

Extranet Security

Mark K. Mellis

Consultant

SystemExperts Corporation

What We'll Talk About

- ◆ What's an Extranet?
- ◆ How Are We Using Extranets?
- ◆ Incident Scenarios
 - War Stories
- ◆ What Can We Do?

What's an Extranet?

- ◆ (1) the extension of resources from a corporation to its partners and other third party users - usually using IP networks, often using the public Internet
- ◆ (2) an opportunity to cut costs, increase efficiency, leverage business relationships, and be a hero
- ◆ (3) an information security officer's nightmare

The End of Perimeter Security

- ◆ We are allowing people outside our organization access to proprietary *data* and *applications* - over the *Internet*
- ◆ These are the things we built our firewalls to prevent!

A Two-headed Beast

- ◆ It works both ways
- ◆ We allow our partners access to our network resources
 - Will our extranet technology work with their firewall?
- ◆ Our partners allow us access to their network resources
 - Will their extranet technology work with *our* firewall?

There are lots of extranets

- ◆ **Traditional “partner networks”**
 - Often frame relay or leased line networks
 - Sometimes protected by firewalls
 - Costly to implement and maintain
- ◆ **EDI (Electronic Data Interchange)**
- ◆ **Publishing**
- ◆ **Engineering Data**
- ◆ **Legal and Travel Services**

There aren't many extranets

- ◆ "Extranet" is a buzzword
- ◆ Few standards
- ◆ Few integrated solutions
- ◆ Lots of RISK!

How Are We Using Extranets?

- ◆ Publishing Data
- ◆ Exchanging Data
- ◆ Simple Applications
- ◆ Complex Applications
- ◆ Multimedia

Publishing Data

- ◆ Catalogs and Datasheets
- ◆ Tech Support Information
- ◆ Software Updates
- ◆ News
- ◆ Calendars and Contacts
- ◆ Other Intellectual Property

Exchanging Data

- ◆ Documents
- ◆ Designs
- ◆ Orders and Confirmations
- ◆ Status
- ◆ Engineering Data (CAD, source code)

Simple Applications

- ◆ Web Forms
- ◆ Search Engines
- ◆ Database Queries

Complex Applications

- ◆ **Legacy Applications**
 - mainframe
- ◆ **ERP**
 - Oracle Financials
 - SAP
- ◆ **Human Resources**
 - PeopleSoft

Multimedia

- ◆ “Too Many Magazines” syndrome
- ◆ Internet conferencing

Incident Scenarios

- ◆ Partner attacks your systems
- ◆ Hacker breaks into partner, hacks your systems
- ◆ Hacker breaks into your systems, hacks partner
- ◆ Hacker breaks into one partner, hacks another partner
- ◆ Partner uses your network inappropriately

What Can We Do?

- ◆ Strategy
- ◆ "Solutions"

Strategy

- ◆ Specify
- ◆ Limit
- ◆ Encrypt
- ◆ Authenticate
- ◆ Isolate
- ◆ Monitor

Specify

- ◆ You can't control everything
- ◆ Policy will help to bound the problem - who is responsible for what
- ◆ Policy is the medium by which management expresses its will
- ◆ Keep "data owners" in the loop

Limit

- ◆ **Limit the capabilities of the system**
 - You don't want to deploy an IPsec VPN when all that is needed is a secure web server
- ◆ **Limit the services offered**
 - If the requirement is for file transfer, turn off interactive logins
- ◆ **Limit the data exposed**
 - Don't publish information that isn't required

Encrypt

- ◆ You must encrypt data traversing insecure networks
- ◆ Use the best crypto you can afford
- ◆ Don't forget export issues

Authenticate

- ◆ You must know with whom you are interacting
- ◆ Authentication mechanisms vary with the sensitivity of the data
- ◆ Basic “username/password” authentication
- ◆ Two-factor authentication
 - something you know and something you have
- ◆ Certificates and PKI

Isolate

- ◆ Stand-alone servers
- ◆ Application proxies
- ◆ Static content
- ◆ Data warehouses
- ◆ Batch jobs
- ◆ Partitioned databases

Monitor

- ◆ Intrusion Detection
- ◆ Traffic Patterns
- ◆ Authentication Successes and Failures
- ◆ Application Logs

"Solutions"

- ◆ There are no solutions
- ◆ That said, here are some extranet components
 - Firewalls
 - Secure Web Servers
 - VPNs
 - Outsourcing

Firewalls

- ◆ Basic component for delimiting network zones with differing security stances
- ◆ Must be flexible enough to adapt to needs of various other “solutions” - both your own and those of your partners
- ◆ Still needs to be secure

Secure Web Servers

- ◆ Most basic building blocks of today's extranet
- ◆ https
- ◆ authentication
- ◆ CGI's
- ◆ Database back ends

VPNs

- ◆ Powerful - too powerful
- ◆ hard to get through most firewalls
- ◆ still a single-vendor solution
- ◆ beware of end points
 - client end acts as router
 - server end terminates on firewall, not at application server
- ◆ implications for other infrastructure
- ◆ performance and scalability issues

More VPNs - specifics

◆ SSH

- TCP tunnels only, but...
- port forwarding
- X forwarding

◆ Aventail

- Hybrid of SOCKS and SSL
- lots of system integration “glue”
- targeting extranets
- easy to get thru firewalls

Outsourcing - general

- ◆ **Generic VPNs**
 - AT&T, MCI, Concentric Networks, others
 - Provide secure IP but little else
 - terminate on firewalls

Outsourcing - targetted

- ◆ **WAM!NET - vertical markets**

- Graphic Arts
- Medical
- Entertainment

- ◆ **Pilot Network Services**

- “Escrowed” partner connections

What We Talked About

- ◆ What's an Extranet?
- ◆ How Are We Using Extranets?
- ◆ Incident Scenarios
- ◆ What Can We Do?

It's the same old stuff

- ◆ Extranets are the same old same old - an opportunity to use networks to help business.
- ◆ They're just IP, firewalls, intrusion detection, policies, authentication, cryptography, best practices, and the web - assembled in a new, improved package.
- ◆ Your business units will be asking for them when you get back to the office. Be ready!

How to reach us

◆ Corporate Headquarters

- Toll Free +1 888 749 9800
- Phone +1 978 440 9388
- Fax +1 978 440 9636

Mark K. Mellis
Consultant

Mark.Mellis@SystemExperts.com
<http://www.SystemExperts.com>

757 Londonderry Drive
Sunnyvale, California 94087
+1 408 733 6054 (direct)

Please remember to fill out the evaluation form.