

What Price Insularity?

Dialogs about Computer Security Failings

Fred B. Schneider

Department of Computer Science
Cornell University
Ithaca, New York 14853
U.S.A.

Joint work with Deirdre Mulligan, Aaron Burstein

di·a·logue

Variant(s): *also* **di·a·log** /'dɪ-&-"lɒg, -"lɑːg/

Function: *noun*

Etymology: Middle English *dialoge*, from Anglo-French *dialogue*, from Latin *dialogus*, from Greek *dialogos*, from *dialegesthai* to converse, from *dia-* + *legein* to speak -- ...

...

2 a : a conversation between two or more persons; ... b : an exchange of ideas and opinions <organized a series of *dialogues* on human rights> c : a discussion between representatives of parties to a conflict that is aimed at resolution <a constructive *dialogue* between loggers and environmentalists>

Merriam Webster Online Dictionary

Surprised?

Trustworthiness problems invariably involve solutions with **both** technical and policy dimensions.

- Neither dimension can be ignored.
- Neither dimension provides the whole solution.
- Separation of concerns is inappropriate.
- Interactions are fine grained.
- “System” is larger than you might think.

Examples = Current Events

- E-voting
- Digital rights management (DRM)
- Trusted computing platforms
- Identity fraud and Identity theft
- Liability for software producers
- Network neutrality

Dialog:

ID Fraud and ID Theft

ID fraud: abuse information to impersonate and charge purchases to the victim.

ID theft: abuse information to create new accounts and use these for purchases or other actions attributed to the victim.

ID Fraud and ID Theft: The Way of the World

- Seller rolls losses into cost of doing business.
 - All customers pay for the crime.
- Costs to victim:
 - Loss of reputation.
 - Lost time to correct the record.

What's wrong with this picture?



ID Fraud and ID Theft: Reality: Credit Cards

Modern credit card transactions
(1951 -):

- In person:
 - charge plate, acct num, and signature
- By phone:
 - acct num and past signature
- Over the network:
 - acct num



ID Fraud and ID Theft:

Identification and Authentication

Identifier: label associated with an individual.

Authenticator: Establishes confidence that speaker is who it purports to be.



Authentication is based on:

- Something [not easily forged that] you have.
- Something [secret that] you know.
- Something [that is a hard to forge characteristic] you are.

ID Fraud and ID Theft: Identification → Authentication

Modern credit card transactions (1951 -):

- In person:
 - charge plate, acct num, and in-person signature
- By phone:
 - acct num and past signature
- Over the network:
 - acct num



} 2 factor authentication !!!!



} 0 factor authentication !!!!

ID Fraud and ID Theft:
Solution to Managing Losses

- Create incentives for better security.

ID Fraud and ID Theft: Managing Losses

- ~~Create incentives for better security.~~
- Cap cardholder liability at \$50.00.
 - Losses passed thru to merchants
 - Use on-line fraud detection
 - Requires “matching” → privacy issues
 - Add verification numbers to cards
 - Authenticator today; identifier tomorrow!



ID Fraud and ID Theft: Cultural Disconnects

Failures to distinguish between identifiers and authenticators:

- Social security numbers
- Mother's maiden name

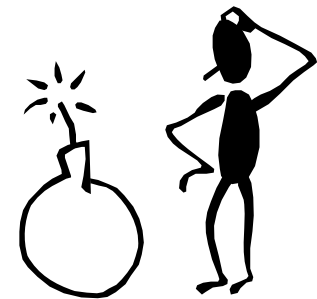


Hide problems from relevant principals.

- If only credit card users knew...

Manage the wrong risks.

- Pain of repairing your credit history?



ID Fraud and ID Theft: Fixing the Problem

- Make it difficult to steal identifiers (*qua* authenticators)
 - Incentivize / enable use of:
 - encryption, access control, trusted computing, ...
 - authenticate both sides of transaction (people + machines),
 - intrusion detection, ...



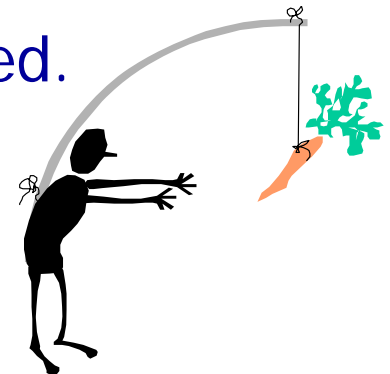
ID Fraud and ID Theft: Incentivizing a Solution

- **Institutions** have little to gain but have much to contribute.
- **Individuals** have much to gain but have little to contribute.

Government: Fosters the greater good when parties lack incentives / power to compel appropriate behavior.

