

Risk, Complexity, and Network Security Bruce Schneier

CTO, Counterpane Internet Security, Inc. schneier@counterpane.com

BlackHat Asia Hong Kong and Singapore 23 and 26 April 2001





It's a Dangerous World

- Every week we see new break-ins, new attack tools, new vulnerabilities
- 2001 CSI/FBI Computer Crime and Security Survey (538 responses):
 - 64% of respondents detected "unauthorized use of computer systems" in the last 12 months
 - 40% detected "system penetration," even though 95% had a firewall and 61% had an IDS
 - 26% detected "theft of proprietary info," and 18% detected "sabotage"
 - The combined losses from just 196 respondents totaled \$378 million
 - \$151 million from "theft of proprietary info" and \$19 million from "system penetration"

3



Random Stories from January 2001

- Cybervandals hacked and stole player accounts on Battle.Net; the virtual items in the game have real monetary value to other players
- Hacker who was angry at the outside activities of an ISP sent customer information to Computerworld
- Egghead.com announced that an intruder into its system more than two weeks ago did not grab any numbers from its database of 3.7 million credit cards; but the investigation cost millions of dollars
- Group of hackers attacked government sites in the United States, United Kingdom, and Australia
- Ramen, the Red Hat Linux-based Internet worm, spread into the wild and defaced the Web sites of several different organizations, including a NASA lab
- Microsoft's Web sites experienced several days' worth of outages, first reportedly from a technician's error, then from a malicious denial-of-service attack

.



These are only a small percentage of the stories that made the news

And most stories never become public



Security: Why Should We Care?

- Computer security is a fundamental enabling technology of the Internet
 - Privacy, authentication, integrity, fairness
 - Security turns the Internet into a serious tool for both business and personal uses
 - The limits of security are the limits of the Internet
- Attacks make it harder to do business on the Internet
 - Attacks cost money
 - Attacks result in bad publicity
 - Attacks have the potential to cause unbounded losses
 - Attacks INCREASE THE RISK of being on the Internet



There Are Many Risks

Direct Losses

• Theft

- Money
- Trade secrets and company information
- Digital assets
- Consumer information
- Computer resources
- Productivity Loss
 - Corruption of data
 - Diversion of funds
 - Recovery and continuity expenses

Indirect Losses

- Secondary Loss
 - Loss of potential sales
 - Loss of competitive advantage
 - Negative brand impact
 - Loss of goodwill
- · Legal Exposure
 - Failure to meet contracts
 - Failure to meet privacy regulations
 - Illegal user activity
 - Officer liability

7



The Biggest Risk?

- The opportunity cost of not participating:
 - Competitive advantages
 - Revenue and cost improvements
 - Expansion of business
 - Customer loyalty
 - New business models
- The benefits of being online more than make up for the risks



The Traditional Approach to Computer Security

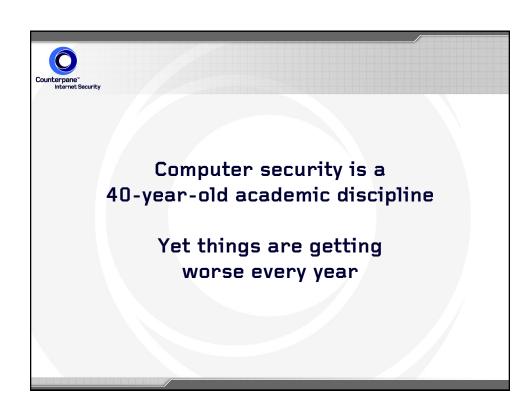
- Techies to the rescue!
- Technology can "solve" the computer-security problem
 - Encryption, firewalls, IDSs, vulnerability scanners, VPNs, PKI, biometrics, etc.
- Technology can counter the threats
- Technology can make us secure

9



The Traditional Approach Is Not Working

- Computer and network security is getting worse
 - Defensive technologies are getting better, but so are attack technologies
- The future of digital security doesn't look good
 - Migration to digital media means that we are depending more on technology
 - More people using products means fewer intelligent users
 - More applications on the Internet means more potential targets







Complexity and the Failure of Security



Why are Complex Products Insecure?

