


Protecting a Public Server

Public server must be secured even if it is isolated or if you have a firewall.

Layers of security

- f* Internet Service Provider
- f* Host
- f* Communications (TCP/IP)
- f* TCP/IP application



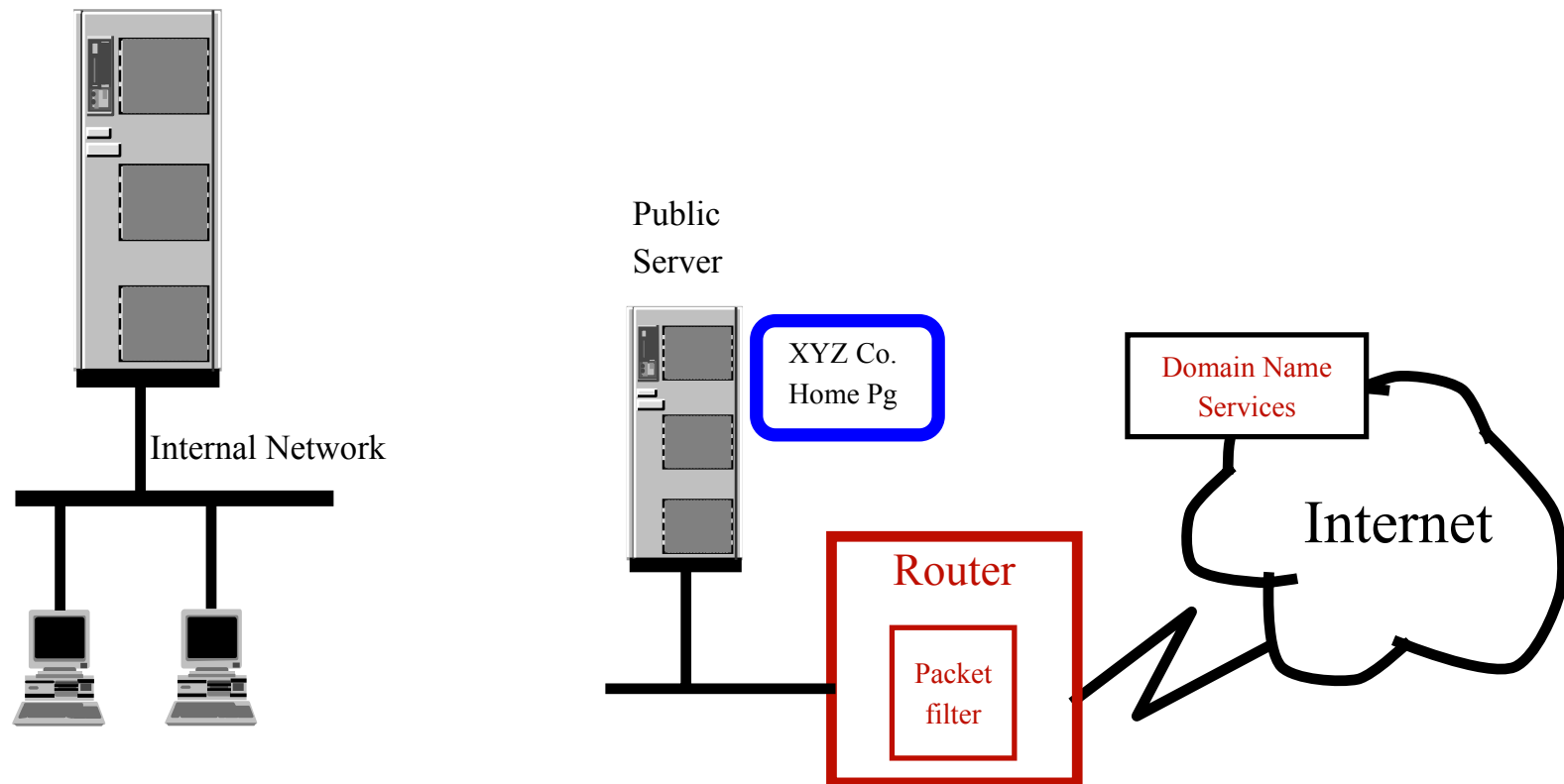
Internal Network

Internet Service Provider Security

Block incoming telnet connections

Block finger, snmp, ...

Provide Domain Name Services



OS/400 Host Security

You manage the front door letting in only those you people and things you choose to.

