

IT Security Conference

20 May 2004

Part II is Hard to Do

Peter Coffee, Technology Editor

***e*WEEK**

Security: Selling the Sequel

- Thanks for asking me to come back
- I hope you didn't expect a happy ending
- If security were a movie series:
 - Rocky VI: Concussion
 - Die Hard 4: Yes, Bruce Dies
 - Lord of the Rings: Gollum Gets the Gold
- The only good news: everyone now *realizes* things are bad

Fed up in the heartland

- Business Roundtable, yesterday (5/19/04)

“Up until now, the IT suppliers have deflected criticism and redirected criticism to end users. It's time that IT suppliers and manufacturers stepped up to the plate.”

- Marian Hopkins, BR Security Task Force

- In Reply:

“Cybersecurity is everyone's responsibility, including the vendors, the users, enterprises and government agencies...We all have responsibilities to lock our doors in our homes and to buckle up when we get in our cars.”

- Greg Garcia, IT Association of America

The tempo is accelerating

- Slammer exploited a vulnerability discovered six months earlier
- Blaster exploited loophole 26 days old
- The new security posture must be built for “Day Zero” readiness
 - “Warhol” threats: 15 minutes to spread
 - “Flash” threats: 30 seconds to spread
- Symantec monitors 20,000 sensors
- Terabytes of cross-reference required

So many ways to lose

- Sasser sweep found 7 of 9 sites pre-infected
- Source code theft: Microsoft, Cisco
 - Many researchers shunning access
 - Most attackers target sites, not whole network
- Actual methods used by attackers
 - password cracking (brute-force) 13.9%
 - IP spoofing 12.4%
 - DoS 16.3%
 - traffic analysis 11.2%
 - scanning 15.9%
 - data substitution 15.6% (Computer Security Institute, 5/18/04)

So many sorry losers

- 68% of UK companies attacked in '03
 - Up from 44% in '02, 24% in '00
 - 50% of companies (70% of incidents) had virus infections
 - 12% of companies >1000 had DoS attacks
 - Direct attacks also on the rise
 - 17% of all companies
 - 39% of large companies
 - *Detected* attacks (PWC, 101 IT mgrs.)
- U.S. has 65 million handguns; 128 million cars; 199 million Internet users

All those unlicensed drivers

- Practices aren't followed:
 - Yes, 90 percent of organizations update virus signatures at least daily...
 - ...but only 63 percent of enterprises usually or always require the use of difficult passwords;
 - Only 35 percent usually or always require different passwords on all accounts;
 - Only 69% of enterprises verify the integrity of back up data at least monthly (111 IT mgrs as of 2/04)
 - www.securecomputing.com/pdf/BasicInsecurity.pdf
- Spam overload still grows
 - 350,000 to 400,000 unique spam attacks per day
 - 30 to 40% spam increase since 1/1/04
 - 71% of spam URLs are Chinese (CommTouch Software)

It must be assumed...

- Attackers know the technology
- Attackers have access to bug lists and source code
- Attackers understand the IT environment
- Attackers have time



Adopting a Black-Hat Perspective

- Controlling the perimeter doesn't work
 - Applications themselves harbor defects
 - Client applications assume non-hostile users
 - Naïve trust relationships give excessive privileges
 - Too many applications are written to require systemwide access
- IPv6 closes many loopholes
 - Integrates IPSec, source authentication
 - DoD mandating compatibility now, pushing toward use by 2008
- Block *behaviors*, not signatures

The Need for Many Layers

- The valuable stuff is in the safe
- The safe is behind a locked door
- The door is connected to an alarm
- The hallway is watched by a camera
- The camera is connected to a monitor
- Someone is paid to listen for the alarm and watch the monitor screen
- Someone is paid to respond if something unusual is heard or seen

Product→Process→Platform

- It's tempting to buy security tools as “set and forget”
- It's essential to support those products
 - update schedules
 - log review responsibilities
 - role management that tracks organization change
 - response drills that detect and correct procedure gaps
- It's desirable to integrate security into platforms
 - Solaris 10 incorporates “trusted” elements
 - Sun Java Studio Enterprise includes identity server
 - Platform enables process that exploits product...
...but it all depends on people

Guidelines and Resources

- *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST)
 - Assessing effectiveness of controls
 - Determining business and mission risk
 - csrc.nist.gov/publications/nistpubs
- *Security Assessment: Case Studies for Implementing the NSA Information Assurance Methodology* (Syngress Publishing)
 - Information types
 - Impacts of insecure practice
 - Availability and practicality of measures

Reducing Reaction Time

- Once: “I don’t have to outrun the bear...
...I just need to run faster than you.”
- No longer an acceptable doctrine
- Attacks spread more quickly
 - Witty worm began spread < 48 hours after disclosure
 - Penetrated 12,000 systems in < 1 hour
- Attacks do more damage
 - No longer mere “ego announcements”
 - Witty dropped random “byte bombs” on file systems

The simple nouns and verbs

Preserve accuracy, availability, & access

Permit authentication and authorization

Create awareness and accountability

Perform inspection; maintain protection
detection; assure reaction; build
on reflection

The simple nouns and verbs

- Preserve accuracy, availability, & access
- Permit authentication and authorization
- Create awareness and accountability
- Perform inspection; maintain protection; enable detection; assure reaction; build on reflection



***e*WEEK**