Seven Reasons:

- 1. More security bugs
- 2. Modularity
- 3. Interconnectedness
- 4. Difficulty of understanding
- 5. Difficulty of analysis
- 6. Difficulty of testing
- 7. Unfeasibility of patching



1. Software Security Bugs

- Faulty code is as old as code
- Faulty code has resulted in some spectacular disasters:
 - Ariane 5 rocket
 - NASA Mars missions
- Errors are commonly used to attack systems:
 - Buffer overflows
 - CGI scripting errors, cross-site scripting, etc.
 - Cryptographic implementation errors
 - Flaws in Java, JavaScript, ActiveX, etc.

1



Programming Errors and Security

- Increased complexity means increased errors
 - More complexity → more code → more errors
 - More errors \rightarrow more security vulnerabilities
- Buffer overflows (they just won't go away)
 - Buffer overflows were first identified in the 1960s
 - They were first used to attack networked computers in the 1970s
 - The Morris Worm used buffer overflows: 1989
 - Today, buffer overflows are the most common way to attack systems (two-thirds of all CERT advisories)

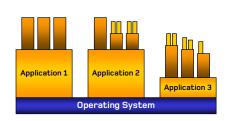


2. Modularity of Modern Software

- Old paradigm:
 - Large applications on top of small operating system



- New paradigm:
 - Applications with components, plug-ins, dynamic linked libraries
 - Operating systems with components, plug-ins, libraries, modules



17



Security Problems with Modularity

- You can't assume all the modules are trustworthy
- You can't assume the modules will work securely in your configuration
- You can't assume the modules will interact in a secure manner
- You can't rely on the operating system to mediate security between modules.
- Both the Java sandbox and ActiveX security paradigms have holes



3. Interconnectedness of Modern Systems

- As systems get connected, a security flaw in one can affect the others
 - MS Word is now a networked program
 - Java applets
 - PostScript files can have viruses
 - Maintenance ports on routers, printers, etc.
 - Home computers as Internet servers
 - Small devices connected to the Internet
 - Reusing protocols for new services
- Windows NT had a C2 security rating, but only if it is not connected to a network

19



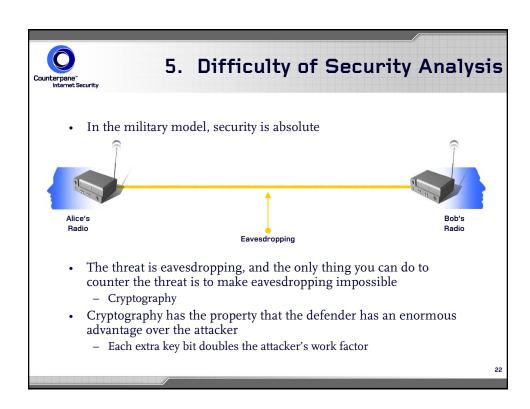
Security Implications of Interconnectedness

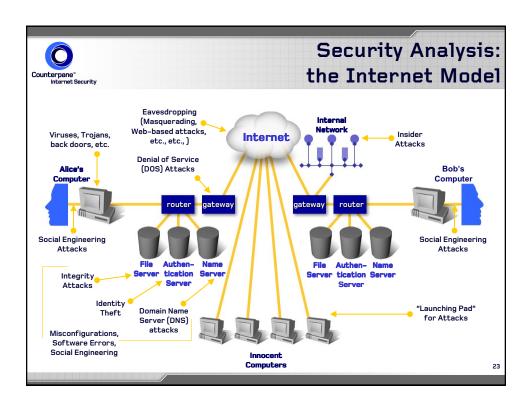
- Modern systems are non-linear
- Modern systems are tightly coupled
- We don't fully understand the interconnectedness of most corporate networks, let alone the Internet
- Reference: *Normal Accidents,* by Charles Perrow



4. User Understanding of Complex Software

- Complex systems are harder to understand:
 - PKI attacks based on people not verifying certificates
 - Viruses and Trojans rely on people not understanding security ramifications of their actions
- · Complex systems are harder to install
- Lack of understanding makes social engineering attacks more dangerous







Internet Security Is Complex (and Relative)