Configure

f System Security Configuration

- iSeries Navigator Security Wizard; OR
- <http://www.ibm.com/servers/security/planner>

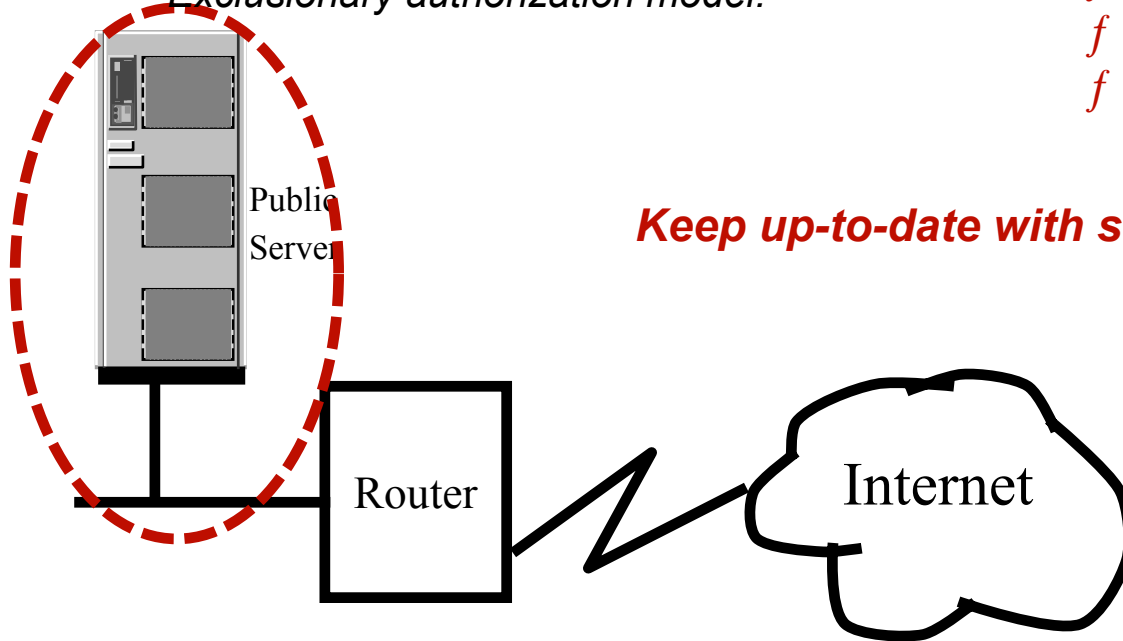
eServer Security Planner

f Object level resource access control
Exclusionary authorization model!

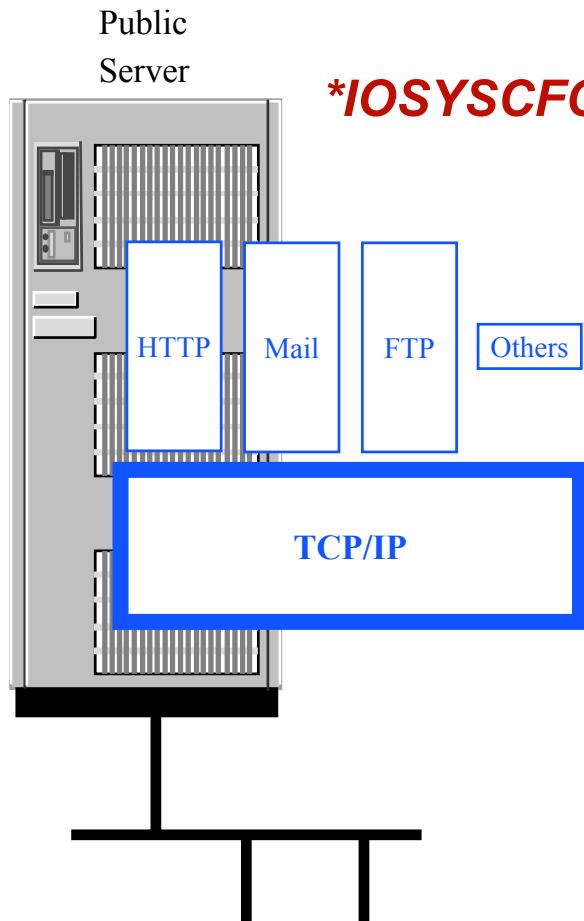
Verify and Monitor

- f* GO SECTOOLS or GO SECBATCH
- f* Check passwords (ANZDFTPWD)
- f* Check security relevant values (PRTSYSSEC)
- f* Use QSYSMSG message queue
- f* Security Wizard
- f* Third party packages

