# Proposing Unsecurity Credits

Mark G. Graff

19 Apr 02

# When I Have Explained All This I Will Stop Talking

- Forces Acting on Corporate Security Today
- A Solution: “Unsecurity” Credits
- Criticisms and Obstacles
- Unsecurity Credits Can Work!
- First Steps
- Summing up

# Forces Acting on Corporate Security Today

- The goal has to be "just enough" security
  - Just enough to keep out of the papers
  - Just enough to avoid lawsuits from stakeholders
  - Just enough to not attract attention of regulators
- Money spent on security cannot be used to advance product line, pay workers, etc.
- It's the Tragedy of the Internet Commons
- Antidote is to force all participating companies to expend resources. Seat belt analogy is useful here

# A Solution: "Unsecurity" Credits

- The Internet is a critical part of the 21st century environment
- Every company on the Net today "pollutes" it, weakening our security with weak practices
- Best-known example: "Zombie" sites used to amplify distributed DOS attacks
- Other impacts: confusion, noise, vandalism effects
- So, penalize polluters--and allow selling/trading of unsecurity credits by those with clean operations

# Criticisms and Obstacles

- "No one will try it"
- "Better security in one place means worse security somewhere else"
- "It will create a vested economic interest in bad security"
- "Companies that are the worst offenders will get the biggest initial allotments"
- "We can't regulate what we can't measure"

# Unsecurity Credits Can Work!

- Require all U.S. publicly traded companies with an Internet presence to participate
- Recognize that an economic interest in bad security practices already exists
- Require U.S.-based multinationals to contribute to U.S. national security
- Acknowledge that a rising tide lifts all boats
- Yes, we need sound security metrics now!

# First Steps

- Promote awareness of Internet security as a critical national/international resource
- Hold the line against indemnifying
  (a) software vendors against security bugs
  (b) corporate officers against unsecure practices
- Require publicly held companies to operate basic security programs (like anti-drug awareness)
- Fund research into network security metrics
- N.B. Model also works inside enterprise networks

# Summing up

- We will only progress by recognizing and accommodating the economic forces acting on U.S. corporations
- “Pollution credits”, while still controversial, set a sound and effective precedent
- The biggest obstacle is the lack of established, standardized security metrics. This must be a top national security priority

# Mark G. Graff

Internet Security Foundation International

www.markgraff.com

Markg@meer.net