- There are many threats, and they come from all directions
- Your security is often dependent on the security of others
 - And you can't control their security
- There is a balance between attack tools and defensive tools
 - Attack tools might even have a slight advantage
- New developments are happening all the time
 - New network products and services, new vulnerabilities, new hacking tools, new patches, new defensive technologies



6. Impracticability of Security Testing

- Security is orthogonal to functionality
 - Just because a security product functions properly does not mean that it's secure
- No amount of beta testing can ever uncover a security flaw
- Experienced security testing is required to discover security flaws

25



Programming Satan's Computer

- Security engineering assumes a malicious and intelligent adversary that forces particular bugs
- Security engineering is different from any other type of engineering
 - Most products are useful for what they do
 - Security products are useful for what they do not allow to be done
 - Most engineering involves making things work
 - Security engineering involves figuring out how to make things not work...and then preventing those failures



The Failure of Testing Security

- Imagine a vendor shipping a product without any functional testing
 - No in-house testing
 - No beta testing
 - Just make sure it compiles and then ship it
- A product like this will have hundreds of bugs; the odds of it working properly are negligible
- Now imagine a vendor shipping a security product without any security testing
- The odds of it being secure are negligible

27



Complexity Makes Security Testing Harder

- Imagine a system with ten different settings, each with two possible choices:
 - 45 different pairs of choices
 - 1024 different combinations altogether
- Imagine a system with 20 different settings, each with two possible choices:
 - 190 different pairs of choices
 - One million different combinations
- 30 different settings = 190 different pairs and a billion different combinations



7. The Patch Treadmill

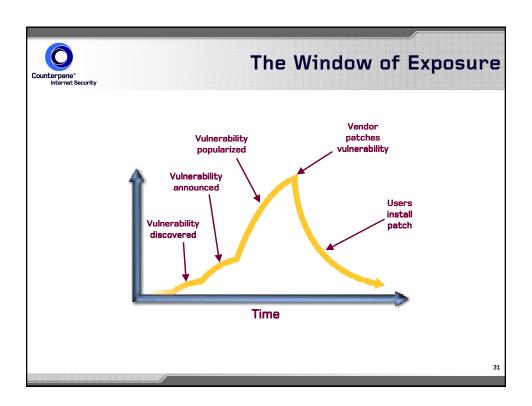
- Because pre-release testing is impossible, security is based on finding bugs after the fact and patching them
- Sysadmins can no longer keep up with the flood of patches
 - Dozens per week that could be relevant
- Patches sometimes break other things
- It is unrealistic to expect companies to keep their patches up to date
 - Blaming the victim

29



Not Installing Patches: Examples

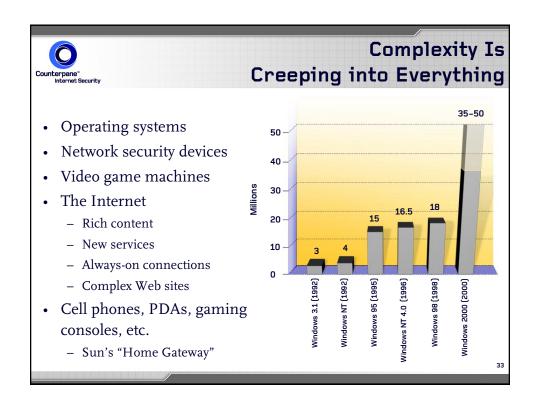
- Credit card number thefts in January 2000
 - IIS bug was fixed eighteen months ago
- Ramen worm
 - Targeted Red Hat Linux bugs that were patched
- Microsoft hack (October 2000)
 - QAZ Trojan was identified months ago
- FBI announcement of March 2001
 - Eastern European hackers using well-known vulnerabilities to steal credit card numbers and extort businesses





The Window of Exposure Has Five Phases

- Phase 1: Before the vulnerability is discovered
- Phase 2: After it is discovered, but before it is announced
- Phase 3: After it is announced
- Phase 4: After an automatic attack tool is written
 - "Script kiddies," with no skill, can use vulnerability
 - Exposure goes up considerably
- Phase 5: After a vendor patch has been issued
 - Exposure still exists, because patches are not installed