Keep up-to-date with security PTFs



TCP/IP Security



****IOSYSCFG authority controls who can make changes***

Only start TCP/IP applications you need

- f* CHGCMDDFT CMD(STRTCPSVR)
NEWDFT('SERVER(*HTTP)')
- f* CHGTELNA AUTOSTART(*NO)
- f* CHGWSGA AUTOSTART(*NO)...

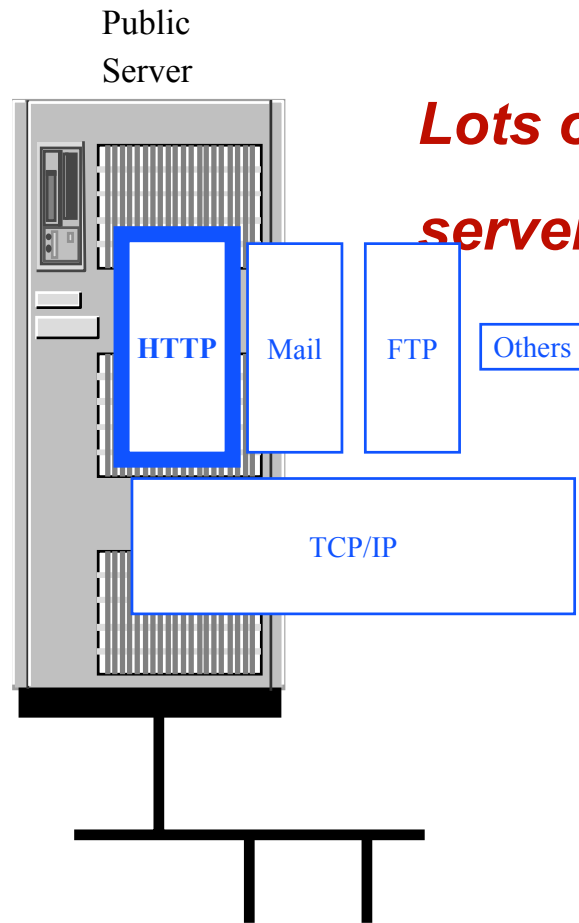
No IP forwarding

- f* CHGTCPA IPDTAGFWG(*NO)

Don't define host name of internal systems

Define only one route (default)

