How to live and prosper with insecure cyberinfrastructure

Andrew Odlyzko
Digital Technology Center
University of Minnesota
http://www.dtc.umn.edu/~odlyzko

Main points:

- Dominant issue in security: people
- Economics, psychology, and sociology trump technology
- We are incapable of building secure systems (and could not live with them if we could)
- Chewing gum and baling wire will continue as main security techniques
- Math and CS research efforts important, but should be redirected

Half a century of evidence:

- People cannot build secure systems
- People cannot live with secure systems

Civilian Cryptography of last 30 years:

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

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.

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

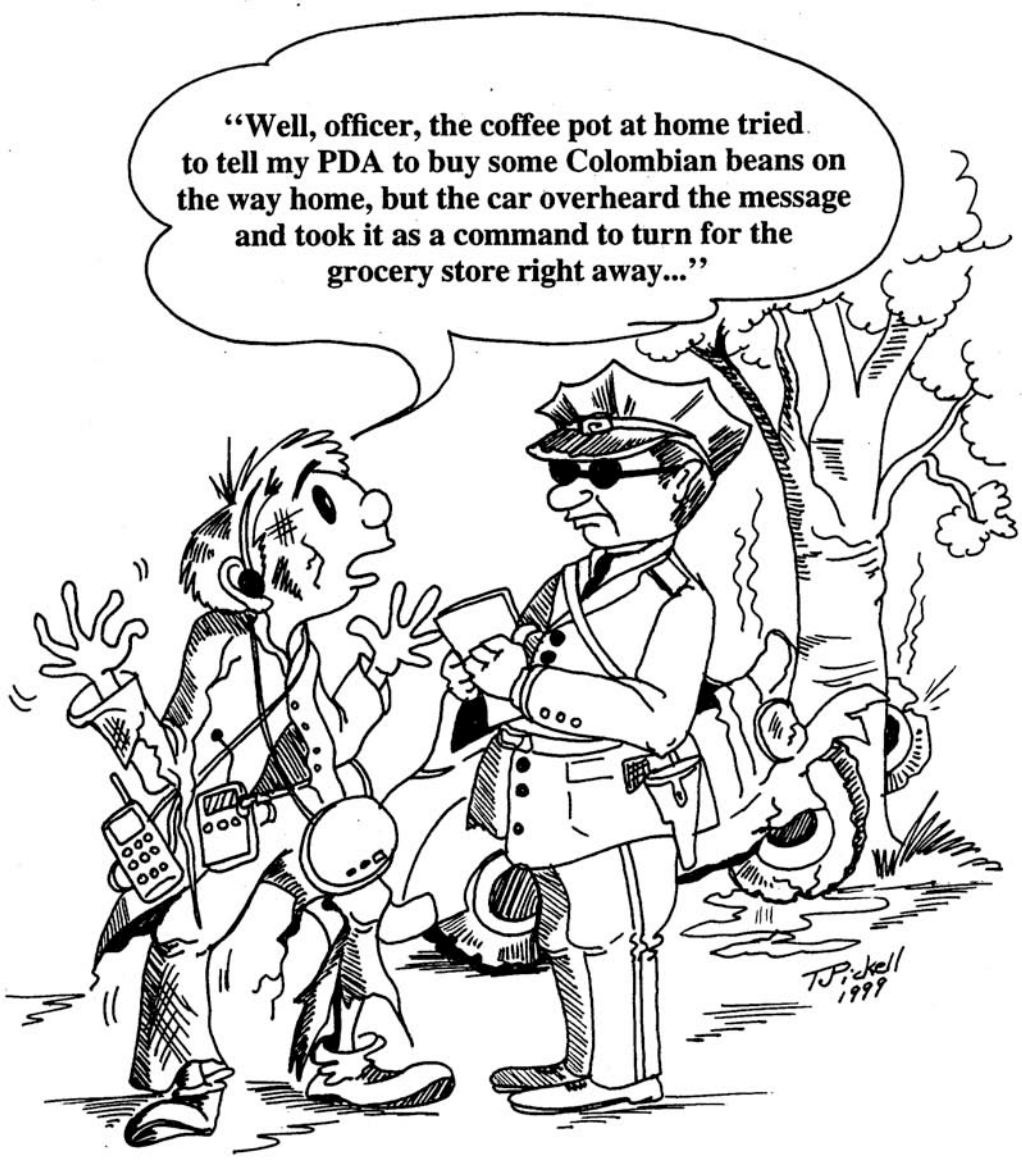
Evidence of a material violation means information that would lead an attorney reasonably to believe that a material violation has occurred, is occurring, or is about to occur.

