# Networks, security, and economics

Andrew Odlyzko

Digital Technology Center
University of Minnesota

odlyzko@umn.edu
http://www.dtc.umn.edu/∼odlyzko

Motivation and outline:

- Basic question: Why haven't cryptography and security lived up to their promise?
  - Is the future going to be any better?

- Main points:
  - Strong economic, social, and psychological reasons for insecurity
  - People and formal methods don't mix well
  - We will continue to rely on the equivalent of chewing gum and bailing wire for security
  - Need to think not of absolute security but of adding "speed bumps" to the "Information Superhighway"

# Honor System Virus

This virus works on the honor system.

Please forward this message to everyone you know and then delete all the files on your hard disk.

Thank you for your cooperation.

More seriously:

- Nigerian 419 scam
- “social engineering”
- ...

Do not expect improvement: teaching people about security won’t help because:

- growth in ranks of users of high tech
- proliferation of systems and devices

improvements in usability of individual systems and devices to be counteracted by growth in general complexity

# Human difficulty with formal reasoning illustrated by the Wason selection task:

Rule: People traveling from DC to NYC take the train

- Alice: went to Boston
- Bob: flew
- Charlie: went to NYC
- Donna: took the train

Problem: which cards (each one with one side describing where an individual went, the other side how that person got there) have to be turned over to decide whether rule is satisfi ed.

Typically about 25% get this right!

The other part of Wason selection task:

Rule: A kid that has ice cream for dessert has to do the dishes after dinner

- Alice: had apple pie
- Bob: watched TV
- Charlie: had ice cream
- Donna: washed dishes

This time on the order of 75% of the people get it right!

Main point of citing the Wason selection task:

Shows people are optimized for some tasks, but logical reasoning is not one of them

Note that typical 4-year old is far superior to any computer in speaking, understanding speech, face recognition, ...

Major problem with secure systems:

secretaries could not forge their bosses’ signatures

Intentional ambiguity (in proposed SEC rule for corporate lawyers):

Evidence of a material violation means information that would lead an attorney reasonably to believe that a material violation has occurred, is occurring, or is about to occur.

vs.

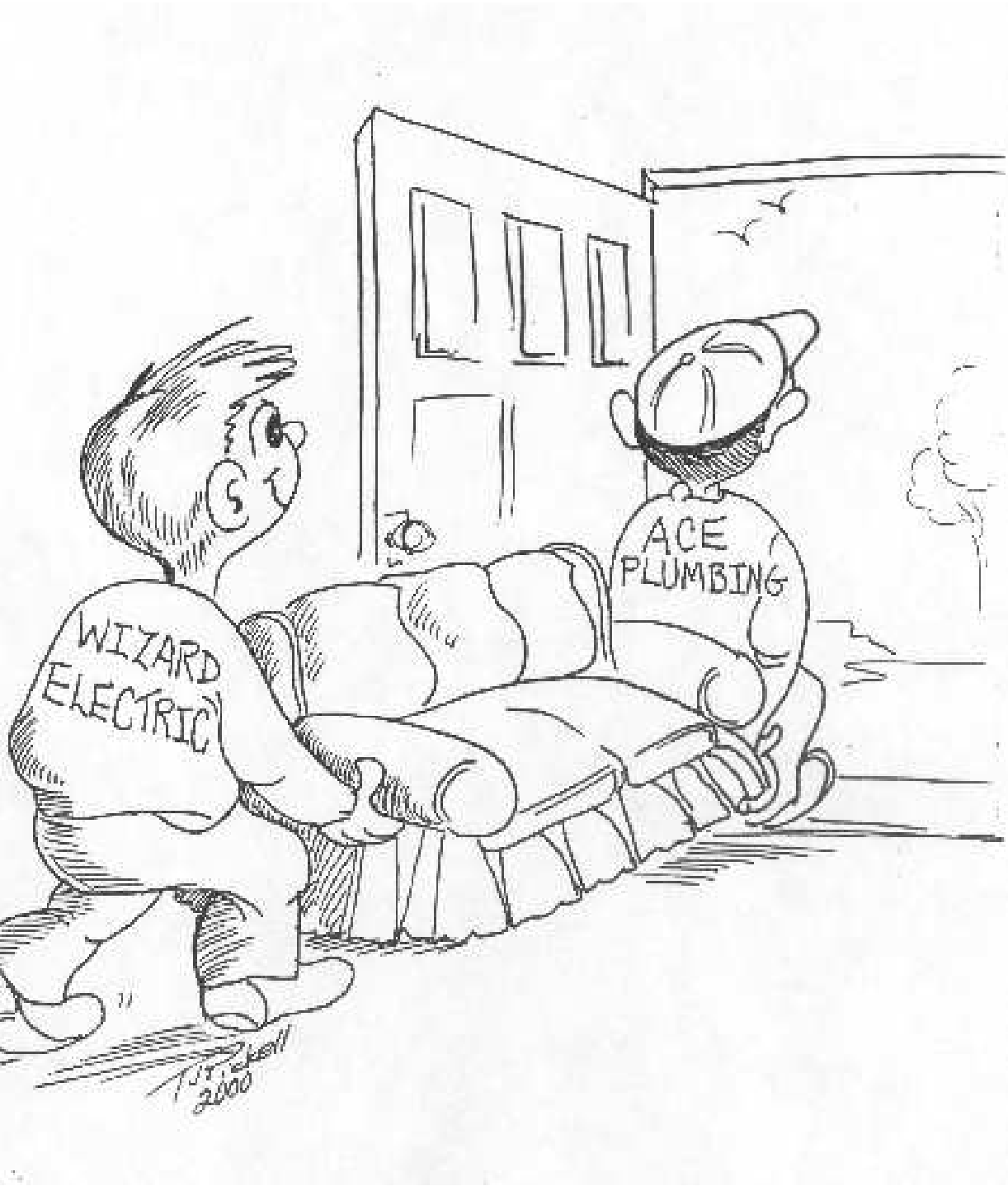
Evidence of a material violation means credible evidence, based upon which it would be unreasonable, under the circumstances, for a prudent and competent attorney not to conclude that it is reasonably likely that a material violation has occurred, is ongoing, or is about to occur.