Web Server Security



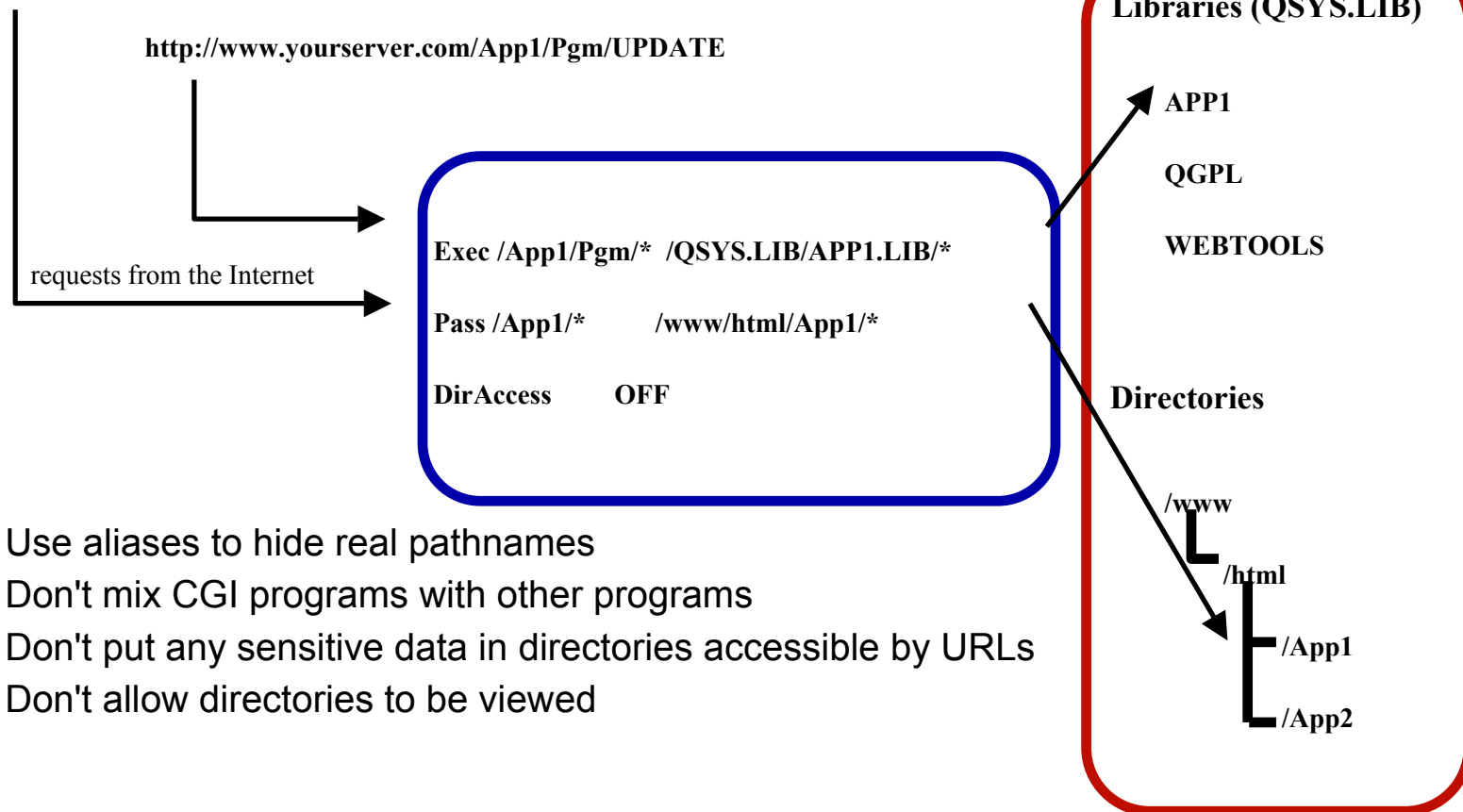
Lots of things to consider when securing web servers and web applications!

- f* Server directives
- f* Protection directives
- f* Secure data transmission (encryption over the wire)
 - Secure Sockets Layer (SSL)
 - Digital Certificates
 - Managing digital certificates
- f* CGI-BIN programs
- f* Java Servlets

Web Server Configuration Directives

Server directives control which directories can be accessed

`http://www.yourserver.com/App1/Main.htm`



- f* Use aliases to hide real pathnames
- f* Don't mix CGI programs with other programs
- f* Don't put any sensitive data in directories accessible by URLs
- f* Don't allow directories to be viewed

Web Server Protection Directives

Server *PROTECTION* directives control who can access data

Application #1 - public application

- f* No userid or password required
- f* Programs and data are accessed using a default profile (e.g. QTMHHTTP)

Sample Security Models ***Application #2 - employees only***

- f* AS/400 user profile and password required (basic authentication)
- f* Programs and data are accessed using the user profile

Application #3 - limited set of Internet users only

- f* "Internet userid" and password required (basic authentication)
- f* Userid are entries in a Validation List object
- f* Programs and data are accessed using a default profile (e.g. WEBAPP3)

