Internet Security Principles For ASP's

M. C. (Butch) Maxwell
Andrews Consulting Group
Cheshire, CT USA

With special credit to:
Patrick Botz
IBM Rochester

Asia is Growing

Estimated B2B e-Commerce
Transaction Value by 2005

Source: GS Research, IDC

- Asia's B2B revenues increasing
  - 2000 $8 billion
  - 2001 $50 billion
  - 2005 $350 billion
- Web-based payment system required
  - "Having the ability to close the loop on payments is what's going to distinguish those market places that succeed from those that fall by the wayside"
  - Peter Hohenstein, Bank of America
- The challenge is trust
  - Internet payment infrastructure
  - International certificate standards
  - Legal acceptance of electronic signatures

Internet Security Threat

ANDREWS CONSULTING GROUP

Explosive growth of the Internet

- $1.3T market forecast in 2003
- Estimated $50B in 1998
- Revised from $32B mid-1998 estimate

(IDC - March 99)

Makes the Internet...

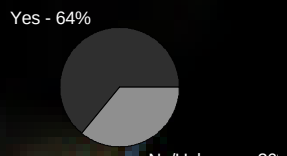
- Desirable place to do business
- Attractive place to steal from business

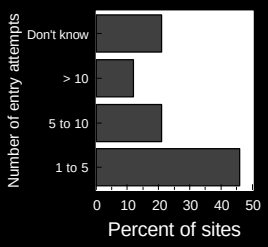
Serious Breaches Occurring

- 500 firms surveyed
- 32% sought help from law enforcement
- Up 17% from last year

(Computer Security Institute - March 99)

Percent whose computer systems had unauthorized use within the year.





... and not just once.

(Computer Security Institute - March 98)

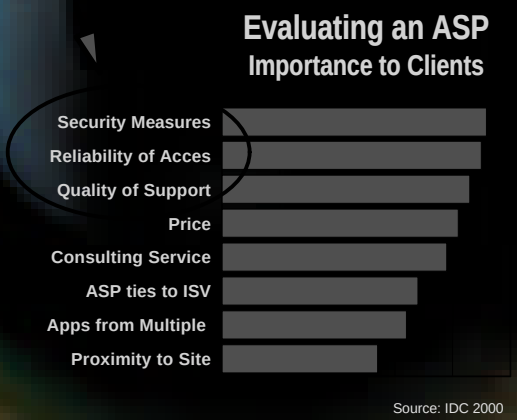
Financial losses

- $124 million from all security breaches
- Down from $137 million in 1997
- Losses from financial fraud and theft of data up sharply
- Estimated real losses in $10s of billions

(Computer Security Institute - March 99)

Agenda

ANDREWS CONSULTING GROUP



Source: IDC 2000

- Reliability
- Application Availability
- Security
  - ISP Security
  - Host Security
  - Network Security
  - Application Security
  - The Role of a Firewall

The "Industrial Strength" ASP

ANDREWS CONSULTING GROUP

- How do we make an ASP a reliable place to do business ?
  - Systems reliability
  - Applications availability
- ... a safe place to do business ?
  - Confidentiality/privacy
  - Authentication
  - Integrity
  - Non-repudiation

- **Authorization**
  - *"Does this person have access to this data or application?"*
- **Privacy**
  - *"Is any personal information I give out being compromised?"*
- **Authenticity**
  - *"Is this person who he says he is?"*
- **Integrity of Information**
  - *"Am I confident that the data I receive and send is not being tampered with?"*
- **Non-repudiation**
  - *"How can I ensure the data was received, signed for, and time stamped? Will it stand up in court?"*

Why is Reliability So Important?

ANDREWS CONSULTING GROUP

Bottom impact of downtime is $'s

	Case A	Case B
HW	$ 1.1M	$ 1.1M
SW	1.0	1.0
Services	2.0	2.0
Availability		
99.98 (105 mins)	1.05	NA
99.999 (5.2 mins)	NA	0.05
Total Cost - Year 1	$5.15M	$ 4.15M

Cost per minute of down time is $13K for ERP and $10K for e-commerce
Source: Standish Group Study

99.98 vs 99.999 yields **$1.0 Million** dollars in annual savings from downtime alone

Ebay 2Q99 To Take Hit From Outage
SAN JOSE, Calif. (Reuters) - Online auction house eBay Inc. said second quarter revenues will be about $3 million to $5 million lower on the fallout from a nearly 22 hour outage on its Internet site Friday... 6/14/99

