Providing security with insecure systems

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

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
  - Chewing gum and baling wire will continue to rule
  - Not absolute security but “speed bumps”
  - New design philosophy and new research directions

Half a century of evidence:

- People cannot build secure systems

- People cannot live with secure systems

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.

Major problem with secure systems:

- secretaries could not forge their bosses’ signatures

Proposed solution:

- **Build messy, not clean**

- (Lessons from past and now)

- (Related to “defense in depth,” “resilience.” …)

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?

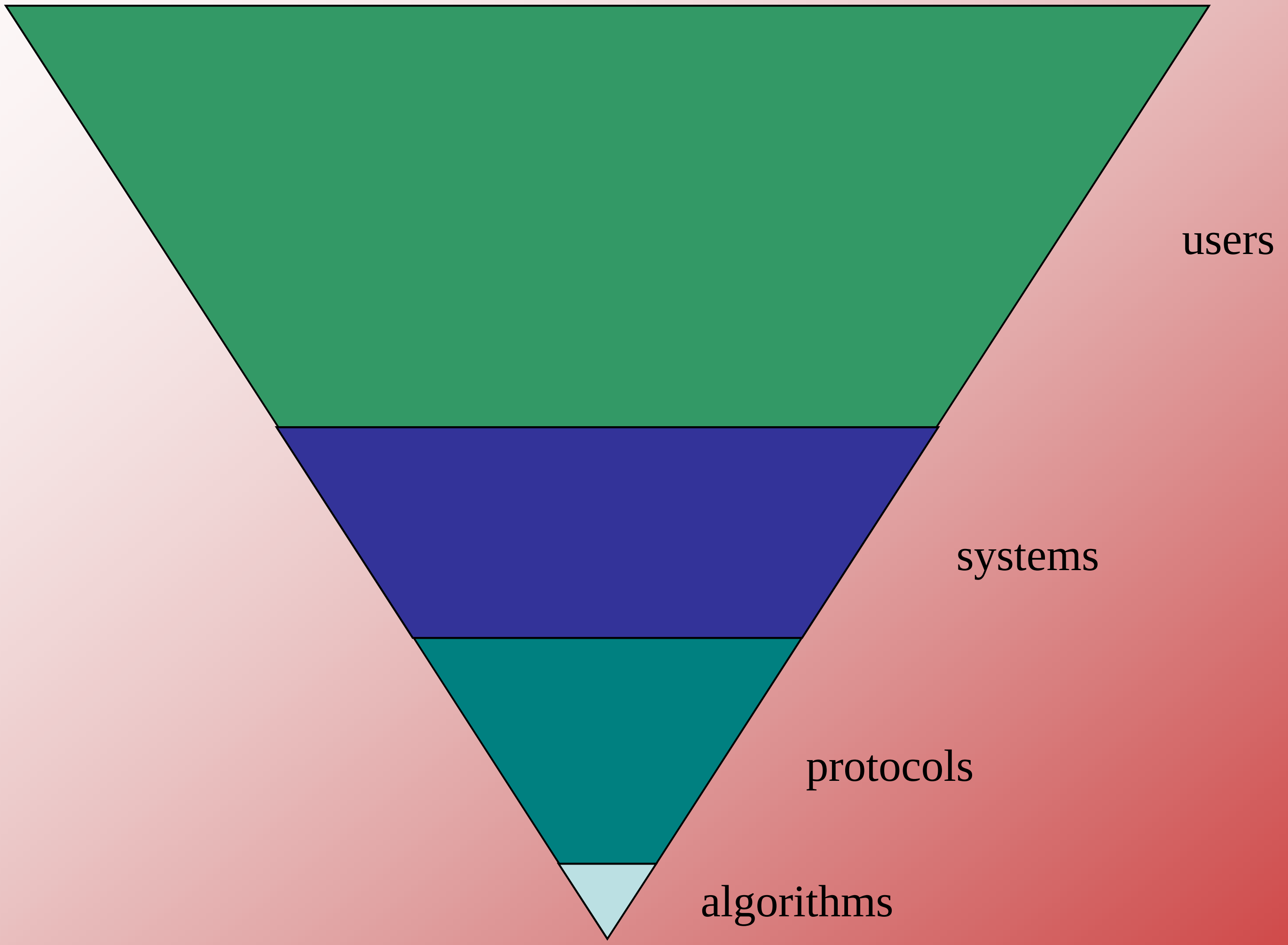
Key point:

