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-making process
- 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

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

Negotiating for Real Security

- In the end, all security decisions come from a negotiation between players
  - Understanding how to be more secure involves understanding these negotiations
- Each player in a negotiation has his own agenda
  - The power of a player determines how much influence he has in the negotiations
- If you don’t have power in the negotiation, there’s not much you can do to affect your own security
  - You have almost no control over most of the security systems that affect your life
  - This doesn’t mean you’re completely powerless to affect your own security
- When you peel away the surface, security is all about money
  - Getting a bigger say in security means getting more power
Changing Agendas

- The best way to affect your security is to change the environment
  - This changes the agendas of the players
- There are several ways to accomplish this:
  - Government intervention: laws and regulations
  - Marketplace
  - Technology
  - Social norms
- The method that makes sense in any given situation depends on the details of that situation

Aligning Interests with Capabilities

- The goal of a security system should be to manage risks as effectively as possible
- Figure out an acceptable level of risk, based on what trade-offs are necessary to achieve it
- The best way is to have the player in the best position to mitigate the risk also be accountable for it
- A good security system is one where security requirements are aligned with the agendas of the players
Examples

- ATM cards (in the U.S. vs. in the U.K.)
- “Your purchase free if you don’t get a receipt”
- Making employees liable for fraud
- Airport screeners (airline-paid vs. TSA)

Accepting Risk

- Even with all of the security countermeasures we can institute, we simply have accept some risks
- Countermeasures reduce risk, but never to zero
  - Trade-offs can quickly reach the point of diminishing returns
- Negotiate as best we can to mitigate the risks that are reasonable to mitigate, then accept the rest
- We have no choice but to accept residual risk—to do anything else is not to be alive