Try to Go Back

- Slow down, simplify, add security
- FDA-type approval for Internet devices and services
- Reverse trend toward convergence
- Limit usefulness of Internet
- Even if we wanted to, this would be very difficult

35



We Need to Go Forward

- Embrace the insecurity of products
- Accept that security vulnerabilities are inevitable
- Put processes in place to deal with those vulnerabilities
- Narrow the window of exposure
- Think "risk management," not "threat avoidance"



Risk Management vs. Threat Avoidance

(Look to the Real World for Guidance)



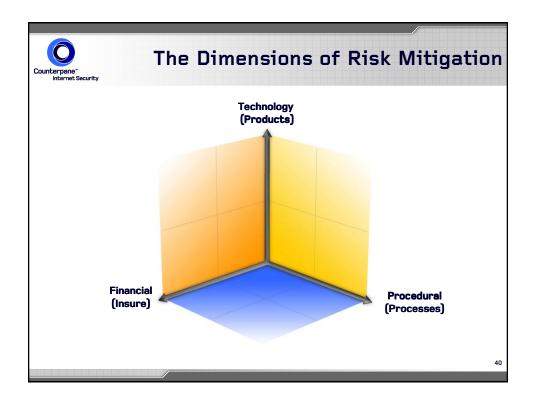
Threat Avoidance (The Military Model)

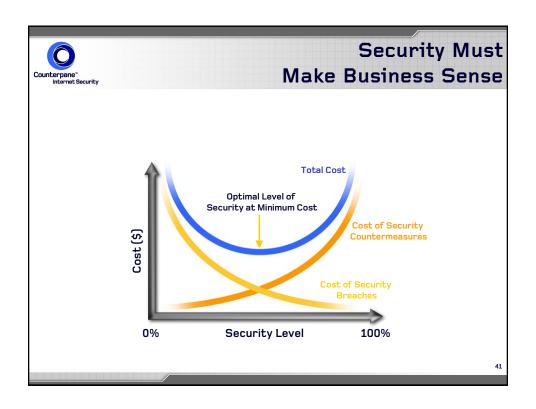
- Security is absolute
 - Either you avoid the threat, or people die
 - Failure is not an option
- Computer engineering mentality
 - Figure out what the threats are, and avoid them
 - Technology can solve computer security
 - New and better products
- Security becomes a barrier to business
 - Security office is the person who says "no" a lot
 - Security becomes an enormous expense



Risk Management (The Business Model)

- Security is relative
 - The risks have to be managed
 - There are lots of different solutions, depending on who you are
 - Things fail all the time; smart companies recover and move on
- You have a variety of options:
 - Accept ("a cost of doing business")
 - Mitigate
 - Reduce technologically
 - Reduce procedurally
 - Transfer (through contracts or insurance)







The Business Case for Security

- Perfect security is too expensive, and not worth it
- No security is too expensive, and not worth it
- Adequate security, at a reasonable cost, is worth it
 - Ability to offer new services
 - Ability to expand into new markets
 - Ability to attract, and retain, customers



The majority of the work to date has centered around threat-avoidance technologies

It's time to think about the dimensions of risk mitigation





Preventive Countermeasures

- Computer security is sold as preventive technology:
 - Firewalls prevent unauthorized network access
 - Encryption prevents eavesdropping
 - PKI prevents impersonation
- This model doesn't work in the real world:
 - No one ever sells a door lock with the slogan "This lock prevents burglaries"
 - Safes are rated by time and materials

45



Prevention, Detection, and Response

- Most of the time, prevention is not perfect
- When you install a preventive countermeasure, you are buying two things:
 - A barrier to overcome
 - The time it takes to overcome that barrier
- Without detection and response, the preventive countermeasure is only of limited value
- Most of the time, detection and response is more effective, and more cost-effective
 - Real-time detection acts as a preventive



Monitoring Provides Robust Security

- Real-time detection can catch attackers, regardless of the vulnerability they exploit
 - If there are enough sensors in a house, you're going to catch the burglar
- Rapid response can repel attackers, regardless of their tools
 - Smart defense beats automatic defense
- Security vigilance helps make individual vulnerabilities irrelevant