It is easy to make fun of lawyers, but don’t we all like to have some slack in our lives?

Deeper ambiguity of human discourse:

Please let the plumber in to fix the leaky faucet.


WIZARD
ELECTRIC
ACE
PLUMBING


WIZARD ELECTRIC
ACE PLUMBING

Yet somehow we have managed to live with all this ambiguity!

The formal world and the human world do overlap and interact, but are far apart.

The formal world was supposed to provide security for the human world, but it is the messy features of the human world that help compensate for the insecurity of the formal world.

How have we survived all these decades of computer and network insecurity?

Many disasters (Long Term Capital Management, WorldCom, Enron, ...) but not a single one where electronic insecurity played a serious role!

1980s: the “Golden Age” of civilian cryptography and security

1980s: the “Golden Age” of fax, including faxed signatures

Search for defi nition of a digital signature hampered by lack of defi nition of ordinary signature:

validity of ordinary signature depends on a variety of factors (such as age of signer, whether she was sober, whether she had a gun pointed at her head, whether the contract is allowed by law, ...)

Why does a fax signature work?

It has to be viewed in context of the entire transaction it is part of. (And it is not used for defi nitive versions of large contracts, ...)

Traditional security concerns of technologists apply to cyberspace.

Cyberspace is just a piece of human space, for physical, social, and economic reasons.

Key factor: economic desirability of price discrimination (which is facilitated by lack of anonymity):

Charlie: willing to prepare a report on digital cash for $1,500

Alice: willing to pay $700

Bob: willing to pay $1,000

Uniform pricing makes transaction impossible

Charging Alice $650 and Bob $950 makes everybody better off (in conventional economic model)

Airlines and railroads: different services or price discrimination?

There was some doubt a century ago, when privacy (transferable tickets) limited what railroads could do, but today, it is clear that price discrimination is the main driving force behind airline yield management:

Fares offered at www.continental.com on Feb. 27, 2002:

Minneapolis to Newark, NJ on Wed., March 20, returning Fri., March 22: $772.50

Minneapolis to Newark, NJ on Wed., March 20, returning Wed., March 27: $226.50

Newark, NJ to Minneapolis on Fri., March 22, returning Fri., March 27: $246.50

Airline “yield management” enabled by lack of anonymity and non-transferability of tickets, which tie passengers to rest of world.

The role of cyberspace is increasing, and attacks and other actions in cyberspace are faster and more far-reaching than in physical space.

