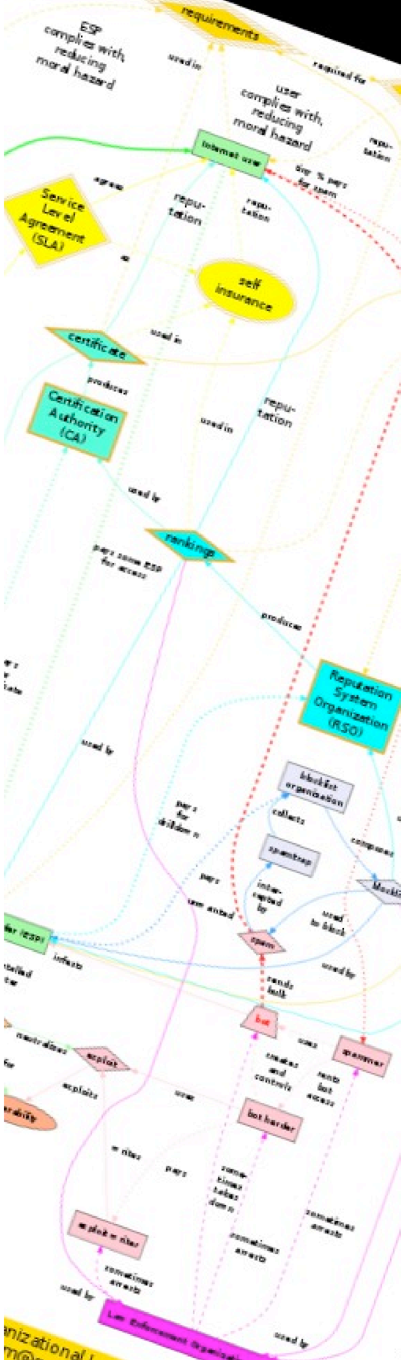
Transparency as Incentive for Internet Security:

Organizational Layers for Reputation

John S. Quarterman, Quarterman Creations
Andrew B. Whinston, U. Texas at Austin
Serpil Sayin, Koç University
E. Vijaya Kumar, J. Reinikainen, J. Ahlroth
IIAR Project

http://crism.mccombs.utexas.edu/iiar-project

Supported by NSF grant no. 0831338; the usual disclaimers apply.



Email

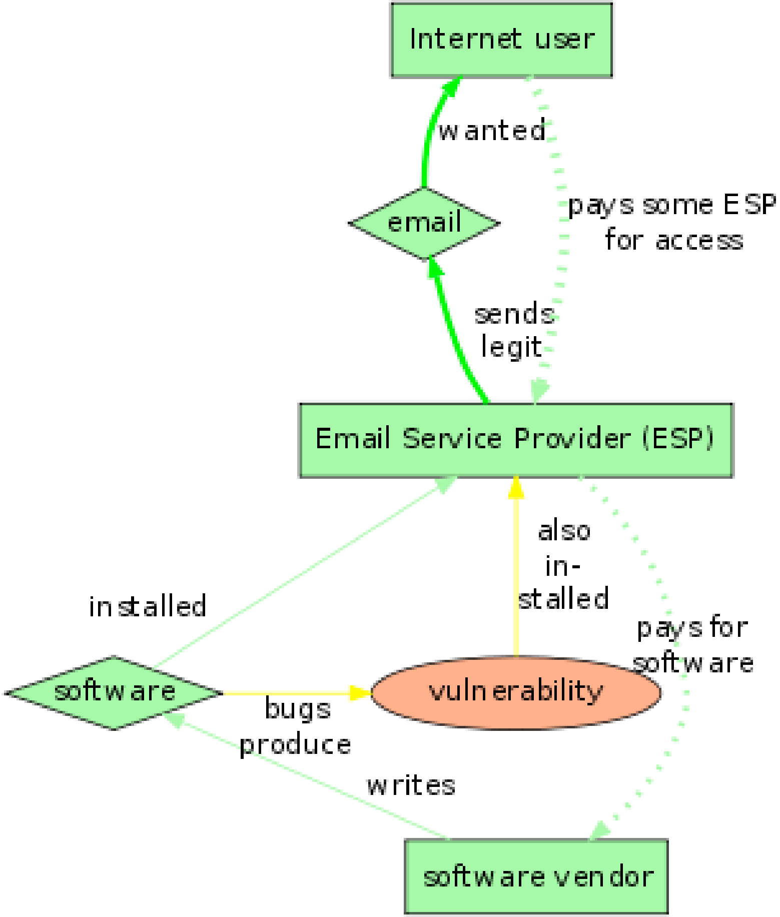


Figure 1: Email (http://cism.mccombs.utexas.edu/iiar-project antispam@quarterman.com)

- Many uses:
  - Banks send statements
  - Professors and students
  - Corporations and customers
- Oops: vulnerabilities

