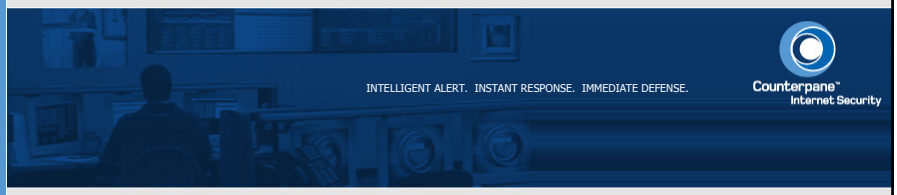
Bruce Schneier
CTO, Counterpane Internet Security

October 2004




# Security Design:
## What Works, What Doesn't, and Why

CSI Asia
Singapore and Beijing

## 1. Security Is a System

Counterpane™
Internet Security

- People often think of security in terms of specific attacks and defenses
- It's not that simple
- Adding security to anything turns it into a system, and systems are complex and elusive beasts
- Understanding systems is the first step toward understanding security

# A Bank Vault

Counterpane™ Internet Security

- Bank vaults secure money against robbers
- But....
  - The combination
  - The usage procedures
  - Customer access
  - Installation
  - Alarms and response
  - Failures



# Understanding Systems

Counterpane™ Internet Security

- If you want to understand security, you need to think in terms of systems
- A system is a collection of simple machines—components—that interact to form a greater whole
- Systems interact with other systems, forming ever-larger systems
- Without the concept of systems, the complexity of modern-day life would be impossible

## Security Systems


- Viewing security in terms of systems is critical to thinking about security
- Security systems interact with other systems; they cannot exist in isolation
- Interactions can happen on purpose, or naturally
- Sometimes, security system affects other systems in surprising ways—these are emergent properties
- Emergent properties often affect security, mostly because they're unanticipated
- A basic mistake is evaluating security as isolated machines or techniques, rather than in the context of the broader systems



## Security Failures


- At a basic level, security systems are different from any other type of system
- Security engineering involves making something—attacks—not work
- It involves figuring out how things fail, and then preventing those failures
- Figuring out how a system fails is more important—to a security expert—than knowing how it works
- And figuring out how it can be *made* to fail is most important

## Security and Safety Engineering


- When designing for safety and reliability, you're designing for a world where random faults occur
- When designing for security, you need to plan for the presence of an intelligent and malicious adversary who forces faults at precisely the most opportune time and in precisely the most opportune way
- Attackers deliberately try to make security systems fail or exploit other people's accidents, and when they find a vulnerability, they can exploit it again and again
- We need to think about how security fails; we need to think like an attacker



## Active Failures and Passive Failures


- Security systems can fail in two different ways:
  - In the face of an attack—*passive failures*
  - By doing what they're supposed to do, but at the wrong time—*active failures*
- Most security systems can fail both ways
- In most systems, active failures are more important
  - There are far more legitimate users than attackers
- A high rate of active failures can mask real attacks
- How a system fails not only affects how successful it is, but how likely it is to be used in the first place

# Security Fails at the Component Level


- Even though security is a holistic system, it doesn't fail in its entirety or all at once
- A piece fails, and maybe that failure becomes a larger failure, and maybe the entire system fails
- We have to look at systems both as a whole and at the components



# Security Fails at the Seams


- The easiest way to attack a system isn't generally head-on
- Security usually fails at the seams
  - Where two systems interact
  - Between security systems and other systems
  - Between parts of a security system
  - When rare conditions occur

## Failures and Rarity

Counterpane™ Internet Security

- When a security event occurs regularly, people become experienced with it and know what to do
- If the event only happens once every few years, there could be an entire office staff that has never seen it
- Computerized systems make mistakes so rarely that operators don't know how to deal with them
- This aspect of human nature can be used to attack systems
- Attackers commonly force failures specifically to cause a larger system to fail



## Expecting Failures

Counterpane™ Internet Security

- An important security precept is to expect systems to fail
- "Unbreakable," "absolute," "unforgeable," and "impenetrable" are all words that makes no sense when discussing security
- Good security systems are designed for failure
- By figuring out how things fail and designing them to fail better, they're made safer

## 2. Technology Causes Security Imbalances


- Sometimes technology can make an enormous difference
- Technology doesn't only aid attackers by making attack tools more powerful; it also makes attack tools more plentiful and easier to use
- Technology creates security imbalances
- Sometimes these imbalances favor the defender, but more often the attacker
- Smart attackers look for leverage points, and technology gives them more leverage



## Complexity and Security


- Throughout history we've seen more and more complex systems
- Computers are more complex than anything else we commonly use, and they're being embedded into everything
- Systems can look simple because much of their complexity remains hidden
- Complexity is great for consumers, but terrifying for security professionals because it fails so badly
- Complexity is the worst enemy of security

## Technology and New Threats


- New technologies can actually create new security risks
- Technological systems require *helpers*: mediators and interfaces between people and the system they interact with
- As helpers mediate more and more interactions, the complexity of the systems supporting those interactions become more complex
- Another cause of security vulnerabilities in modern technological systems are *class breaks*: attacks that can break every instance of that system
- Class breaks mean that you can be vulnerable simply because your systems are the same as everyone else's



## Technology and New Threats (cont.)


- Automation also exacerbates security vulnerabilities in technological systems
- Technology, especially computer technology, makes attacks with a marginal rate of return and a marginal probability of success profitable
- Because class breaks can be automated, they can propagate much faster and cause more damage
- Technology facilitates action at a distance, and this facilitates attacks
- Data aggregation is another characteristic of technological systems that makes them vulnerable

