Non-Security Considerations in Security Decisions

Workshop on Economics and Information Security
29–30 May 2003

Security is Always a Trade-Off

- You can have as much security as you want
  - What are you willing to give up to get it?
- Security always involves trade-offs
  - If no airplanes flew, 9/11 couldn’t have happened
  - Gated communities offer more security but less privacy
- We make decisions every day about these trade-offs
- To do it thoughtfully, we must understand:
  - How security works
  - The threats and risks
  - The costs
Is the Trade-Off Worth It?

- When faced with a security countermeasure, you have to figure out two different things:
  - Is the security countermeasure effective in mitigating your personal risk?
  - Are the problems and trade-offs caused by the security countermeasure worth the additional security?
- You are constantly making that decision
- Sometimes the decision is made for you by others

- I want to formalize that decision process

Five Step Evaluation Process

- Step 1: What assets are you trying to protect?
- Step 2: What are the risks to those assets?
- Step 3: How well does the security solution mitigate those risks?
- Step 4: What other risks does the security solution cause?
- Step 5: What costs and trade-offs does the security solution impose?

- Finally: Is the trade-off worth it?
Why is Security So Rarely About Security?

- People rarely perform this decision
- People succumb to fear and uncertainty
- People believe in false promises of security
- People do things counter to their own security
- People say one thing and do another

Security and Agenda

- Every security decision affects multiple players, and the party who gets to make the decision will make one that’s beneficial to him
- Every player has his own unique perspective, his own trade-offs, and his own risk analysis
- This drives everything about security
- You have to evaluate security opinions based on the positions of the players
- Often security decisions are made for non-security reasons
- The major security issues have nothing to do with security technology
What’s Going on?

These graphics are an attempt at an explanation

Maybe someone with more economics training than myself can help me put an actual model together.

A Security System Protects Assets
Both Legitimate Users and Attackers Interact with the System

The Security Can Fail in Two Ways
There are More Legitimate Users than Attackers

There is a Feedback Mechanism
Threats are Complicated

Attackers Can Be Legitimate Users
And One Outcome of Defense is Attack Diversion

Asset Owner Controls Security System...
...but Not Directly

Asset Owner is Affected by Risks...
...but Not Directly

Asset Owner is Affected by Other Considerations
Asset Owner is Affected by
Legitimate Users

Asset Owner is Affected by
Trusted People
The Effectiveness of the Security System is a Minor Consideration

Examples

- Detecting counterfeit money
- KAL 007
- Salesclerks and credit card verification
- Counterterrorism in the wake of 9/11
- Tylenol poisonings
- Banning things on airplanes
- Home building inspectors
- Mercenaries
- DVD region encoding
- Government regulatory bodies
- Banks’ verification of signatures on checks
- “Your purchase free if you don’t get a receipt”
- ATM cards (in the U.S. vs. in the U.K.)
- Making employees liable for fraud
- Airport screeners (airline-paid vs. TSA)