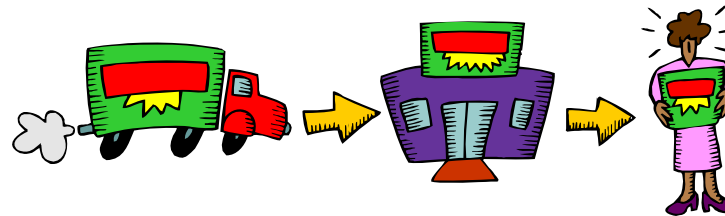
Dialog: Security Investment

- Systems today are not secure.
 - Technology **does** exist to make them more secure.
 - (Ultimately research will be needed, too.)
- To build systems with better security has costs:
 - Increased development time.
 - Fewer features.
 - More and/or better developers.
- Incentives for investment in security are needed.



Security Investment: Clean Slate vs Reality

- “Ideal” incentive scheme:
 - economically efficient.
 - apportions profits according to risk.
 - apportions costs according to benefit.
- Supply chain realities:
 - producers / consumers / users
 - “surprise” implications of software universality



Security Investment: Bridging the Gap

A gap:

- Self-interests of individuals.
- Interests of greater society.

A bridge:

- Avoid legal costs.
- Avoid fines and damages.

Agent of change: accusations by

- the government.
- the private sector.



Security Investment: Liability for Software?

Law 101: “Negligence involves 5 elements:

- Duty
- Breach
- Cause in fact
- Proximate cause
- Damages



... but two can be problematic for software.



Security Investment:

Liability versus Duty

Duty as: Expectations for performance.

- Unable to specify security performance...
- Unable to measure security performance...

Duty as: Extent to which best practices employed in development:

- Correspondence between process and results is tenuous.

Security Investment: Damages

- Damages can be disclaimed for use in certain (all?) settings.
 - ... breach of duty becomes moot.



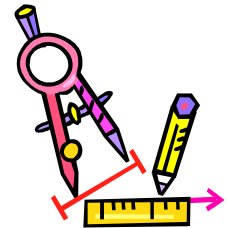
- The “Lloyds of London” conundrum:
 - What if nobody is willing to produce software for a given market?
 - Consumers must choose: abuse existing software or don’t build systems



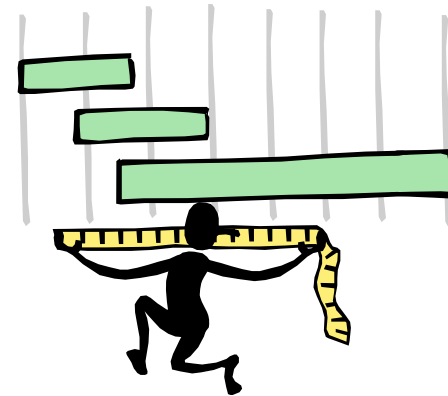
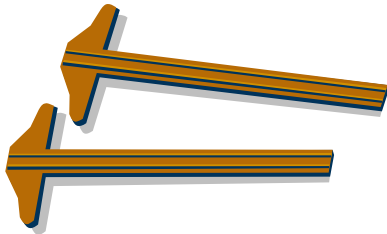
Security Investment: Trustworthiness Metrics

Absence of

- Metrics for evaluating trustworthiness
- Specifications for describing trustworthiness



is a significant impediment to use of traditional incentives for deploying more secure systems.



Dialog:

Network Neutrality

Network Neutrality: Prohibits discrimination by ISP's regarding

- Content
- Applications
- Services
- Origin or Destination

they themselves do not provide.

Analogy to telephone network:

- Hush-a-phone (1956)
- Carter-phone (1968)

Network Neutrality: Hobson's Choice?

Network Neutrality

-versus-

Incentives to invest in new infrastructure.

-versus-

Network trustworthiness.

... "trustworthiness exception"?

Network Neutrality: Net Neutrality “Principles”

ISP, thou shall not:

- block or degrade traffic based on source,
- allow packet routes to be controlled,

Network Neutrality: Net Neutrality “Principles”

ISP, thou shall not:

- block or degrade traffic based on source,
 - Denial of Service defense?
- allow packet routes to be controlled,
 - Ensure packets transit “friendly” countries
 - Enable path-disjoint routing of packet replicas

Disclosure, disclosure, disclosure!

Some Lessons to Learn

- Dialog 1 (id Theft)
 - Evolution (comm) without revolution (auth).
 - Exposing vs hiding (\$ loss) problems.
 - Addressing proximate vs actual problems
- Dialog 2 (Investing in Security)
 - RoI driver vs unsolved technical problem (metrics).
- Dialog 3 (Net Neutrality)
 - Actions by ISPs vs motivation makes all the difference.