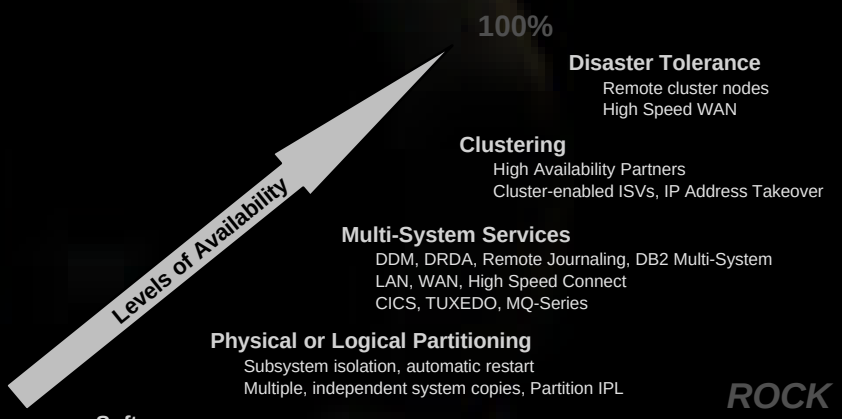
Resources to Protect

ANDREWS CONSULTING GROUP

- There are many things that must be protected
  - Public systems
  - Private systems
  - Network
  - Data
  - Transactions
  - Reputation

Availability Solutions

ANDREWS CONSULTING GROUP



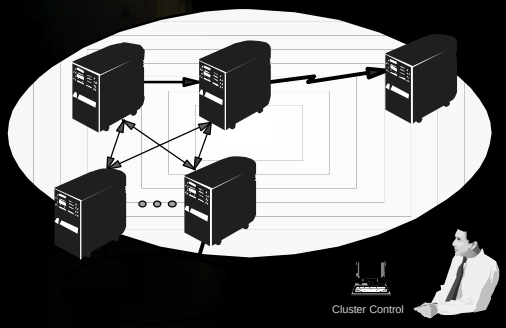
© Andrews Consulting Group, 2000

Clustering

ANDREWS CONSULTING GROUP

Cluster

A group of independent systems working together as a single system.



Cluster Resources

- Single resource view
- Multiple nodes
- Heartbeat services
- Cluster configuration manager
- IP address takeover
- Switchover administration
- Distributed activities

Cluster Management

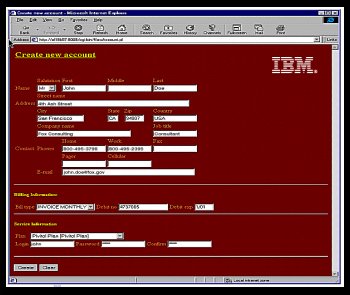
- User Interface
- Data resilience solutions
- **ClusterProven™ Applications**

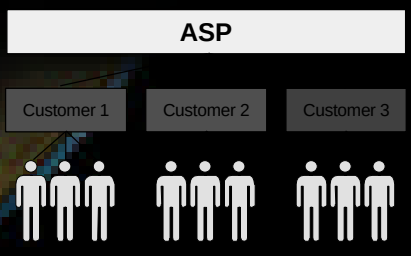
- **Easy to configure**
- **Easy to manage**
- **Planned and unplanned**
- **Disaster Tolerance**

Authorization

ANDREWS CONSULTING GROUP

- **ASP Administration**
- **User Registration**
  - **Client Companies**
  - **Client Administrators**
  - **Users**
- **Billing/Accounting**
- **Auditing**

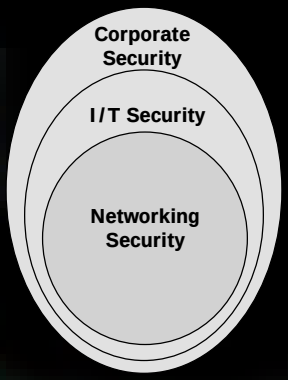




© Andrews Consulting Group, 2000

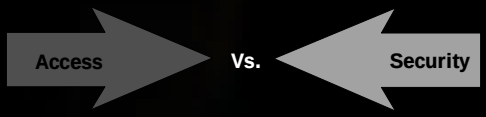
Internet Security Policy

ANDREWS CONSULTING GROUP



What are your security policies?