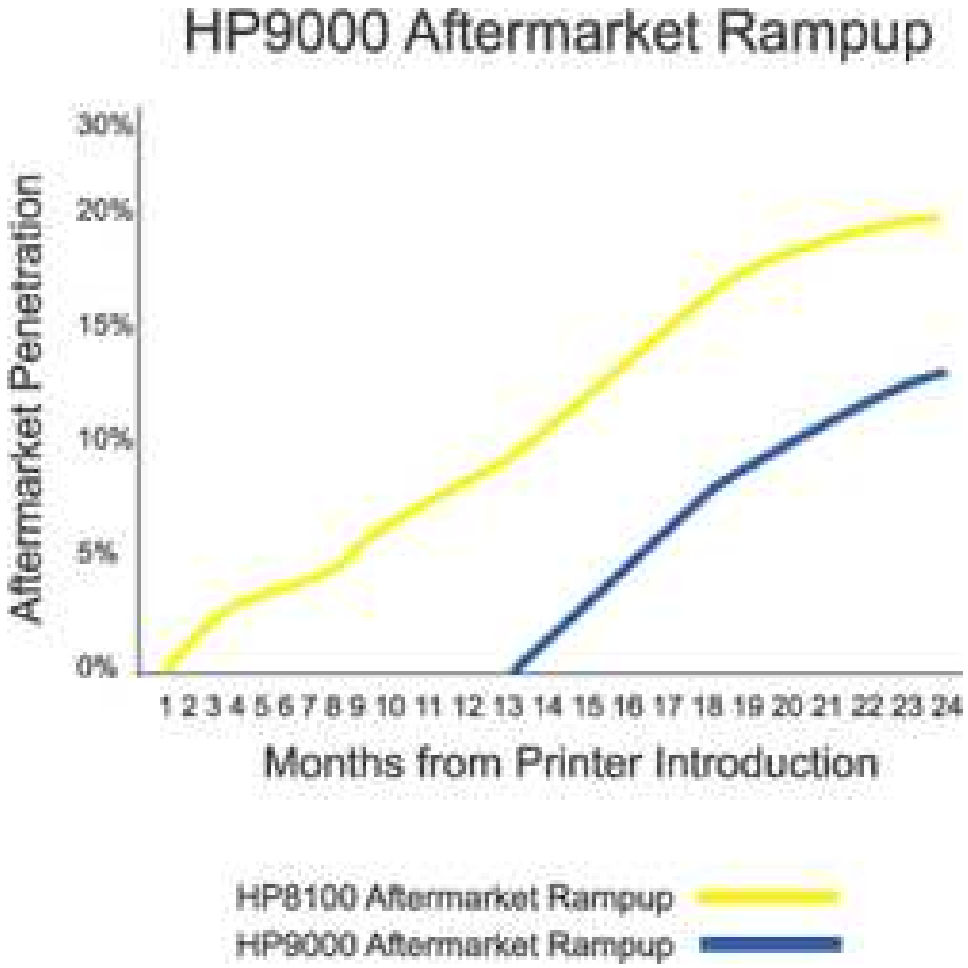
Partial solution:

speed bumps


SPEED LIMIT
186,000 MPH
"It's the LAW"


SPEED LIMIT
186,000 MPH
"It's the LAW"

Quantifi able benefi ts of (incomplete) security:



(Tentative) conclusions:

- We will continue to live on the edge of intolerable insecurity
- Keep usability factors and generally psychology, economics, and sociology in mind
- Keep in mind the opponents' psychology, economics, and sociology
- Think of security as speed bumps
- Consider biological analogies: diversity vs. monoculture, limiting rates of infection, ...
- Compartmentalization
- Require centralization of human expertise, to achieve economies of scale
- Instead of impregnable defense, think of combination of defense and counterattack

References: several papers and conference presentations at
http://www.dtc.umn.edu/∼odlyzko
including two not there yet, as they are in preparation ("Privacy, economics, and price discrimination on the Internet" and "Stronger copyright protection for cyberspace: Desirable, inevitable, and irrelevant")

Also:

- Ross Anderson, Liability and computer security - nine principles, 1994
- Dan Geer, Risk management is where the money is, 1998
- Shapiro and Varian, *Information Rules*, Harvard Business School Press, 1998
- Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, 2000
- Ross Anderson, *Security Engineering - A Guide to Building Dependable Distributed Systems*, 2001