Email

Spam

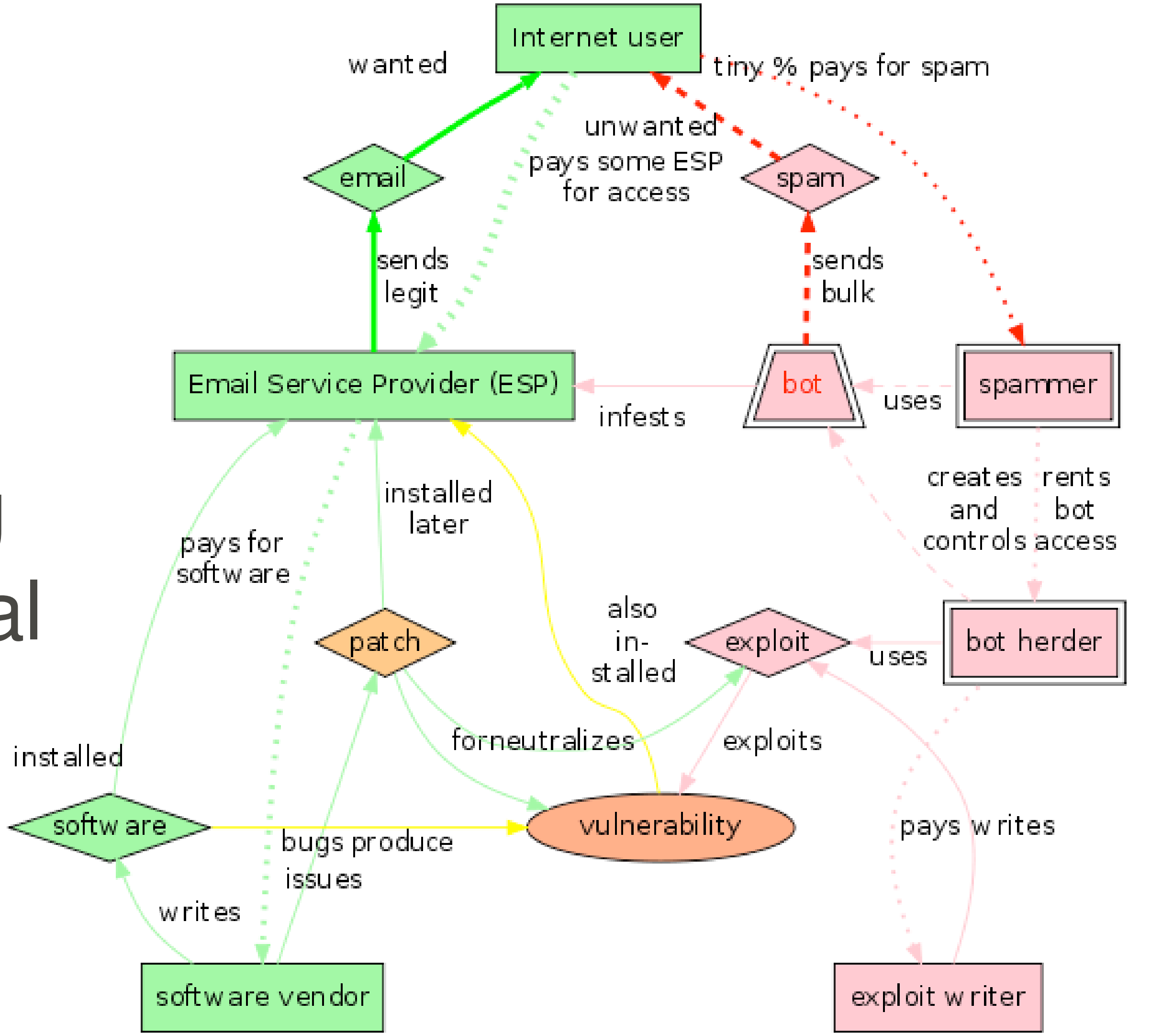


Figure 2: Spam (http://cism.mccombs.utexas.edu/iiar-project antispam@quarterman.com)

Existing Technical Layers

Criminal Economy

Economic Incentives

Profit: Spammers, bot herders, phishers, et al.:
They're all in it for the money.

Loss: Email service providers (ESPs),
any organization that sends email,
from ISPs to universities:
Security is an expense, a cost center.
And *outbound* spam is an externality.

Action: How do we change this?

Blocklists

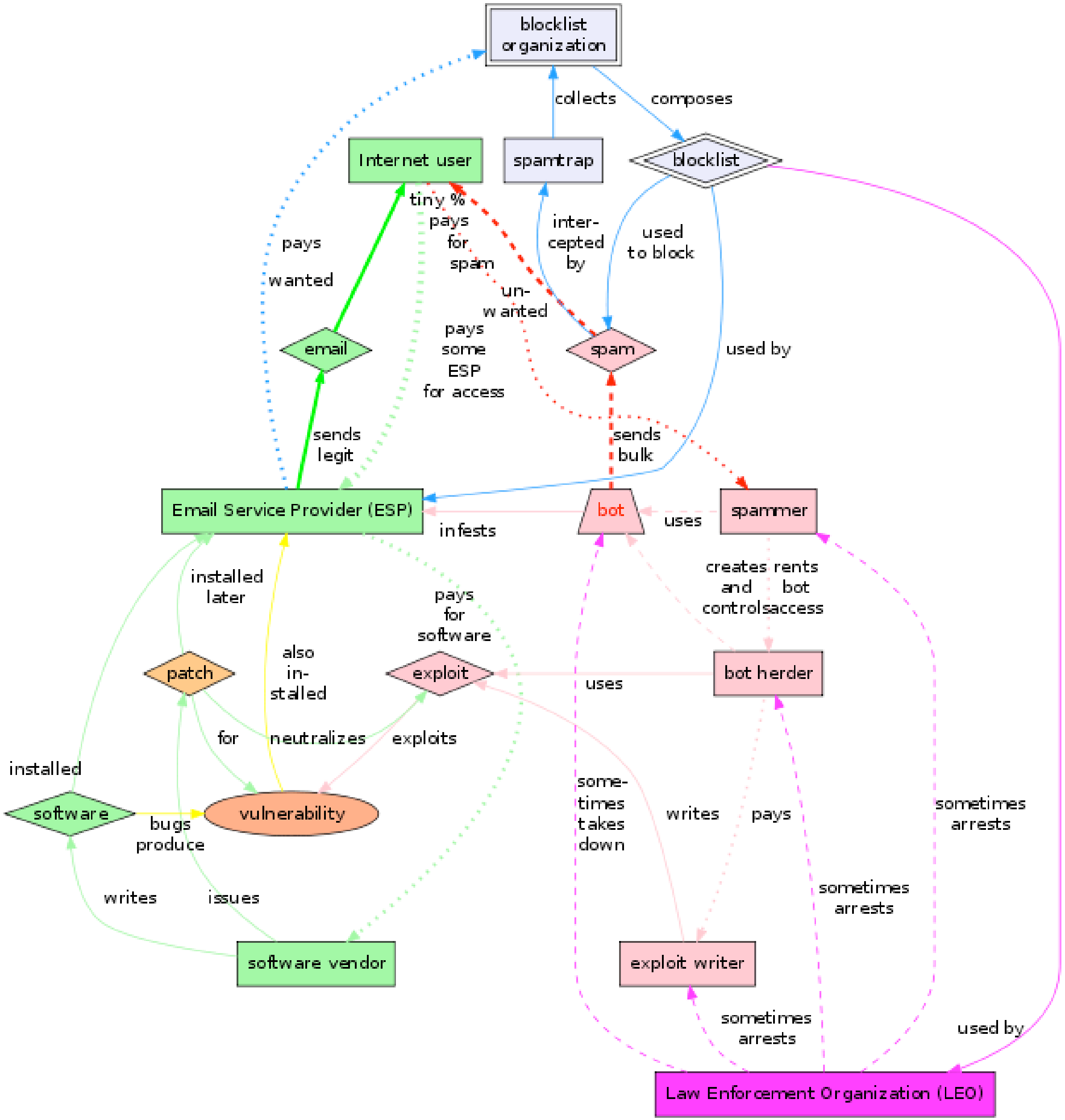


Figure 4: Blocklists (http://cism.mccombs.utexas.edu/iiar-project antispam@quarterman.com)