Normal iSeries object level security "backs up" the server directives

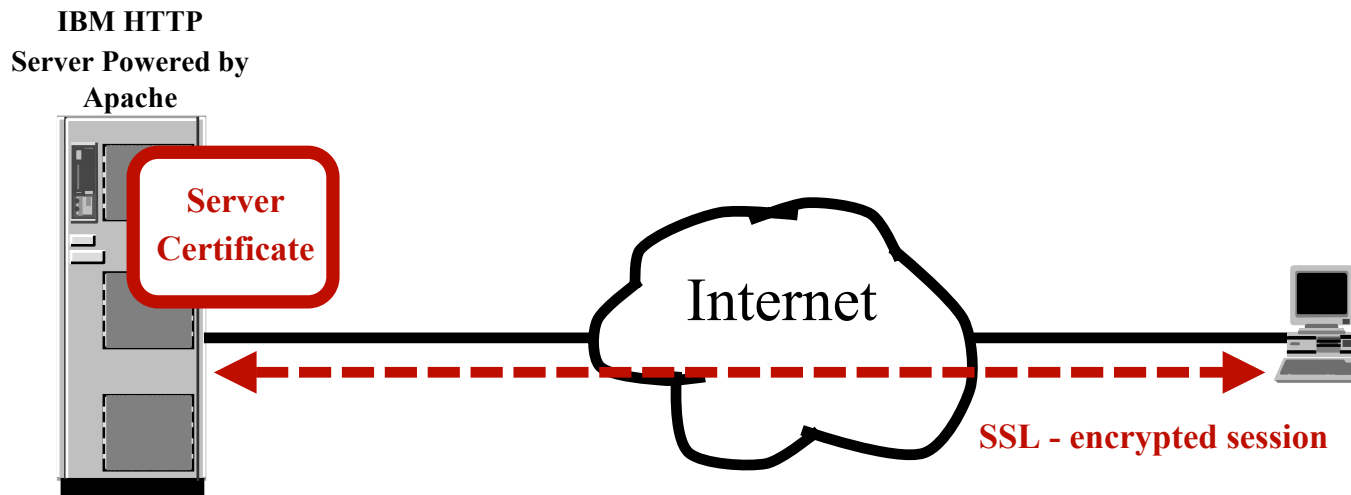
Additional Web Server Considerations

Securing the public server is not enough

- f* Internet users want secure communications (e.g. passwords)
- f* Internet users want secure transactions (e.g. credit card numbers)

HTTP Server Powered by Apache

- f* Provides encryption support for HTTP
- f* Secure Sockets Layer (SSL)
- f* Digital Certificate Manager



CGI-BIN Considerations

Validate form input - HTML can be changed

```
<p>Pick the flavor to order:
<form method="POST" action="update">
<select name="flavor">
<option>grape
<option>orange
<option>cherry
</select>
<input type="submit" value="OK">
</form>
```

What came back

What was sent

```
<form method="POST"
action="http://yourserver.com/cgi-bin/update">
<select name="flavor">
<option selected>apple
</select>
<input type="submit" value="OK">
</form>
```

Hidden variables aren't really hidden

```
<form method="POST" action="/cgi-bin/query">
<input type="hidden" name="employeenum" value="12345 ">
<input type="submit" value="Query current salary">
</form>
```