## Attackers Look for Leverage

- Technology continually gives attackers new opportunities for leverage: class breaks, automation, technique propagation, and action at a distance all give attackers leverage
- Leverage is why many people believe today's world is more dangerous than ever
- Leverage is one of the scariest aspects of modern technology, because we can't count on previous constraints to limit the effectiveness of an attacker



## Dual-Use Technologies

- All technology has good and bad uses; it's *dual-use*, to use the military phrase
- When we make a technology generally available, we're trading off all of the good uses of that technology against the few bad uses
- Technology can also reduce some threats, but fast-moving technology generally favors the attacker

## 3. Knowing the Threats Means Knowing the Attackers


- Knowing the attacker allows you to evaluate the risks he poses and the countermeasures that might thwart him
- Attackers can be categorized along several basic lines: objectives, motivations, expertise, access, resources, and risk aversion
- If you mischaracterize your attackers, you're likely to misallocate your defenses—you're likely to worry about nonexistent threats, and ignore real ones



## Who Are They?


- Criminals
- Insiders
- Emotional attackers
- Friends and relations
- Media
- Police
- Intelligence organizations
- Terrorists
- Wartime governments

# Attacker Economics


- Rational attackers choose attacks that gives them a good return on investment
- Attackers consider their particular budget constraints: expertise, access, manpower, time, and risk
- Basically, it's a series of business decisions



# Attacks Don't Change


- There hasn't been a new crime invented in millennia
- What does change is the nature of attacks: the tools, the methods, and the results
- Understanding how attackers work is vital to understanding security; in a sense, the attacker is just another part of any security system

# Smart Attackers Cheat

- Attackers regularly cheat; they think outside the box
- By reframing the problem, they can render existing countermeasures irrelevant
- Most attackers are copycats
  - They aren't clever enough to invent new techniques for fraud
  - They read stories of attacks in the newspaper and think: "Hey, I could do that too"
  - On the other hand, they don't need to think up new ways of attack if the old ways still prove to be effective



# 4. Security Strategies

- A chain will break at the weakest link
- Improve the strength of the weakest link, and you improve the strength of the chain
- Just as the definition of security is subjective, the definition of the weakest link is also subjective
- It's not true that all systems with a single weakest link are insecure, and all systems without one are secure
- And a smart attacker will find the weakest link, or make it

## Rule of Least Effort

- You can't find the weakest link without first doing a threat and risk assessment, and securing the weakest link often costs more than the additional security received
- Too often, we improve security haphazardly, recognizing a problem and fixing it without having identified the weakest link
- Complex systems are much harder to understand and analyze
- On the other hand, it also makes the attacker's job a lot harder, because he might not be able to find the weakest link, either



## Defense in Depth

- The best security systems don't have any single points of failure; when one piece of the security system fails, another piece can take over
- This is called defense in depth
- Relying on a single security countermeasure that may protect you absolutely is much less resilient than relying on a series of countermeasures that can back each other up if one fails
- The best security systems don't have a single point of failure
- Sometimes defense in depth comes through overengineering

# Compartmentalization


- Compartmentalization is another way to help secure the weakest link
- It limits the damage from a successful attack and makes security fail well
- Many attacks can be traced to breaking this principle of compartmentalization
- Compartmentalization also prevents flaws in one security system from affecting other systems
- Compartmentalization makes security systems more robust, because small failures don't easily become large disasters



# Choke Points


- A choke point is another way to secure a weak link—one that forces something into a narrow channel, one that you can more easily secure
- Choke points only work if there's no way to get around them
- Choke points can also get clogged, either accidentally or as part of an attack
- Too many systems use choke points as a replacement for defense in depth or compartmentalization

# Dynamic Security

Counterpane™ Internet Security

- All security systems fail sooner or later, but brittle security systems fail badly; break them at one point, and they break completely
- Good security systems are resilient, and can withstand failures
- Resilient systems are naturally more secure
- A system is resilient if it is dynamic, if it can respond to new threats and new attacks
- Dynamic defenses that can adapt quickly provide more security than defenses that can only perform in a single manner



# Heterogeneousness

Counterpane™ Internet Security

- Homogeneous systems can be brittle because they are more vulnerable to class breaks
- In homogenous systems, when someone invents a new attack, it's almost always a class break
- While diversity is a good security goal, it's rarely possible in modern systems
- Diversity tends to sacrifice the security of the individual in favor of the security of the population

# Trusted People


- People are a double-edged sword
- They are the weakest security link, and why security fails so often
- Every security system needs trusted people to function, though these people are not necessarily trustworthy
- Trusted people can subvert security
- The more trusted people a system employs, and the more you must trust them, the more brittle it is



# Trusted People (cont.)


- There are three basic ways to deal with trusted people or machines
  - Try to put trustworthy people in positions of trust, or at least in positions of extreme trust
  - Compartmentalization
  - Apply the principle of defense in depth: give trusted people overlapping spheres of trust, so that they effectively watch each other
- Trusted insiders are often eager to help, regardless of whether the person they're helping is an attacker or not

# Conclusions: Security Design

Counterpane Internet Security

- Security is a system
  - Think of it as a system
  - Think of how it interacts with other systems
- Think of how the system fails
  - As a system, security fails in surprising ways
  - Think of why can cause it fail, and why
- Develop strategies to minimize the risks

- This stuff is hard
  - There are gotchas everywhere



# Two Useful Resources from Bruce Schneier

Counterpane Internet Security


Beyond Fear:
Thinking Sensibly about Security in an Uncertain World
by Bruce Schneier

Copernicus, 2003
www.schneier.com/bf.html

Crypto-Gram:
Free Monthly Security Newsletter
by Bruce Schneier

www.schneier.com/crypto-gram.html