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

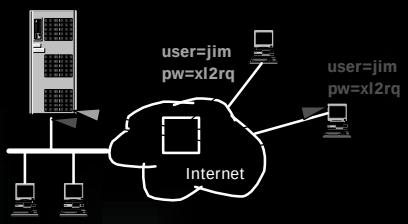


- FTP access<-> PC virus introduction
- Mail exchange<-> mail flooding
- Web server <-> web graffiti

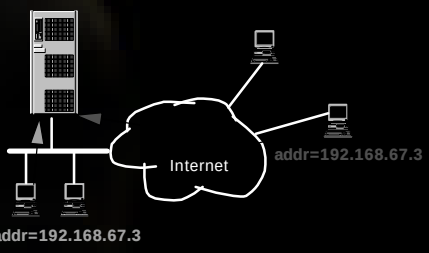
Example Internet Security Exposures

ANDREWS CONSULTING GROUP

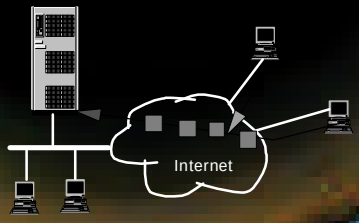
Sniffing



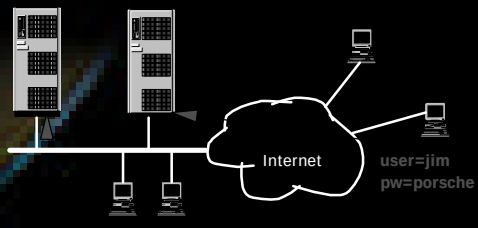
Spoofing



Denial of service



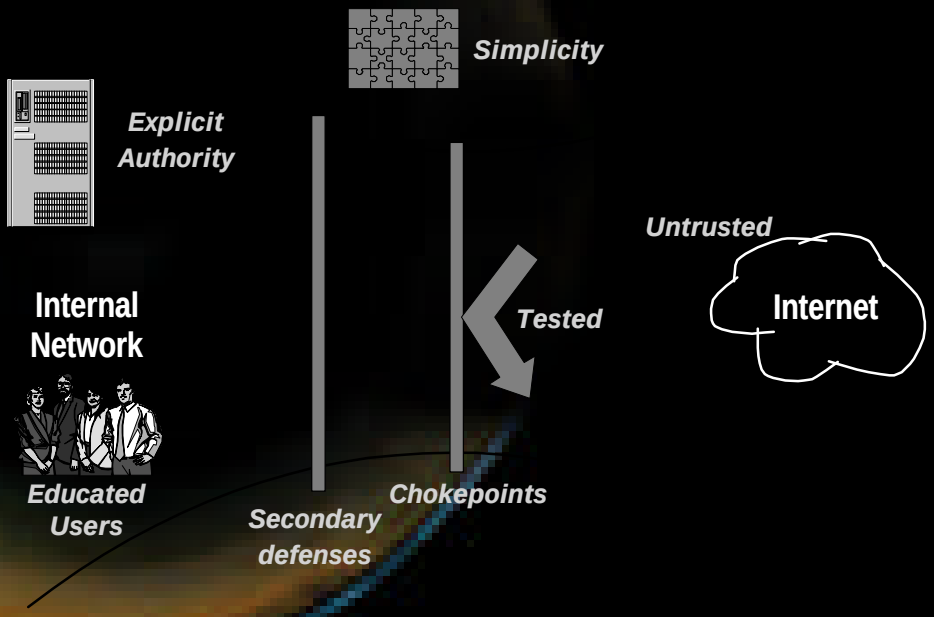
Trusted hosts



© Andrews Consulting Group, 2000

Internet Security Principles

ANDREWS CONSULTING GROUP



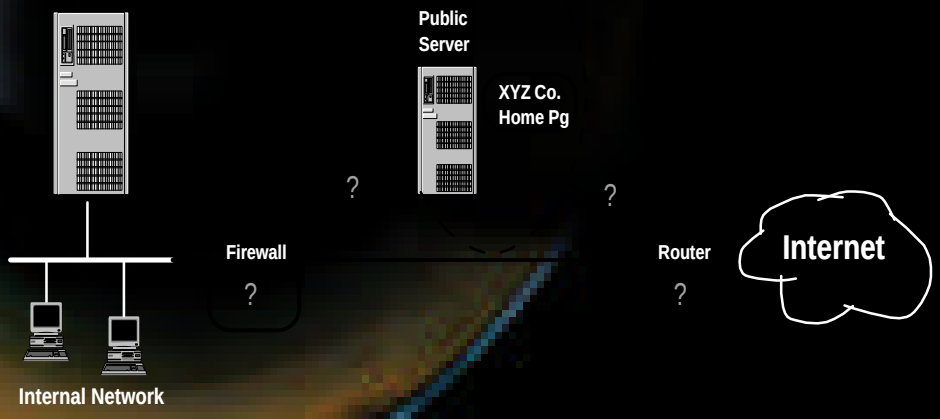
Protecting a Public Server

ANDREWS CONSULTING GROUP

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

Layers of security

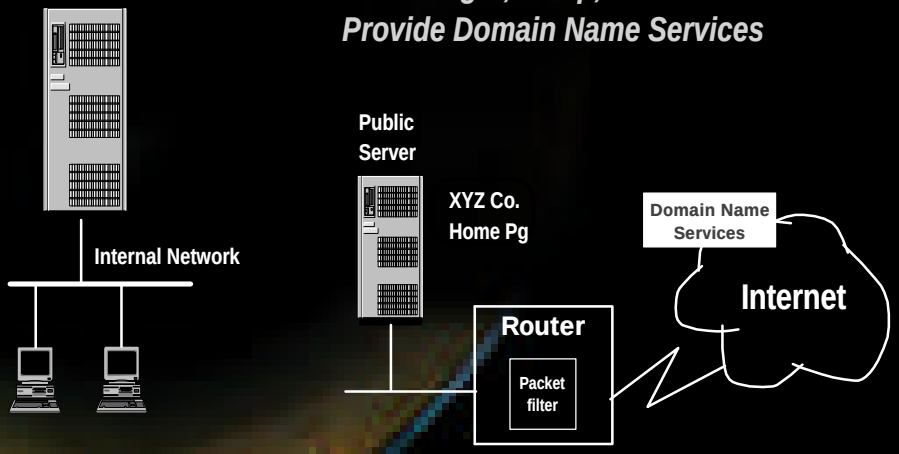