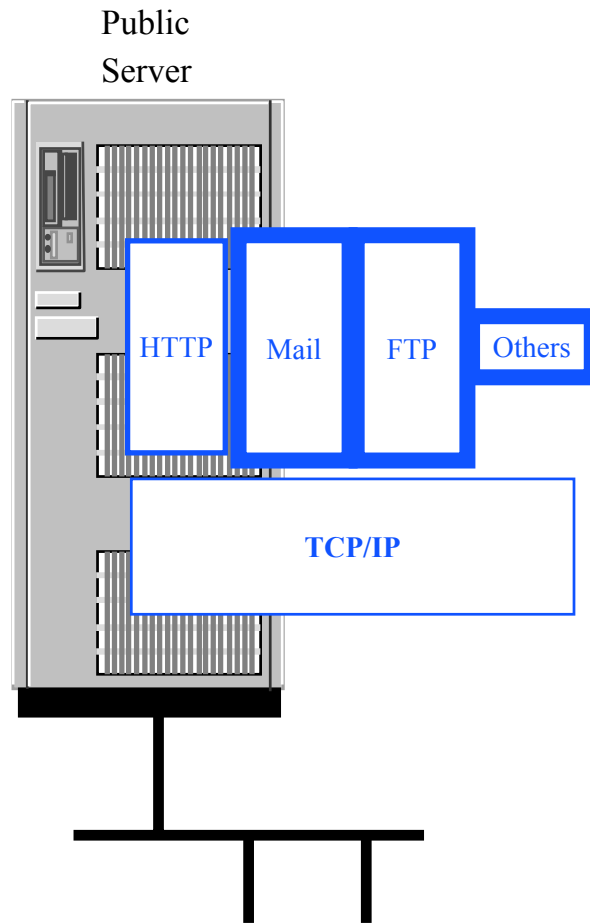
What was sent

What came back

```
<form ...
... value="09876 ">
...
</form>
```

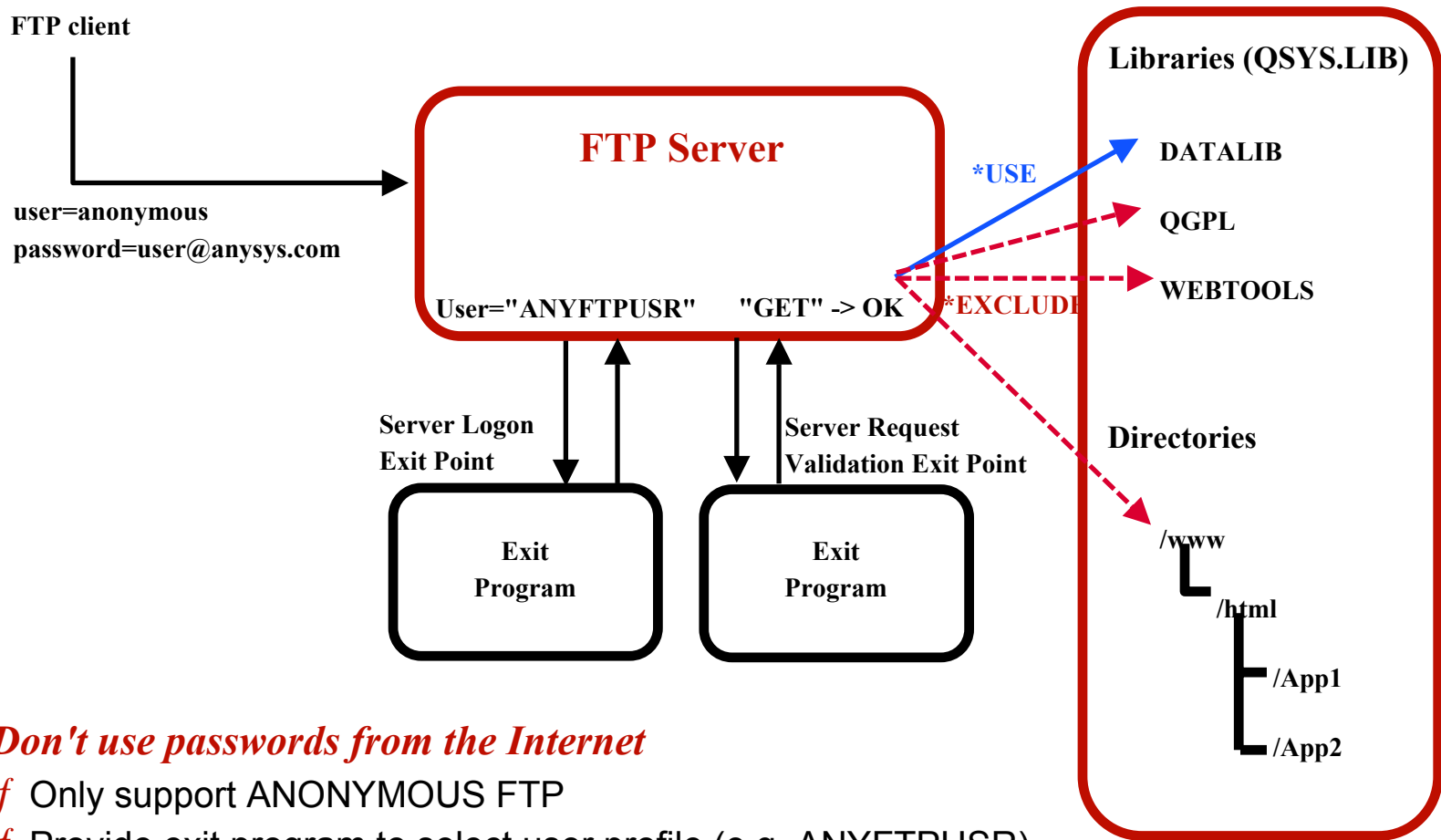
Javascript field auditing can be disabled

Securing Other TCP/IP Applications



- f* FTP
- f* Mail
- f* Various other applications

FTP



Don't use passwords from the Internet

- f* Only support ANONYMOUS FTP
- f* Provide exit program to select user profile (e.g. ANYFTPUSR)
- f* Provide exit program to determine allowed operations (e.g. GET only)
- f* Strictly limit access of FTP user
- f* Don't rely on client's IP address

Mail

A public server should have limited or no mail support

f Don't want to store mail on system accessible by the public

f Not for general mail delivery

f Set auxiliary storage threshold

f No *ANY *ANY directory entry

SMTP mail  support@yoursys.com

Directory entries

```
- INFO          YOURSYS
- SUPPORT      YOURSYS
```

Other TCP/IP Applications

When the iSeries system is accessible from the Internet



Telnet

- Don't start it! But if you must...
- Set QLMTSECOFR, QMAXSIGN, QMAXSGNACT, QAUTOVRT
- Set maximum storage per user profile



SNMP

- Don't start it! But if you must...
- Set community name (like a password)
- Only allow GETs



LPD

- Don't start it!



