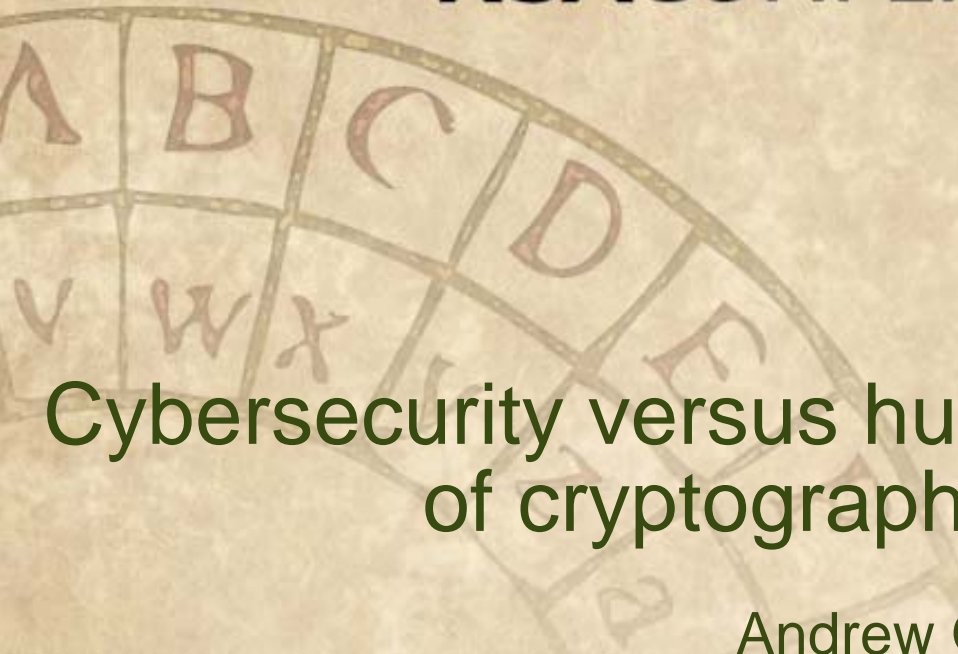





RSA[®]CONFERENCE 2007



Cybersecurity versus human space, and the role of cryptography and security

Andrew Odlyzko,
Digital Technology Center, University of Minnesota,
02/09/2007 - CRYP-402



Motivation and outline:

- **Basic question: What is the role of cryptography and security in society?**
 - 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 baling wire for security
 - Need to think not of absolute security but of adding “speed bumps” to the “Information Superhighway”

Many limitations on ecommerce schemes from economics:

- **reigning dogma of telecom world: charging by the byte or minute**
- **supported by increasing ability to price discriminate**

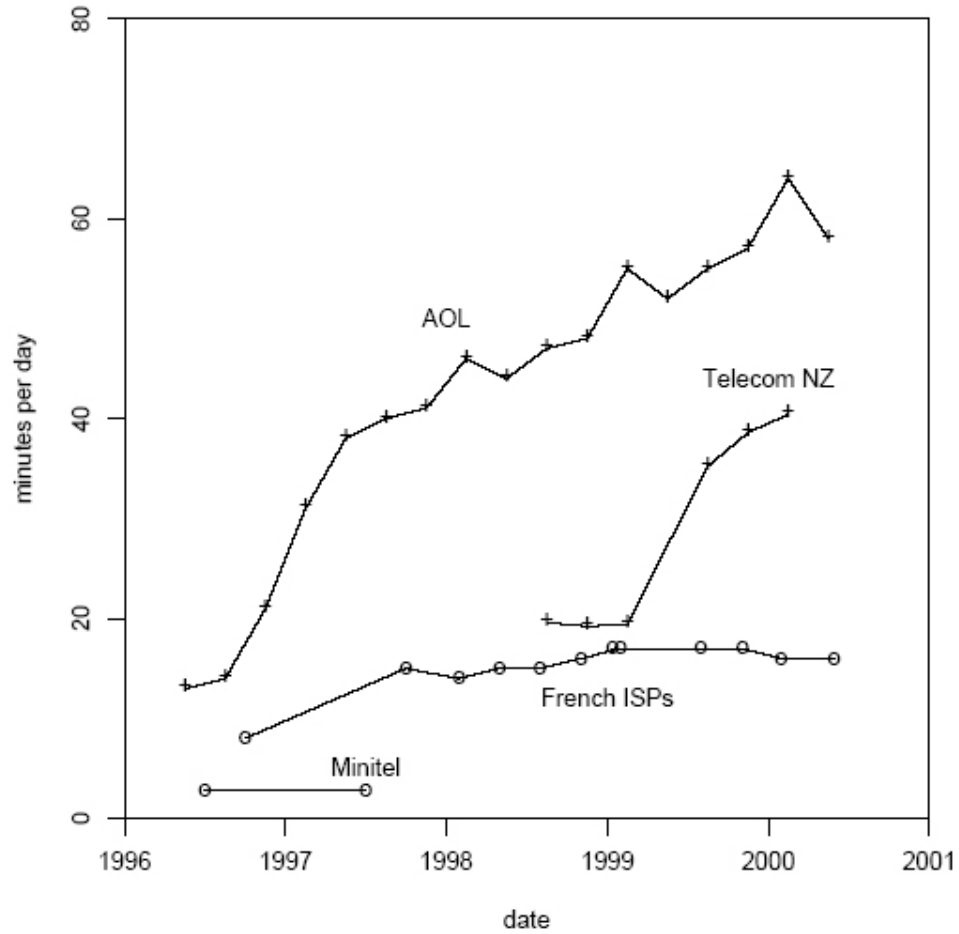
Flat rate pricing as bundling: Alice is interested in downloading 1 MB per month from each of 10 Web sites

