SystemEXPERTS

Security in an E-Business World

Philip Cox

Consultant

Monday September 10, 2001

What the course is...

- A discussion of the most common operational security problems organizations face
- The characteristics of a securable architecture
- A Hacker Primer

What the course isn’t...

- A course to secure your enterprise
- A detailed treatment of systems, firewalls, or product configurations
- A survey of security products

Where are we?

- **Common Operational Security Problems**
- Architecture Characteristics
- Hacking Primer

General Thoughts

- The most common problems…
  - Are not new
  - They are not “sexy”
  - Are just derivation of old problems
    - …there is nothing new under the sun. Ecclesiastes 1:9
- A large part of security is due diligence
- Security is still mostly a reactionary model in most organizations
- Now, on with the show …

Top 10 Most Common Operational Security Problems

10. User passwords and data sent in the clear

9. A single reusable username and password for internal and external access

8. Relying on switches to prevent network sniffing

7. Thinking that the Firewall is the only point of entry

6. Allowing too many services on individual systems or non-business critical services

Top 10 Most Common Operational Security Problems

5. No User education

4. Block incoming traffic, but allow all outgoing traffic

3. No Intrusion detection

2. No configuration management

1. No time to do it right

What’s the problem?

- User passwords sent in the clear
  - Telnet, FTP, HTTP BASIC Auth, POP, IMAP, NTLM
  - *CM: Encryption {SSL, SSH, Application}*
- A single username and password for internal and external access
  - Get a POP password
  - Then use a VPN to get in
  - Then access internal systems
  - *CM: Strong Authentication, separate credentials for internal and external access*

What’s the problem?

- Relying on switches to prevent network sniffing
  - Switches are designed for performance not security
  - Many programs to “corrupt” ARP tables
  - *CM: Hardcode MAC addresses in switch, encrypt sensitive traffic*
- Thinking that the Firewall is the only point of entry
  - Partners, Modems, VPN’s, Wireless, ASP’s
  - *CM: Routinely perform external testing for connectivity*

What’s the problem?

- Allowing too many services on individual systems or non-business critical services
  - More targets likely to be exploited
  - More services to keep secure
  - *CM: Only implement services that are required for the business to succeed. Use the one-server/one-service rule*
- No User education
  - They need to know how to defend themselves
  - They are a major focal point of new attacks
  - *CM: Regular user training on current attacks and countermeasures*

What’s the problem?

- Block incoming traffic, but allow all outgoing traffic
  - The hacker may be one of your employees
  - Many new attacks use this “feature” to download files
  - *CM: Configure perimeter controls to only pass “allowed” traffic regardless of direction*
- No Intrusion detection
  - How do you know if you have been hacked?
  - Liability issues, Insurance companies will require it
  - *Implement an enterprise-wide Intrusion Detection System (IDS) {more later}*

What’s the problem?

- No configuration management
  - You just can’t do multi-system secure deployments without it
  - *CM: Implement a comprehensive Configuration Management process {more later}}*

- No time to do it right
  - It is just an excuse, time is coming where this will be a liability
  - *CM: Bite the bullet, and do the right thing!*

More on Intrusion Detection: Recommendations

- How do you eat an Elephant? One bite at a time
- Start with the following, in order of preference
  - Network ID at the firewall/perimeter networks
  - Host and Application ID on most critical externally accessible systems
  - Host and Application on critical internal servers
  - Network ID on critical internal networks
  - Host and Application on secondary internal servers
  - Network ID on internal networks
  - Host ID on desktop/user systems
- Have a plan on how to respond to a security event

Configuration Management

- Having a process and procedure to…
  - Perform testing before rolling out updates
  - Apply critical security patches in a timely manner
  - Schedule upgrades and configuration validations
  - Backup and restore systems
  - Track and control software versions
  - Rollback if problems occur

Where are we?