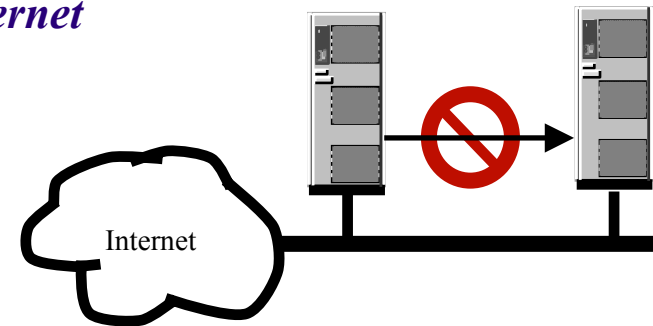
TCP/IP File Server

- Don't install it!

Preventing Hacker Written Applications

When the iSeries system is accessible from the Internet

- Don't allow trojan-horse applications to be installed
- Don't allow your system to be used to attack others
 - Don't install compilers
 - Restrict usage of TCP/IP communications



TCP/IP port restrictions can limit usage of well known ports (ADDTCPPORT)

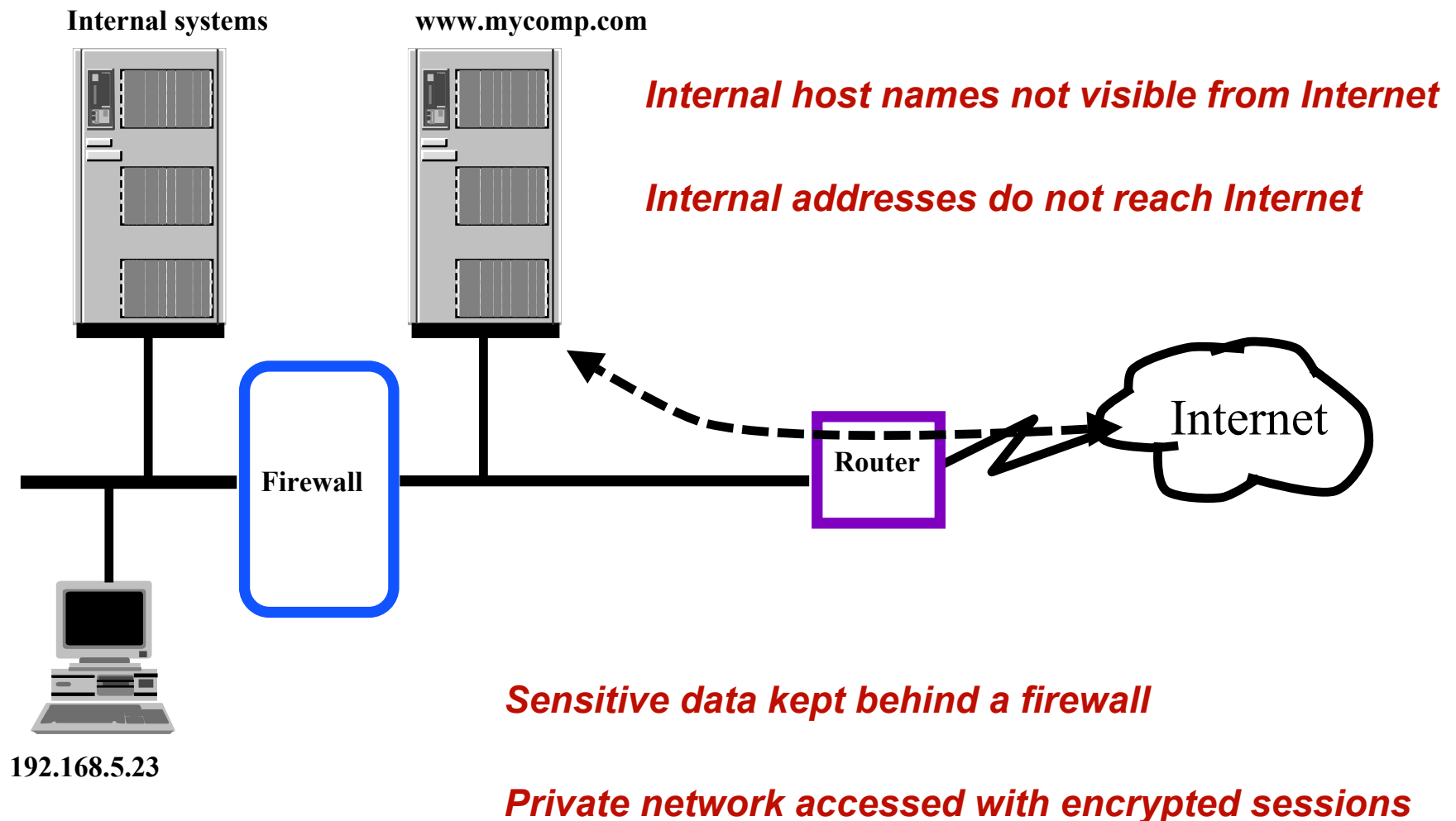
Lower port	Upper port	Protocol	User profile (deny/permit)
23 (telnet)	*only	*tcp	QUSER/--
20 (ftp)	21	*tcp	QUSER/QTCP
25 (smtp)	*only	*tcp	QUSER/--
80 (http)	*only	*tcp	QUSER/QTMHHTTP
5061 (wsg)	*only	*tcp	QUSER/QTMTWSG
161 (snmp)	*only	*tcp	QUSER/--
161 (snmp)	*only	*udp	QUSER/--

