Internet Security

Presented by

Paul Forney

Domain Architect

Invensys Software Systems

Session Outline

- Domain Security Architecture
  - Network Protection
  - Platform Protection
  - Client (Member) Access Control
- Key Points
- SuiteVoyager Security Implementation
- Ten Immutable Laws of Security
- General Security Considerations

Introduction

Security is about managing risks by providing protection for information:

- Confidentiality
- Privacy
- Integrity
- Availabilty

“Prevent, detect, and react"

Key Points

- Security is not an add-on feature
- Protection Mechanisms include:
  - Network security
  - Platform security
  - Application security
- Client authentication and authorization are key
- Policy

Security Domains

- Invaluable for insuring consistent policy and most cost-effective application of security controls
  - Regions of consistent security
  - Prevent unauthorized disclosure
  - Right level of protection at the right place
  - Internet, DMZ, Corp Network

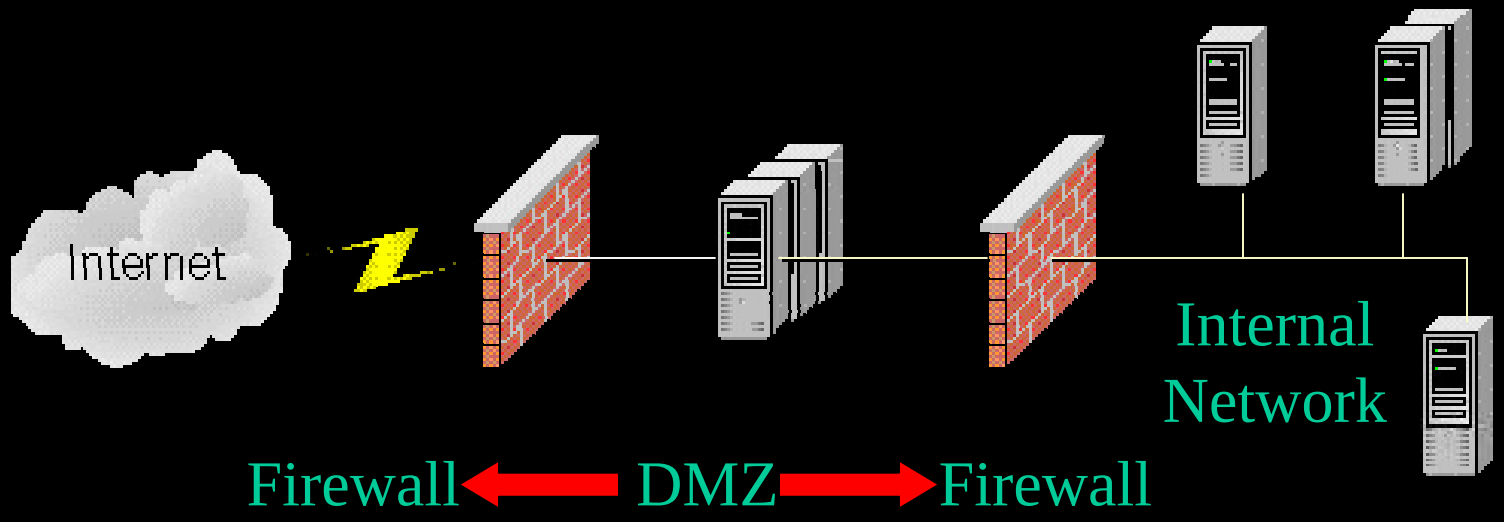
First Step

Analyze:

- **Business risks**
- **Nature of systems and data**
- **Costs**
- **Usability**

Then determine what is optimal!

Network Protection



Firewalls

- Function at the protocol layer
- Mechanism to control the flow of data between two parts of a network
- Three types of firewalls–
  - Network Routers (Stateless)
  - Packet Filters (Stateful)
    - Cisco's PIX
    - Check Point's Firewall-1
  - Application-level
    - MS ISA

Network Segregation

- Segregate different kinds of traffic to different clusters
- Segregate Internet traffic from back end traffic
- Use non-routable network addresses for internal web site networks
- Implement a management network

HTTPS –SSL for Encryption

Provides confidentiality and integrity for transmitted data

- HTTPS Protocol
- SSL – Secure Sockets Layer
- Server Certificates

Problems with SSL

- SSL protects in-flight communications only
- SSL is stateful
- Encryption/decryption is computationally intensive
- Not a substitute for other security measures

Intrusion Detection (IDS)

- Examples: Cisco's NetRanger or ISS's RealSecure
- Provide real-time monitoring of network traffic
- Detect hostile attack signatures and terminate session
- Can generate alarms

Problems with IDS

- Performance
- False Accepts/rejects
- Cost

Platform Protection

Hardening Components

- **Restrict access to all resources using ACL's**
- **Eliminate all non required protocols, services, and utilities**
- **Employ filtering on TCP/IP protocol stacks (IPSec)**