Existing organizational Layers

The Law

Blocklists and the Law

- Blocklists list; ESPs block
- Expensive to transmit and block spam
- Spam erodes trust in email that banks, businesses, etc., need
- 90% of email remains spam (ENISA 2009 Spam Survey)
- It's a standoff

- Law enforcement sometimes arrests spam gangs or takes down botnets
- Multiple jurisdictions and procedures make slow
- Funding is low
- There's always another botnet

Confusopoly

Ask any ESP:

Which organizations

send the most spam?

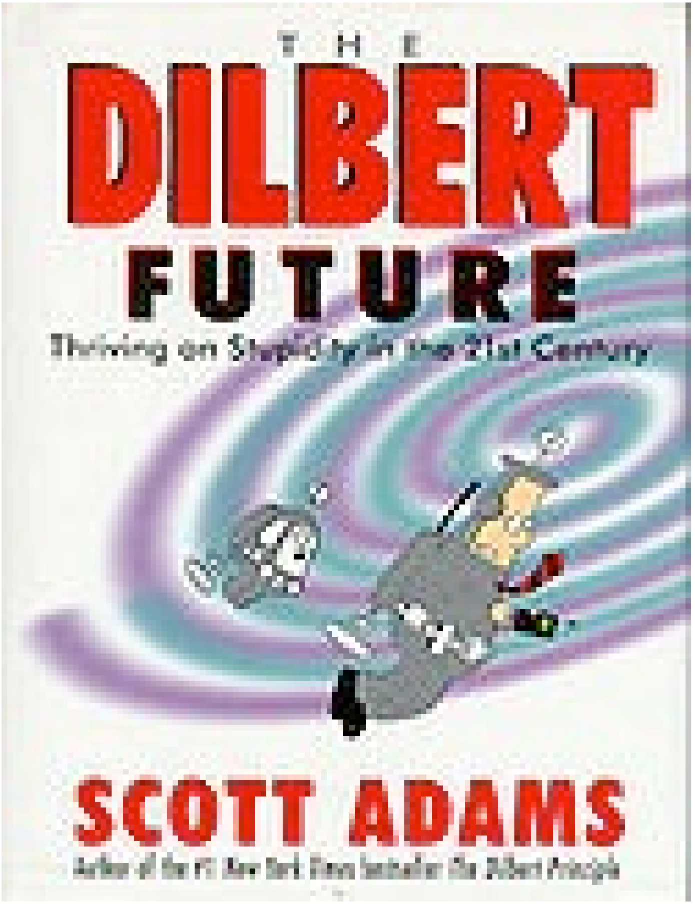
They don't know.

ESPs don't mean to,

and don't want to admit it.

This is a confusopoly:

Buyers can't distinguish.



Which orgs send the most spam?

Volume	ASN	CC	Description
270597276	9829	IN	BSNL-NIB National Internet Backbone
165718151	24560	IN	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd. Telemed
147963786	7738	BR	Telecomunicacoes da Bahia S.A.
142822134	7643	VN	VNPT-AS-VN Vietnam Posts and Telecommunications (
130337496	6849	UA	UKRTELNET JSC UKRTELECOM
110489232	27699	BR	TELECOMUNICACOES DE SAO PAULO SA - TELESP
103761533	9050	RO	RTD ROMTELECOM S.A
89794979	5384	AE	EMIRATES-INTERNET Emirates Internet
88841357	8167	BR	TELESC - Telecomunicacoes de Santa Catarina SA
84639370	25019	SA	SAUDINETSTC-AS Autonomus System Number for Sau