47



Effective Monitoring Demands Vigilance

- Detection/response only works 24x7
 - Notice you never see: "Please restrict all hacking attempts to between the hours of 9:00 AM and 5:00 PM, Pacific Time, Monday through Friday"
- Detection/response should be administered in layers
 - Security personnel are in an ideal position to commit crimes
 - Internal audit watches the processes; external audit watches the internal audit







Monitoring is the Feedback Loop for Security

- Monitor first
 - If you don't monitor security, how do you know what kind of security you have?
- Monitoring is how you determine if a security countermeasure is effective
- Monitoring is how you measure the success of your security
- Without monitoring, you're just guessing

49



Monitoring Will Be Outsourced

- Aggregation of expertise
 - Security experts are difficult to hire, train, retain
- Economies of scale
 - It is inefficient to staff 24x7 for rare events
 - One organization can keep abreast of intelligence: new attacks, new vulnerabilities, new capabilities
- Large network visibility
 - An outsourced organization sees many different customer networks



Managed Security Monitoring: The ADT of the Internet

- A new category of security service
- Vigilant security analysts watching customer networks in real time
- Intelligent alert
 - Automated detection and filtering combined with experience and judgment
- Expert response
 - Immediate human intervention combined with an adaptive knowledge base
- Outsourced monitoring supplements existing security measures
 - Detection and response makes for effective security

51



Security is complex, important, and distasteful

Outsourcing is the only way to scale what processes work





The Risks Will Always Be With Us

- The downside of being in a global, highly connected society—you are attached to the best and worst of society
- Security products will not "solve" the problems of Internet security, any more than they "solve" the security problems in the real world
- The best we can do is manage the risk
 - Close the window of exposure
 - Enable e-business
 - Thrive on the Internet



Enhanced Risk Management

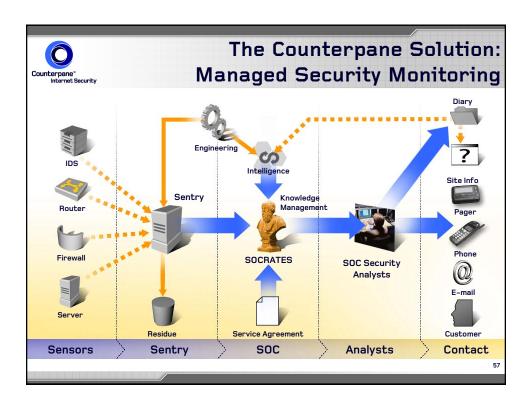
- Prevention, detection, and response
 - Combine the best of products with the best of processes
- 24x7 monitoring of network environment is crucial to reducing the window of exposure
 - More effective, and more cost-effective, than traditional preventive countermeasures
- Prosecution of cyber-criminals is important
- Insurance provides the safety net
 - Insurance is the ultimate risk management tool
 - In the real world, insurance provides absolute security
 - In the real world, insurance drives security requirements
 - Eventually, insurance will drive all aspects of computer and network security

5



Effective Security Comes from Human Intervention

- · Automatic security is necessarily flawed
 - Smart attackers bypass the security
 - New attacks fool products
- Humans can recognize, and respond to, new attacks and new threats
- Expert monitoring is the most cost-effective way to provide security
- Human minds are the attackers: human minds need to be the defenders





Counterpane Internet Security: Unmatched Expertise

- Vigilant
 - Real-time monitoring, 24x7
 - Fast detection, correlation across products
- Adaptive
 - Continual updates: threats, defenses, products
 - Monitoring of underground communities
- Relentless
 - SOC analysts trained in attack methodologies
 - Integrated with intelligence, engineering, customer service
 - High internal security standards



Get More Security...Fast

- No matter where you are in the security process, you need Managed Security Monitoring
 - Expert human intervention maximizes your existing security infrastructure
 - Detection and response tell you where you need to improve
- Counterpane Internet Security can help you
 - Give us a call

5



Two Useful Resources from Bruce Schneier



Secrets and Lies: Digital Security in a Networked World

John Wiley & Sons, 2000 http://www.counterpane.com/sandl.html



Crypto-Gram

free monthly e-mail newsletter http://www.counterpane.com/crypto-gram.html