- Internet Service Provider
- Host
- Communications (TCP/IP)
- TCP/IP application



Internet Service Provider Security

ANDREWS CONSULTING GROUP

Block incoming telnet connections
Block finger, snmp, ...
Provide Domain Name Services



Host Security

ANDREWS CONSULTING GROUP

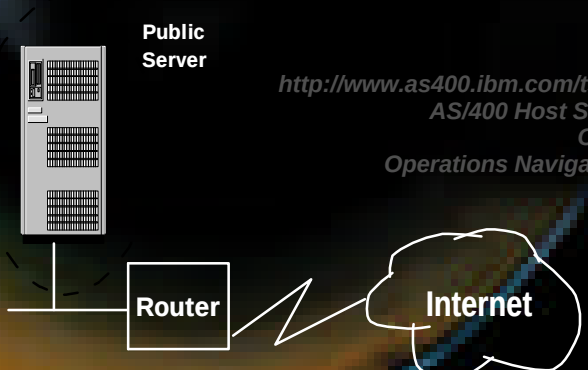
Enable Resource Security

Password attack prevention

Tightly control "high-powered" profiles

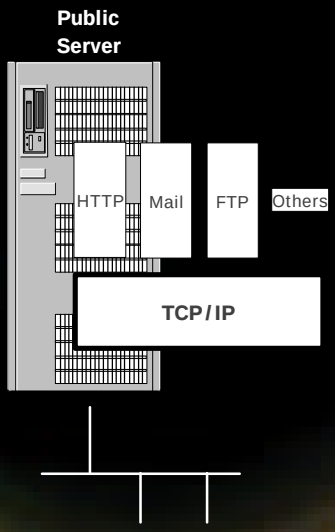
Use Object Security

Verify and Monitor



http://www.as400.ibm.com/tstudio/secure1/index_av.htm
AS/400 Host Security Advisor
OR
Operations Navigator Security Wizard

TCP/IP Security



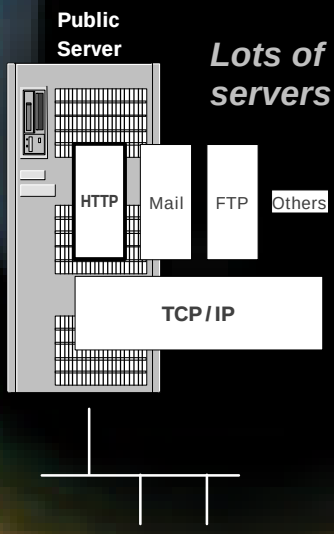
Only start TCP/IP applications you need

No IP forwarding

Don't define host name of internal systems

Define only one route (default)