Worldwide, 8 Sep 2010 – 7 Oct 2010

Volume (message counts)/ASN: IIAR project from custom CBL blocklist data

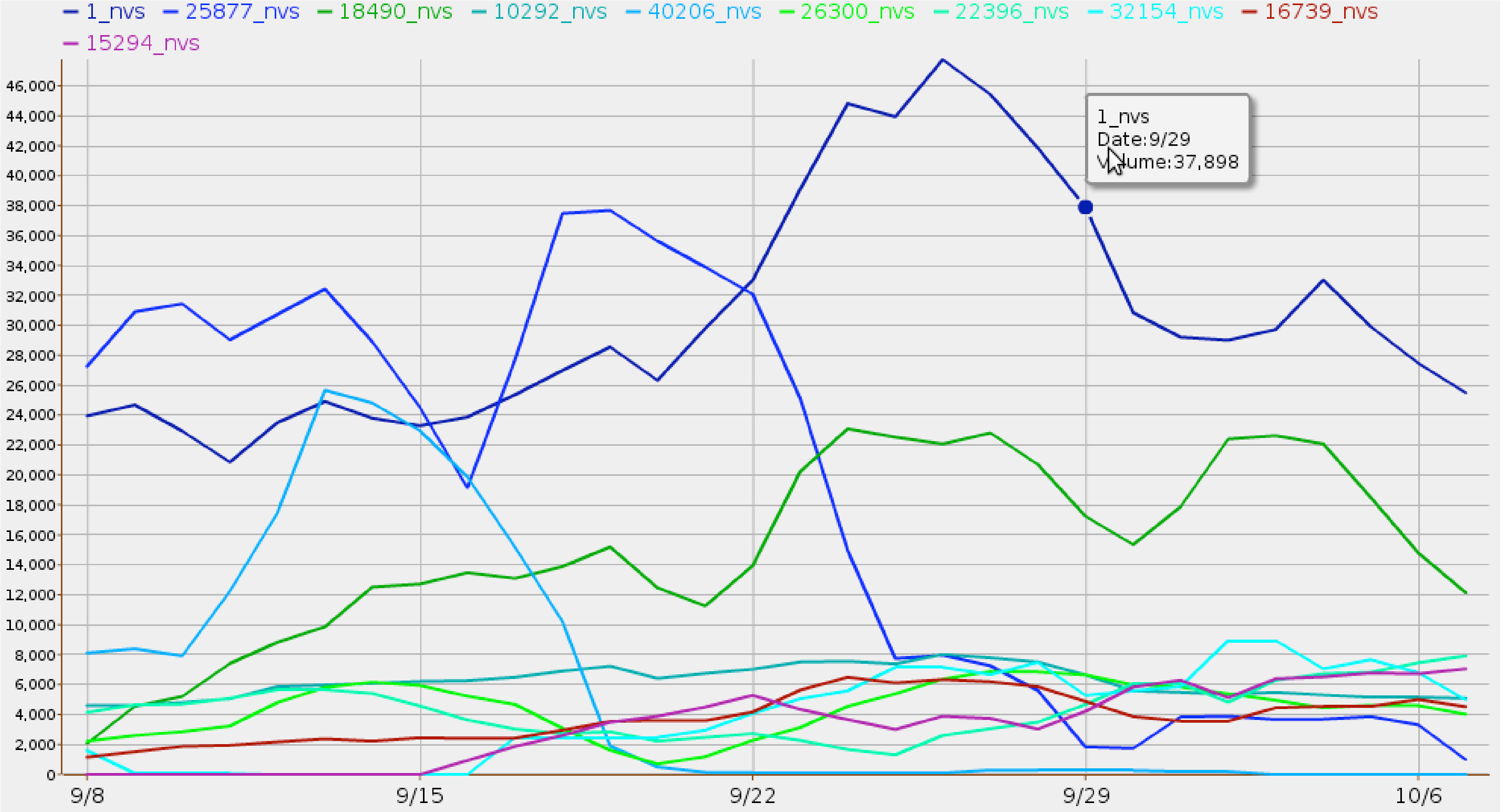
What about in North America?

Easier to guess:
Includes AT&T, Comcast, QWEST, Road Runner (Time Warner), and Verizon.

But in what order?
How often does it change?

Top 10 Spammiest, ARIN

(8 Sep – 7 Oct 2010; by IIAR from CBL data)



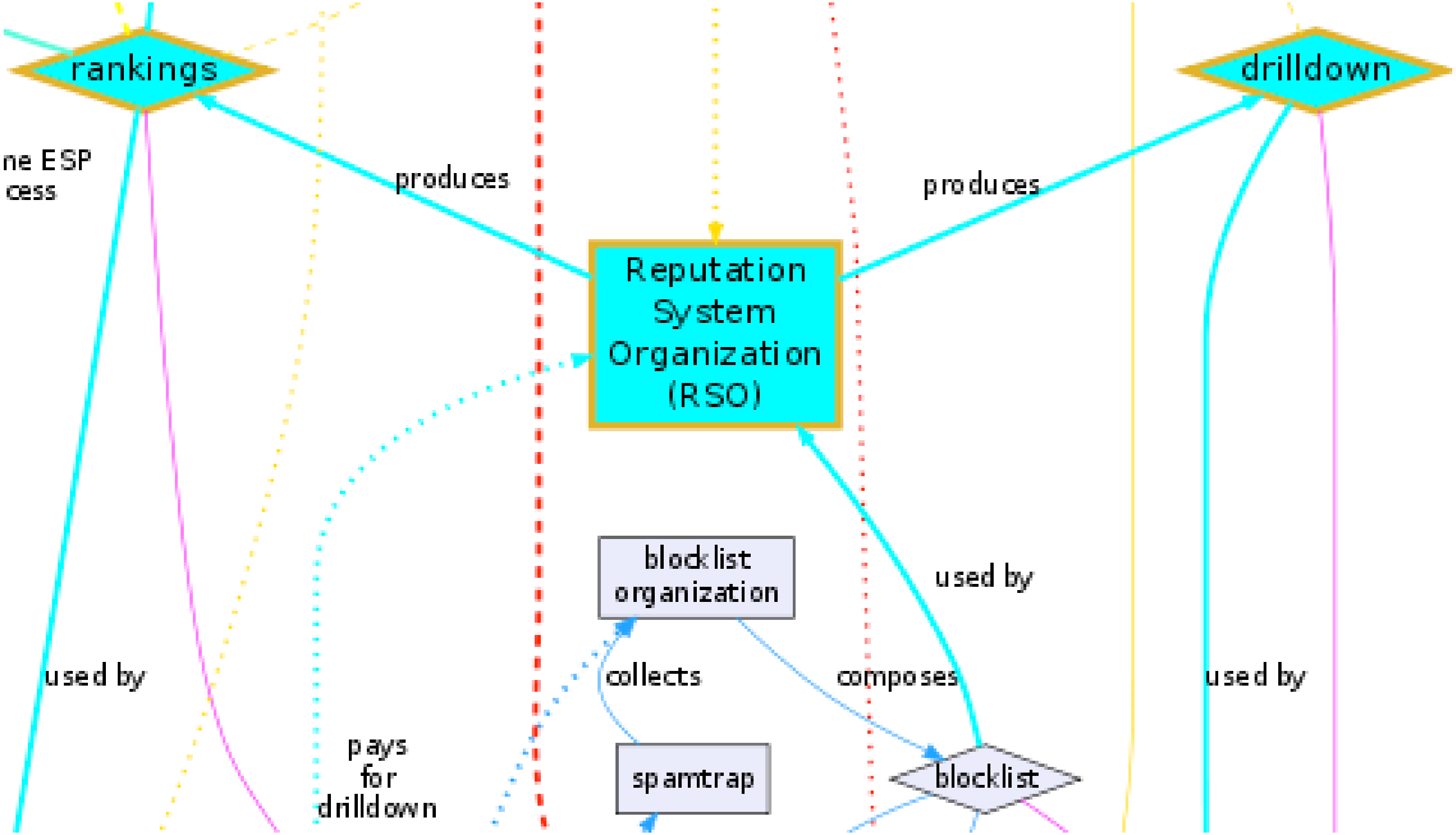
What if everybody knew?