- **security is not the goal, just an enabler**

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:



Human vulnerabilities:

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

More general puzzle: Prosperity and appalling innumeracy

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

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

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

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

But also:

the “Golden Age” of fax, including fax signatures

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

But also:

the “Golden Age” of fax, including fax signatures

Now : deposits of scanned, emailed checks!

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, ...)

Human space vs. cyberspace in technologists' view:

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

Cold dose of reality:

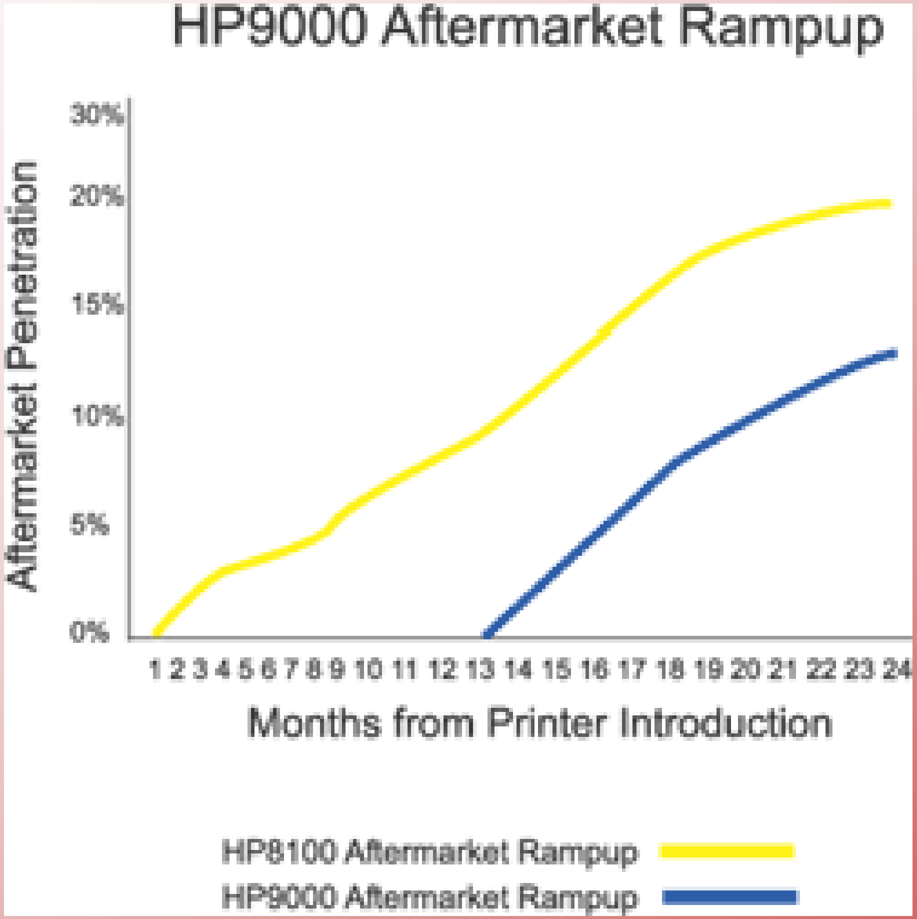
- human space and cyberspace intertwined

- 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:



Advantages of messy: April 20, 2010 story about Apple

- Apple claim: “jailbreaking iPhone OS major source of instabilities, disruption of service”
- Does Apple want clean, modular OS?
- (incentives, incentives, …)

If you can barely keep your system running:

- **how useful will it be to your opponent?**

Contrarian lessons for the future:

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

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"

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