- Common Operational Security Problems
- **Architecture Characteristics**
- Hacking Primer

Top 5 Most Common Architectural Security Problems

5. Confusing DMZ/Firewalls as a security architecture

- outside & inside vs. appropriate access

4. Overlooking one of the 3 A's: Authentication, Authorization, and Auditing

3. Using product definitions to define the architecture instead of vice-versa

2. Adding security after the fact

1. Not understanding business requirements

What We’ve Seen

- Lopsided focus on firewalls
- Growing interest in consistent authentication
- Growing interest in logging and intrusion detection
- Authorization is almost always left out
- Slow development of integrated security across applications and infrastructure Homespun systems tend to tie it all together (at a high long-term cost)

Architecture: What to do?

- Determine what you want to do from a business standpoint
  - Business requirements drive security needs, not vice versa!
- Design an architecture that can meet those needs
  - You may have to develop a migration plan if you are too far off the mark

Securable Architecture’s …

- Have well articulated key risks (3-7 of them) to defend against
- Have well defined and documented key organizational policies (a manageable number)
- Have well articulated, concise, and documented requirements to support key business goals (5-10 of them)
- Define a model of what is to be secured, not a product list of how to secure things
- Are understandable

Authorization Requirements: An Example

- What needs to be protected?
- Are there multiple levels of service?
  - Distinction between groups
    - Employees
    - Customers
    - Partners
  - Distinction among value of service
    - Membership
    - Group accounts
    - Individual accounts

Where are we?

- Common Operational Security Problems
- Architecture Characteristics
- **Hacking Primer**

It’s easy and it’s fun!

- Intrusions are easier than we would like…*why*?
  - poor detection and escalation
  - limited use of real authentication and authorization
  - Internet readiness degrades over time
  - many organizations think in terms of inside and outside
  - OS/application upgrades are a pain
  - there are no business risk/cost analysis tools
    - hard to quantify demands
  - integrating disparate layered technologies on multiple OS environments is time consuming

Hacker Methodology

- Reconnaissance
- Identification of opportunities
- Research
- Exploitation
- Eliminate tracks

Profiling

- Rudimentary data
  - InterNIC data
  - all IP addresses
  - SNMP agents
- Expanded data gathering
  - TCP/IP, UDP services
  - SNMP MIBs
  - DNS names and conventions
  - ISP routes
  - OS types
  - External : mail, DNS
  - Web server exploits

- Research data
  - known service exposure opportunities
  - OS vendors
  - related hacker successes
  - related hacker tools
  - recent exploits
  - detection and prevention tools and techniques

Intrusion Example

- NO detection!
  - main Web server fine…let’s look around
  - staging server not so fine
  - exploit well known Web server bug to initiate interactive login session
  - exploit trust relationship between staging server and main Web server
  - change main Web pages!
- Typical big exploit is a combination of lower level problems

Intrusion Example, cont.

- Vulnerabilities to achieve critical access
  - ICMP echo allowed in (low)
  - Non default but easily guessed SNMP community string (low/medium)
  - Non production quality HTTP server configuration on non production system (low)
  - trust relationship between 2 systems within a close IP address space (low/medium)
  - xterm from DMZ address allowed out through firewall (medium)

What Did We Just Learn?

- Many intrusions and tools require little actual networking knowledge
- There are a lot of tools, techniques, sites, and initiatives that you can use and should be aware of

Wrapping it Up!

- New Network Paradigms to be aware of
- What you need to do
- Security Rules of Thumb
- Contact Information

New Network Paradigms to be aware of

- Increased use of VPN technology
- Use of XML is on the Rise
  - Simple Object Access Protocol (SOAP)
  - Microsoft's .NET
- Use of switched media
- Voice and Data on the same network
- Wireless Networks

What You Need To Do

- Analyze your own requirements
- Analyze your own architecture
  - Too complex?
  - Too many connections?
  - Too many mechanisms?
- Look for consistency from the outside and the inside

What You Need To Do

- Test your configuration
  - Internet exposure tests
  - Content review - application walkthrough
  - Use the same methodology hackers do!
  - Profiling yourself is a big part of being prepared for an intrusion

Security Rules of Thumb

- 90% of all vulnerabilities have fixes
- If it is architected right, it **CAN** be secured technically
  - If not, you may get lucky ☺

SystemEXPERTS
LEADERSHIP IN SECURITY

Philip Cox
Consultant

Phil.Cox@SystemExperts.com
530-887-9251 direct
530-887-9253 fax
978-440-9388 main
http://www.SystemExperts.com/