Customers would avoid spam havens
And flock to clean ESPs.

Could turn IT security cost centers
Into profit centers
That attract and retain customers

Spammy ESPs might clean up their act
By implementing known security measures
And blocking *outbound* spam.

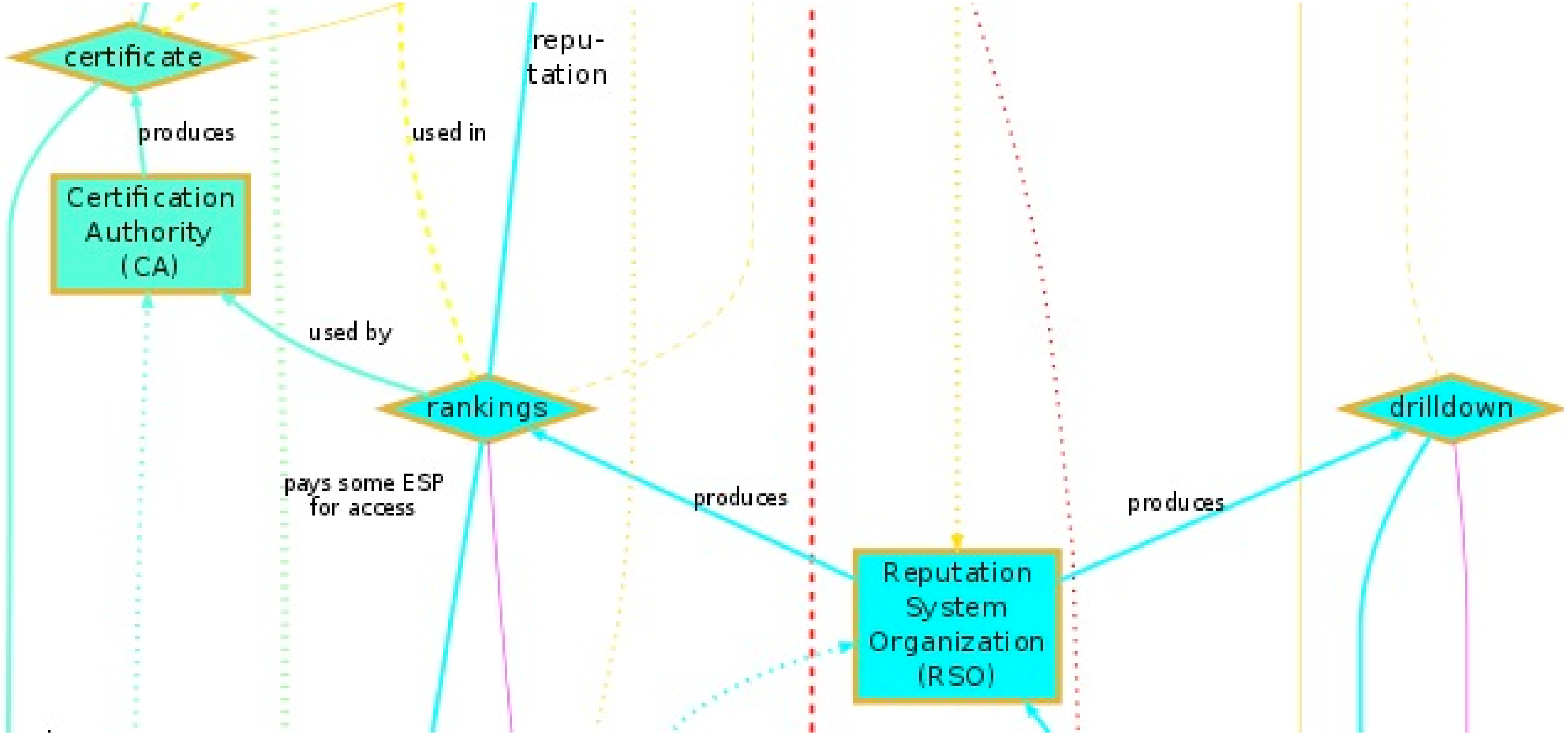
Rankings and Reputation



Reputation System Requirements

- Comprehensive: whole world, every ESP
- Frequent: daily, plus longer periods
- Accurate: as possible
- Transparent: clear and reproducible methodology
- Dimensionality: multiple rankings to compare similar organizations and similar aspects

Certification for ESPs



Transparency

Rankings: FT business school rankings,
US News college rankings,
Kelley Blue Book for cars

Certification: Moody's bond ratings,
Underwriters Laboratory

Reputation systems endogenize economic externalities
by making comparisons transparent,
Providing economic incentive to do better.

“Sellers could use an accumulated positive reputation
to receive economic advantages in different settings.”
(Ba 2002)

Proposed Reputation System

Mine spam blocklist data for rankings and
certification as a Reputation system (RS)
for **market signals** about ESPs and security:
Economic incentive for more effective infosec.

A mechanism to **turn the economic externalities**
Of spam and botnets **into internal incentives**.
(Or for national telecoms, policy incentives.)
Helping users, banks, ISPs, LEOs, etc.
cooperate for a more secure Internet.

Beyond Loss Reduction to Profit

From the ENISA 2009 spam survey:
“When asked if spam prevention is a factor in the customers' choice of provider, over half said yes, while less than a third said no.”

“...suggesting that generally all providers consider it necessary to have effective anti-spam measures for the sake of attracting and retaining customers.”

Reputation for Shareholder Value

PriceWaterhouseCoopers & Economist IU, “Uncertainty Tamed?” 2007:

“28% of financial services bosses felt that reputational risk was a significant threat and 13% felt that it was one of the biggest threats they face.”

“50% of survey respondents also look to risk management to contribute to improved shareholder value.”

No more Cheap Talk

Cheap talk: providers say they're doing effective security, but how do customers know?

No more checklists, either:
Actual measurements of security effectiveness:
Comparative analytics across organizations.

Use reputation and certification to
Turn cheap talk into effective communication.

Elinor Ostrom

Nobel Prize, Economics, 2009:

"for her analysis of economic governance, especially the commons"

Pure government solutions require perfect understanding and monitoring.