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.

Do not expect improvement: teaching people about security won't solve the problem:

- **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**


"Well, officer, the coffee pot at home tried to tell my PDA to buy some Colombian beans on the way home, but the car overheard the message and took it as a command to turn for the grocery store right away..."
T.J. Pickell 1999

1980s: the "Golden Age" of civilian cryptography and security

But also:

the "Golden Age" of fax, including faxed signatures

The dog that did not bark:

- **Cyberspace is horribly insecure**

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

The Big Question:

- Why have we done so well in spite of insecurity?
- Will this continue?
- What can we learn?

More general puzzle: Prosperity and appalling innumeracy

- confusing millions with billions
- most spreadsheets flawed
- peer-reviewed papers with incorrect statistical reasoning

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, ...)

Human space vs. cyberspace in technologist view:

- separate
- cyberspace a new world
- cyberspace to compensate for defects of human space

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

Cold dose of reality:

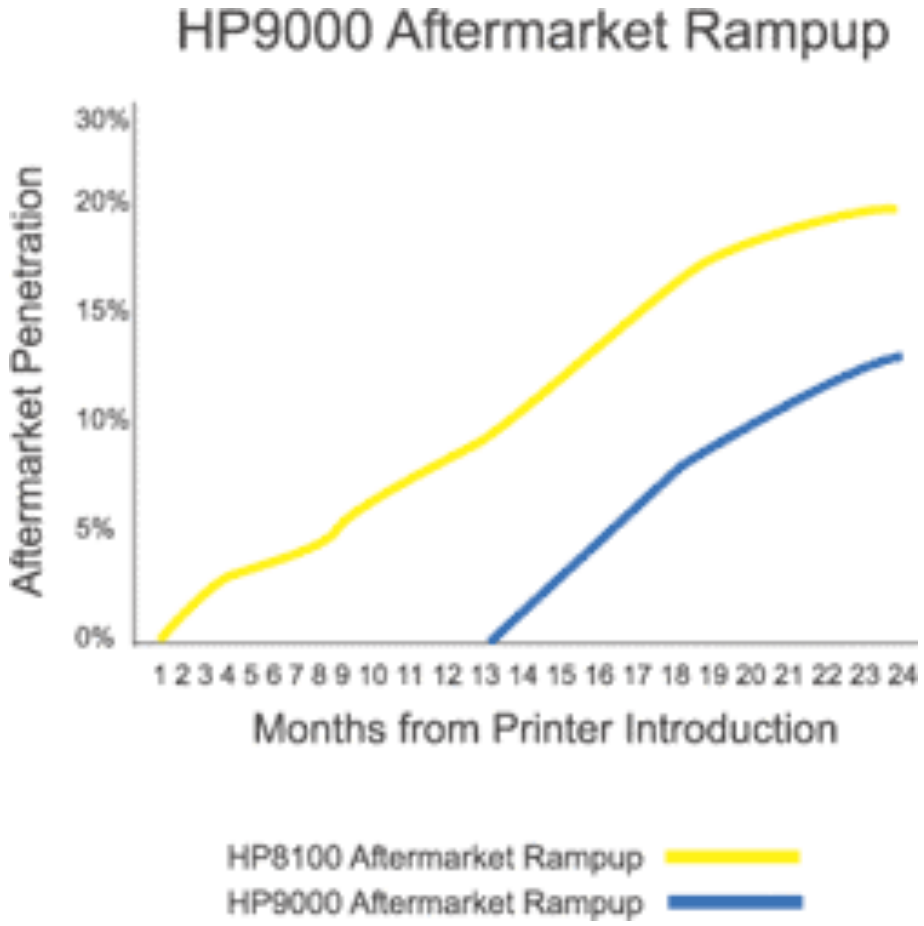
- human space and cyberspace intertwined
- human space compensates for defects of cyberspace

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:



Contrarian lessons for the future:

- learn from spammers, phishers, …
- build messy and not clean
  - create web of ties to other systems
  - permanent records

Contrarian lessons for the future (cont'd, in detail):

- security through obscurity
- code obfuscation, "spaghetti code," …
- "least expressive languages"
- rely on bad guys' human failings
- law and lawyers

Further data, discussions, and speculations in papers and presentation decks at:

http://www.dtc.umn.edu/~odlyzko