Platform Protection

- Monitoring
- Windows Domain Structure
- Securing Site Data

Client Access Control

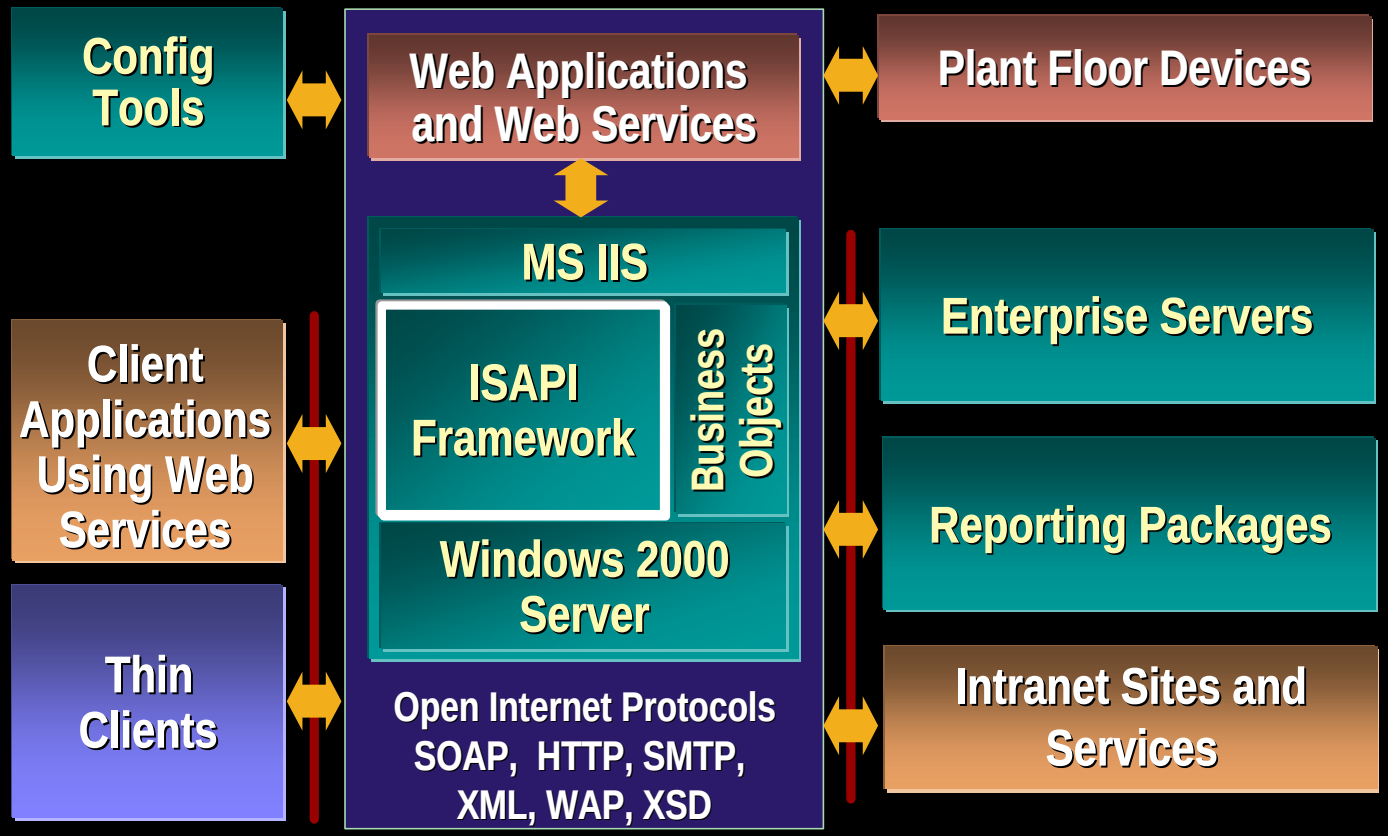
- Authentication mechanisms - verify the client's identity
- Authorization mechanisms - dictate which resources the authenticated client can access

Maintenance

Internet distribution of updates…

- Subscribe for IIS security bulletins and updates
- Always monitor logs
- Keep anti-virus software up to date

Application Security



Ten Immutable Laws of Security

Don't hold your breath waiting for a patch that will protect you from these issues!

Sound Judgment is the key to protecting yourself!

Immutable Law #1

If a bad guy can persuade you to run his program on your computer, it's not your computer anymore!

Immutable Law #2

If a bad guy can alter the operating system on your computer, it's not your computer anymore!

Immutable Law #3

If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

Immutable Law #4

If you allow a bad guy to upload programs to your web site, it's not your web site anymore!

Immutable Law #5

Weak passwords trump strong security!

Immutable Law #6

Law # 6

A machine is only secure as an administrator is trustworthy.

Immutable Law #7

Encrypted data is only as secure as the decryption key!

Immutable Law #8

An out of date virus scanner is only marginally better than no virus scanner at all.

Immutable Law #9

Absolute anonymity isn’t practical, in real life or on the web.

Immutable Law #10

Technology is not a panacea.

General Security Considerations

- Read your corporate security policy – a good source for policy info = *http://www.sans.org*;
- Subscribe to the Microsoft Security Notification Service - *http://www.microsoft.com/security/services/bulletin.asp*

Windows 2000 Security

- Review, Update, and Deploy a high Security Template
- Configure IPSec policy
- Secure the Telnet Server
  1. Open the Local Users And Groups tool.
  2. Right-click the Group node, and choose New Group from the context menu.
  3. Enter TelnetClients in the Group name box.
  4. Click Add, and add the users who are to have telnet access to the computer.
  5. Click Create and then Close

What's the solution?

- Recognize security consists of both technology and policy
- Not a problem that can be "solved"
- Security is a journey not a destination
- The key to good security is awareness and sound judgment.

Conclusion

Combine great technology with sound judgment and you'll have rock solid security!

Acknowledgements

- Designing Secure Web-based Applications – Howard, Levy and Waymire
- Hacking Exposed – McClure, Scambray, Kurtz
- "A Blueprint for Building Web Sites Using the Microsoft Windows DNA Platform" – Microsoft Corp. White Paper
- "The Ten Immutable Laws of Security" – Scott Culp

Questions?

Paul.Forney@wonderware.com