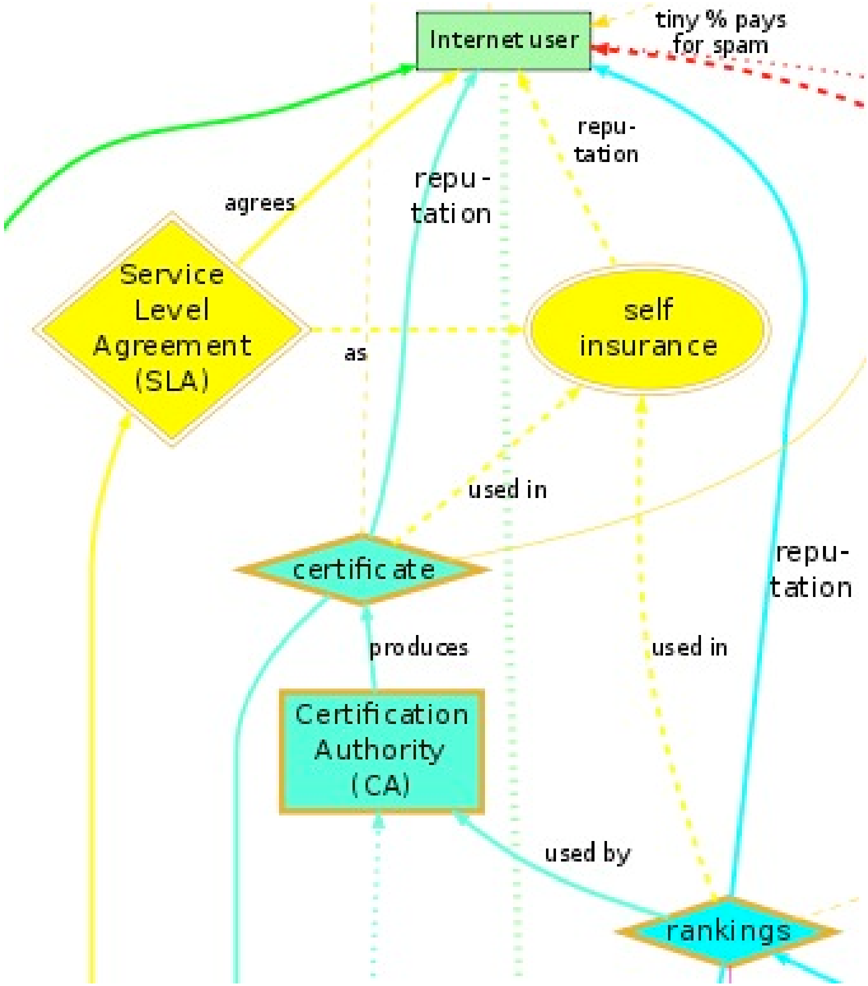
Pure private solutions require a transparent market or end up in monopoly.

Effective Commons Management

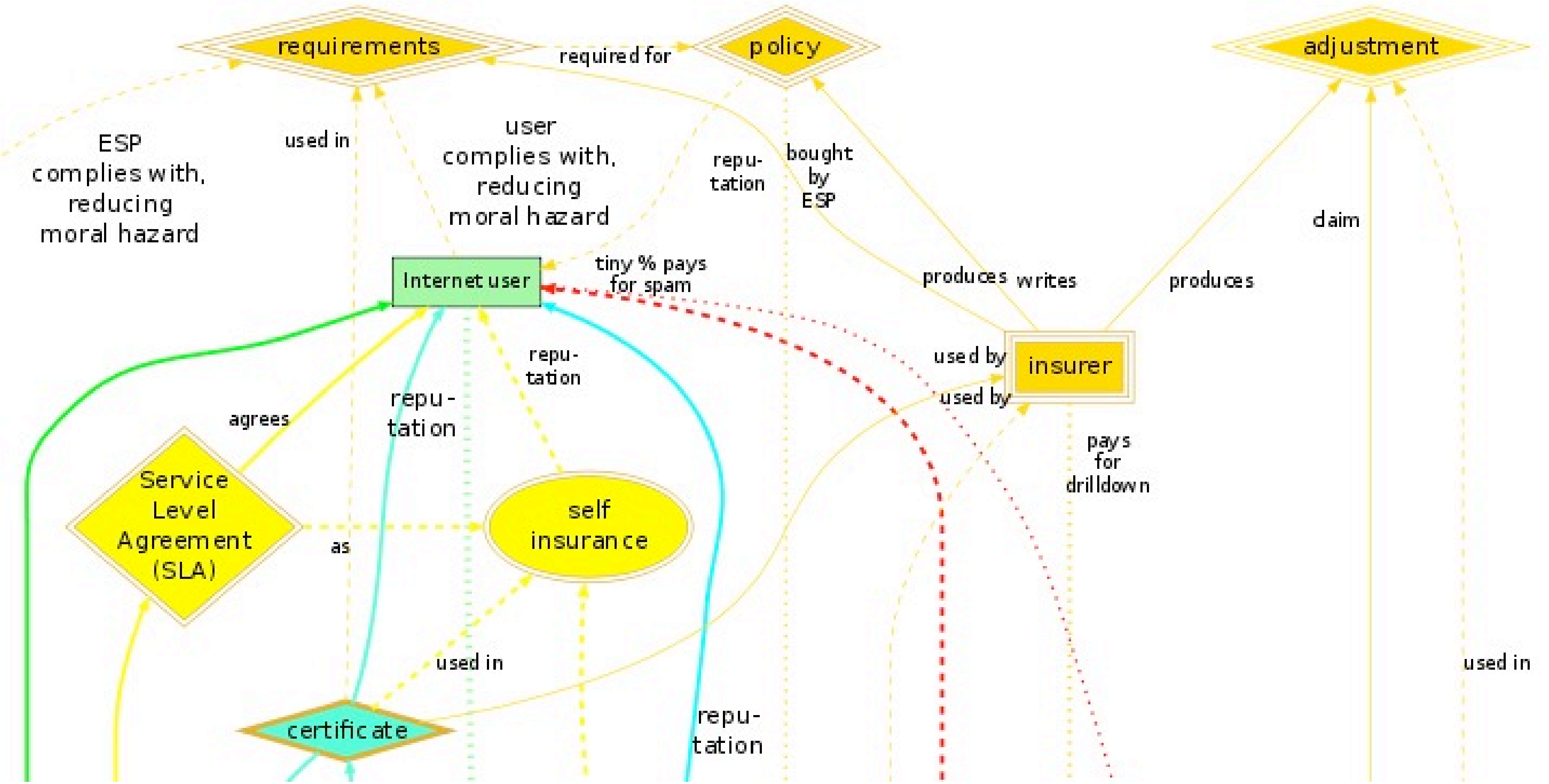
Ostrom examines many historical and current successful commons. All are hybrids, with much participation by those most affected. "Management by the users themselves," Axelrod, 2010.