Restrict use of sockets APIs

- Service programs QSOSRV1, QSOSRV2, and QYSOSSLR --> PUBLIC(*EXCLUDE)
- Authorize specific profiles to the service programs (QTCP, QTMHHTTP...)

Protecting Internal Servers

What we haven't talked about



iSeries Internet Security Summary

The Internet can be a reasonably safe place to do business

- f* Caution is advised, poor planning or mistakes could be disastrous
- f* Cryptography plays a major role
- f* Internet security is still evolving

iSeries security features make it a good Internet Server

- f* Proven operating system integrity
- f* Excellent host level security
- f* Integrated communications security
- f* Secure HTTP serving

Additional Resources

- f* <http://www.ibm.com/series/infocenter>**
- f* Tips and Tools for Securing Your iSeries, SC41-5300-05**
- f* Building Internet Firewalls; Chapman and Zwicky, O'Reilly and Associates 1995, ISBN #1565921240**
- f* <http://www.ibm.com/servers/security/planner>**
- f* iSeries Navigator Security Wizard**
- f* eServer EXTRA focuses on iSeries application development -- to subscribe, send an e-mail to:
serverextra@mspcommunications.com**
- f* *eServer ADMINISTRATOR focuses on security, systems management and related topics -- to subscribe, send an e-mail to:
eserveradministrator@mspcommunications.com**
- f* Experts Guide to OS/400 Security
Carol Woodbury and Patrick Botz
ISBN 1-58304-096-X
29th Street Press, 2003
<http://www.pentontech.com/education>**
- f* OS/400 Virus White Paper <http://www.skyviewpartners.com>**

© IBM Corporation 1994-2002. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

Instruction: Refer to the following URL: <http://iplwww.ncastle.ibm.com/wpts/trademarks/trademar.htm>. Edit the list below, IBM subsidiary statement, and special attribution companies which follow so they coincide with your presentation.

AS/400	IBM(logo)
AS/400e	iSeries
AS/400e (logo) business	OS/400
IBM	

Lotus, Freelance Graphics, and Word Pro are registered trademarks of Lotus Development Corporation and/or IBM Corporation.

Domino is a trademark of Lotus Development Corporation and/or IBM Corporation.

Instruction: For a complete list of Lotus/IBM trademarks, see www.lotus.com/lotus/information.nsf/firstpages/copyright and edit the above statements to coincide with your presentation.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks or service marks of others.

Information is provided "AS IS" without warranty of any kind.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information in this presentation concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Contact your local IBM office or IBM authorized reseller for the full text of the specific Statement of Direction.

Some information in this presentation addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Photographs shown are of engineering prototypes. Changes may be incorporated in production models.