site	willingness to pay
1	\$ 0.40
2	0.80
3	1.20
4	1.60
5	2.00
6	2.40
7	2.80
8	3.20
9	3.60
10	4.00
total	\$22.00

If charge per byte, maximal revenue is \$12.00

Effects of flat rates on usage:

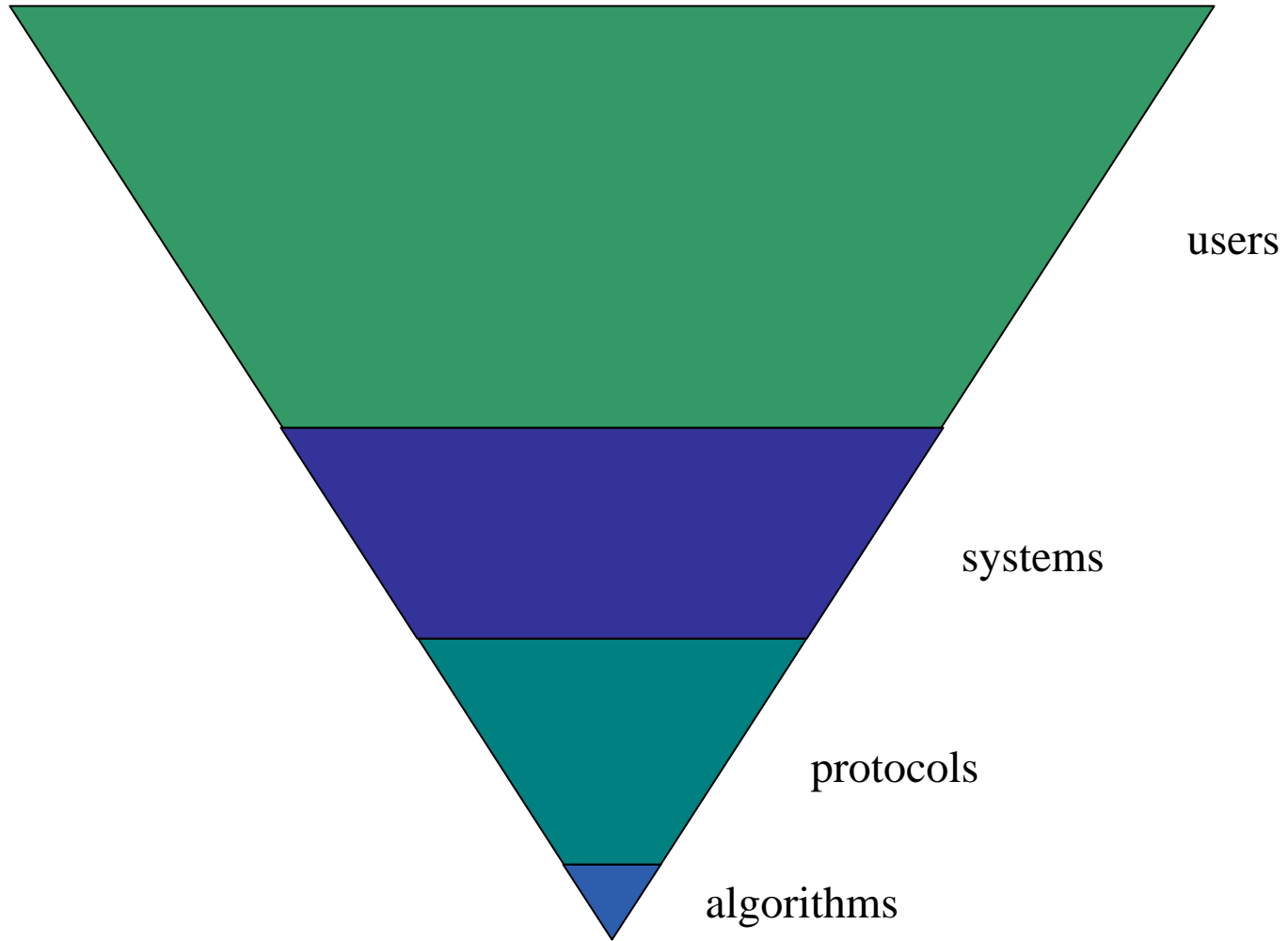
subscriber time online as function of pricing



Civilian cryptography of last 30 years:

- **huge intellectual achievements, based on (and providing stimulus for) mathematics:**
 - integer factorization
 - lattice basis reduction
 - probability
 - elliptic and hyperelliptic curves
 - algebra
 - ...
- **limited by human nature**

Security pyramid:



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:

- **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 Philly 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 satisfied.