They typically require all participants to know what others are doing:
That's a reputation system.

SLAs as Self-Insurance



Insurance and Moral Hazard

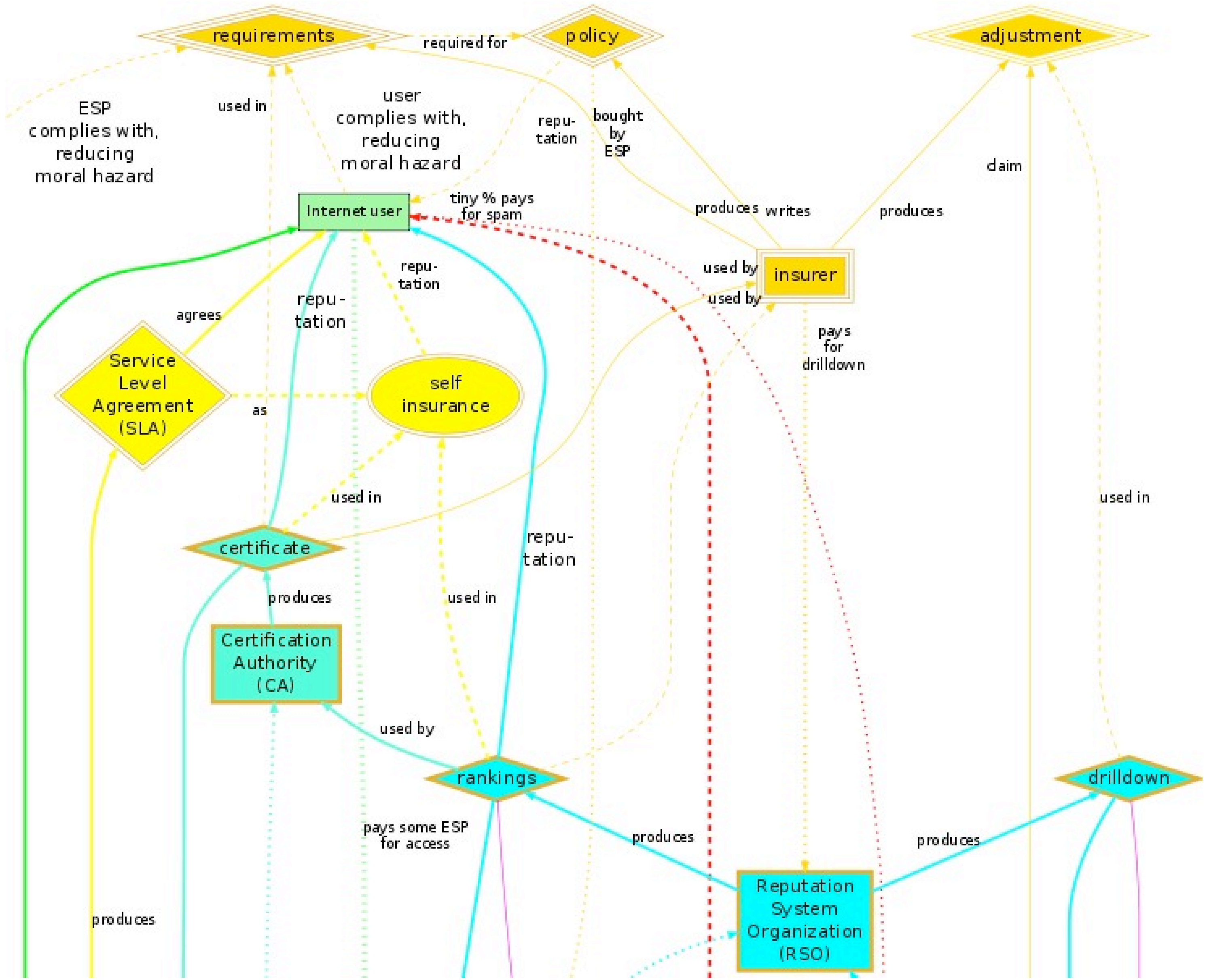


Audit and Insurance

Providers could use rankings or certification
in service level agreements (SLAs),
thus in effect self-insuring with external audit.

Insurers could use rankings or certification
in customer evaluation before writing policies
and in claims adjustment,
thus reducing moral hazard.

New Org. Levels



Three New Levels

- Insurance with requirements for moral hazard
- Self-Insurance from SLAs plus certificates
- Reputation:
  - Certificates
  - Rankings