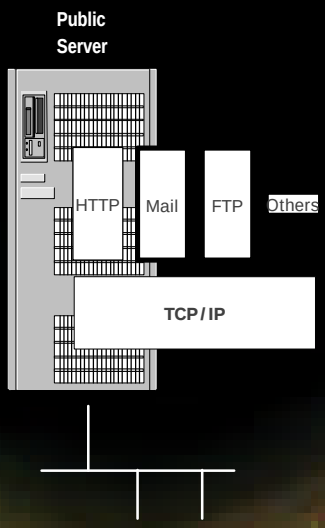
Web Server Security



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

- Server directives
- Protection directives
- Secure data transmission (encryption over the wire)
  - Secure Sockets Layer (SSL)
  - Digital Certificates
  - Managing digital certificates
- CGI-BIN Programs

Securing Other TCP/IP Applications



FTP
Mail
Various other applications

Other TCP/IP Applications

When the system is accessible from the Internet

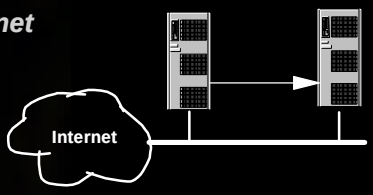
Telnet	Don't start it! But if you must... Set maximum storage per user profile
SNMP	Don't start it! But if you must... Set community name (like a password) Only allow GETs
LPD	Don't start it !

Preventing Hacker Written Applications

ANDREWS CONSULTING GROUP

When the 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

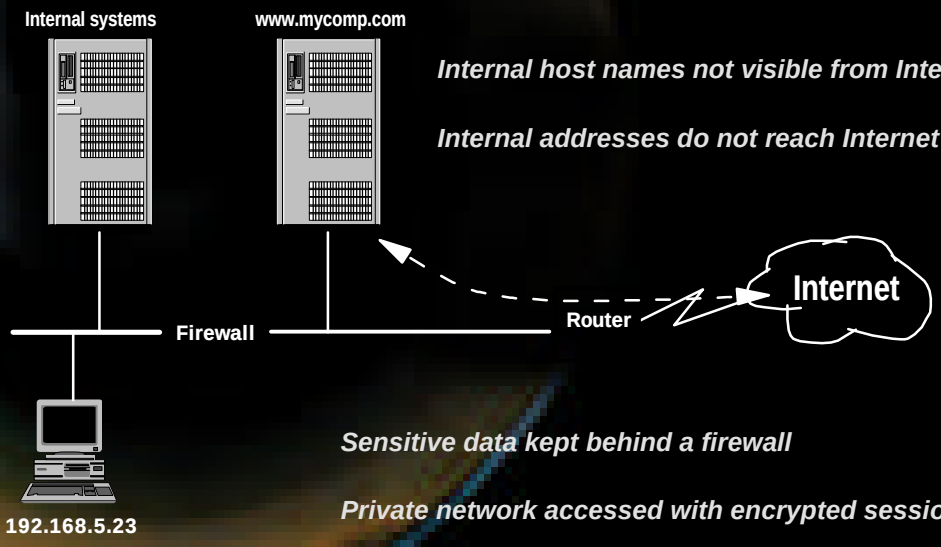


TCP/IP port restrictions can limit usage of well known ports

Protecting Internal Servers

ANDREWS CONSULTING GROUP

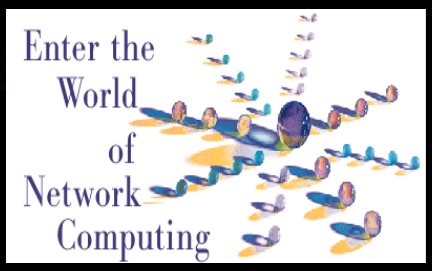
What we haven't talked about



Internet Security Summary

ANDREWS CONSULTING GROUP

- The Internet can be a reasonably safe place to do business
  - Caution is advised, poor planning or mistakes could be disastrous
  - Cryptography plays a major role
  - Internet security is still evolving
- The security features that make a good Internet Server
  - Proven operating system integrity
  - Excellent host level security
  - Integrated communications security
  - Secure HTTP serving



ANDREWS CONSULTING GROUP

© Andrews Consulting Group, 2000