Typically about 25% get this right!

The other part of Wason selection task:

Rule: A child that has ice cream for dessert has to wash 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, ...

General problem of innumeracy:

- **No appreciation for power of compound interest**
- **Most spreadsheets flawed**
 - R. Panko, spreadsheet research website:
<http://panko.cba.hawaii.edu/SSR/home.htm>
- **Many peer-reviewed papers use statistics incorrectly**

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.



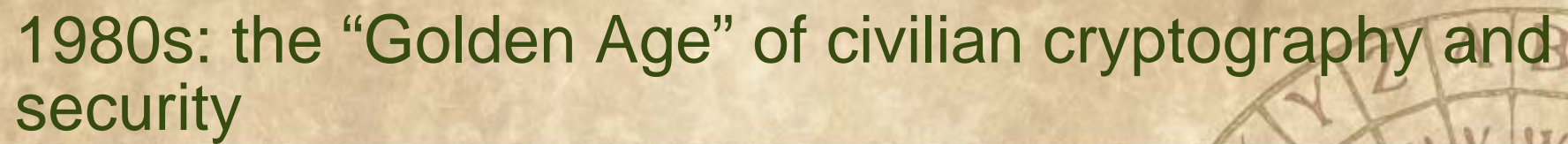


The dog that did not bark:

- **Cyberspace is horribly insecure**

- **But no big disasters!!!**

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



But also:

the “Golden Age” of fax, including faxed signatures

Why does a fax signature work?

- Hard to do serious damage with a single forged fax
- Fax usually just one of many elements of an interaction (involving heterogeneous elements, such as phone calls, emails, personal meetings, ...)

The role of a fax signature has to be viewed in the context of the entire transaction. (And it is not used for definitive versions of large contracts, ...)

Search for definition of a digital signature hampered by lack of definition 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, ...)

Traditional security concerns of technologist apply to cyberspace



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

A Declaration of Independence of Cyberspace

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

...

You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions.

...

Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

...

Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here.

...

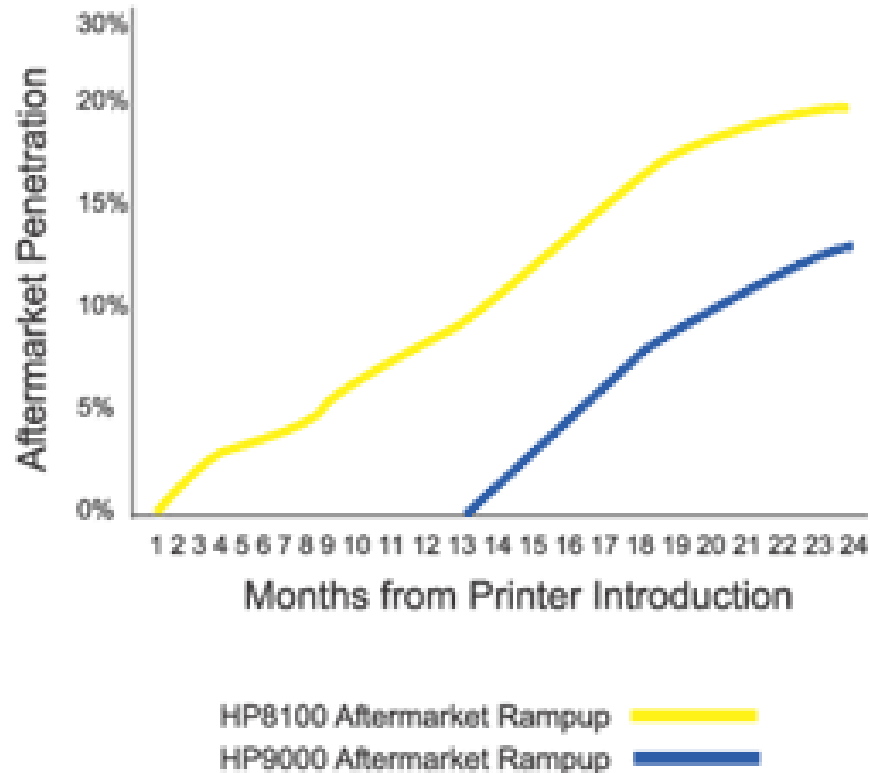
— John Perry Barlow, 1996

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

- Partial Solutions: Speed bumps
- Example: e-voting
 - Untrustworthy electronic systems compensated by printed record of vote

Quantifiable benefits of (incomplete) security:

HP9000 Aftermarket Rampup



Speed of light vs. effective speed of change

- "Internet time" a key misleading myth of the bubble
- diffusion of information (even security holes) not instantaneous
- "hiding in plain sight"

Some contrarian thoughts:

- security through obscurity
- value of code obfuscation, "spaghetti code," ...
- value of "least expressive languages"
- (and not least) law and lawyers

(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>

Especially “Economics, psychology, and sociology of security”
and the literature cited there.