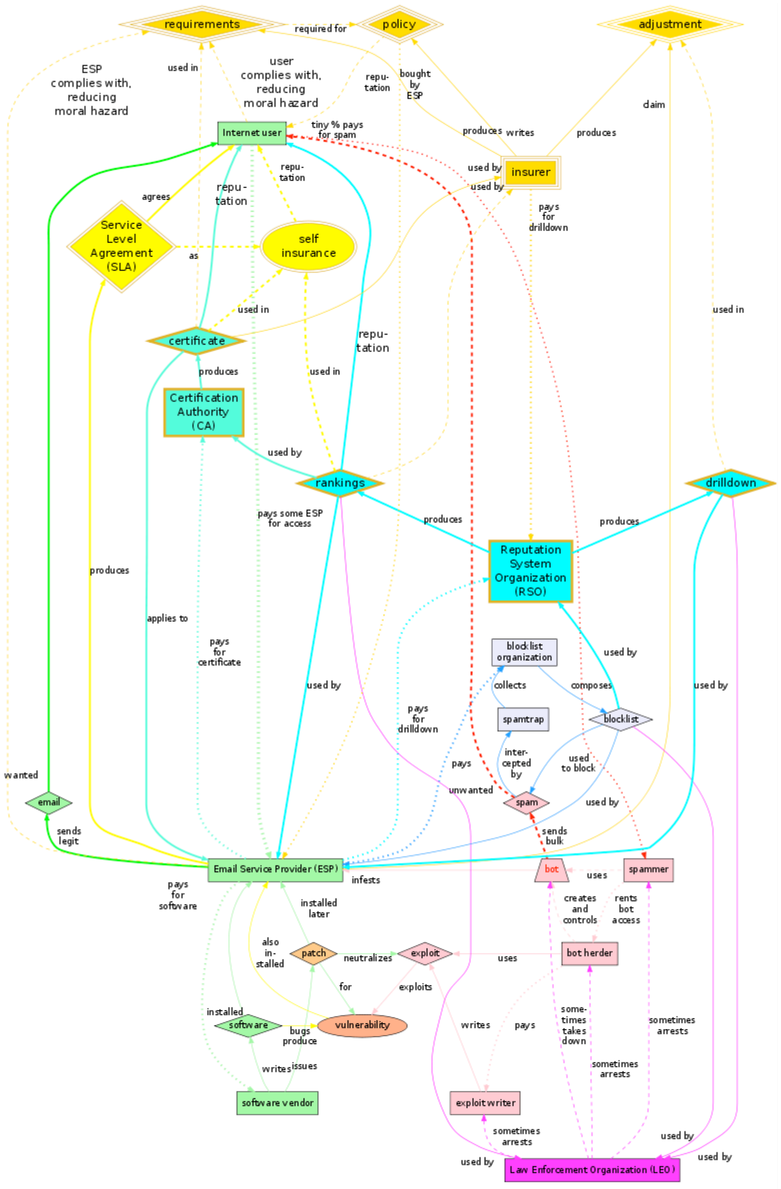


Figure 10: Incentives through New Organizational Layers
http://cism.mccombs.utexas.edu/iiar-project antispam@quarterman.com

Social Comparison Theory

Leon Festinger, 1954:

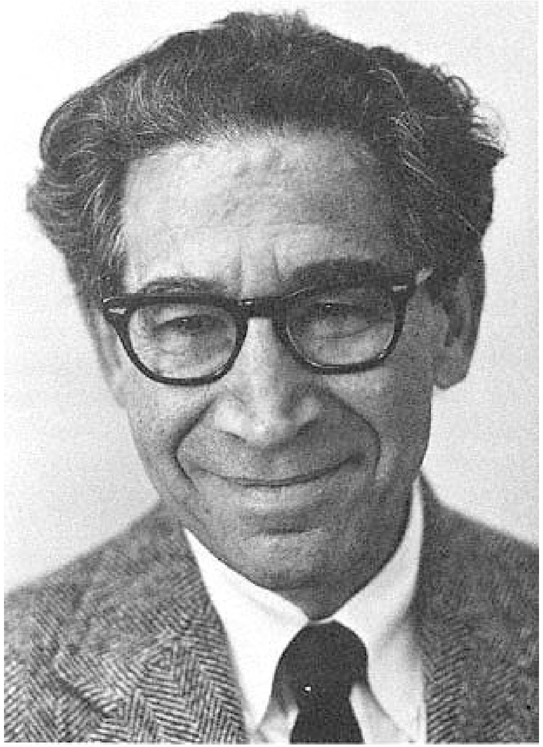
People care how they are doing when compared to similar people, and act on it.

This works online

(Ba 2002, Chen 2010),

and with organizations

(Frei 2010).



Rankings by Org Type

Each type of organization
can be ranked with its peers.

Hosting centers, colos, banks, medical, etc.
Fortune 500: data available to normalize
by customers, by employees, by market cap....

Reputation: improving the security of the Internet
one sector at a time.

Experiments: Effects of Reputation on Organizations

- How does the reputation system change Internet security?
  - Can't use placebo rankings for control groups
- Fortunately, rolling out multiple rankings takes time
  - For example, pick two countries of similar size, such as Belgium and the Netherlands
  - Make rankings for one country public first, see if they change in ways the other doesn't

Example: Belgium October 2010

	Volume	ASN	CC	Description
1	5621169	5432	BE	BELGACOM-SKYNET-AS Belgacom regional ASN
2	2337280	41451	BE	TELEDIS-AS TELEDIS AS
3	1357564	12392	BE	ASBRUTELE AS Object for Brutele SC
4	1204960	3304	BE	SCARLET Scarlet Belgium
5	947642	6848	BE	TELENET-AS Telenet Operaties N.V.
6	517562	12493	BE	AS12493 be.mobistar
7	474940	21491	BE	UGANDA-TELECOM Uganda Telecom
8	387094	29587	BE	SCHEDOM-AS schedom-europe.net
9	325056	48315	BE	ALPHANETORKS-AS Alpha Networks S.P.R.L.
10	304500	25395	BE	Gateway Communications

Questions: Belgium October 2010

- Do these go in BE?
  - Uganda Telecom (AS 21491)
  - Gateway Communications (AS 25395
- RIPE or AfriNIC?

- Which matters most?
  - History?
  - Topology?
  - HQ location?
  - Other?
- Organizational participation in experiments

Other kinds of experiments

- Orgs suggest new ranking types; already have suggestion to normalize by ASN size
- Org changes infosec, watches rankings for changes
- RSO provides drilldowns to interested orgs, giving clues as to why they rank as they do
- Pricing correlations with rankings or certificate changes (long-term experiment)

Acknowledgments and Contact

Thanks to CBL, PSBL ,UTCS, GPE, and Quarterman Creations for volume data. Thanks to CBL, PSBL, Spamhaus, UBL, and UCE for blocklist host data. Thanks to Team Cymru for mappings of different data types. Thanks to Mirjam Kühne and RIPE Labs for posting related articles with more detail.
This material is based upon work supported by the National Science Foundation under Grant No. 0831338.
Any opinions, findings, and conclusions or recommendatioons expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Contact: antispam@quarterman.com
iiar@utlists.utexas.edu