Economic Incentives for Internet Security through Reputation and Insurance

John S. Quarterman, Andrew B. Whinston
antispam@quarterman.com, abw@uts.cc.utexas.edu

a position paper
for the first APWG and IEEE-SA Roadmapping Session
Toward a Global Public Health Initiative Model for eCrime Response

The black hats have their black market that pays them to spam, phish, and DDoS. The white hats are just a cost center to business: they need economic incentives to win.

Technical Internet security measures, procedures, and policies to date have not provided those incentives. The Internet has already spawned at least two organizational layers that start to deal with this problem (in Figure 1, blocklist organizations, middle right, and LEOs, bottom):

- Spam blocklists, increasingly sophisticated in listing spamming addresses, yet fundamentally reactive, dealing with symptoms, not causes.
- Law enforcement, both anti-spam laws and increasing LEO coordination, but funding is low and the law is slow; takedowns are temporary, partial, or replaced by other botnets.

Meanwhile, botnets continue to infest every kind of organization on the Internet that sends electronic mail. Spam: it's not just for ISPs anymore, any organization can be an electronic mail service provider (ESP) and any ESP can inadvertently send spam.

Ask any ESP: which organization sends the most spam? They don't know. And it's not who you might think:

Volume	ASN	CC	Description
270597276	9829	IN	BSNL-NIB National Internet Backbone
165718151	24560	IN	AIRTELBROADBAND-AS-AP Bharti Airtel Ltd. Telemedia Services
147963786	7738	BR	Telecomunicacoes da Bahia S.A.
142822134	7643	VN	VNPT-AS-VN Vietnam Posts and Telecommunications (VNPT)
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 SaudiNet

That's worldwide (8 Sep 2010 – 7 Oct 2010). In North America, the names are much more familiar, including AT&T, Comcast, QWEST, Road Runner (Time Warner), and Verizon. But in what order?

What if everybody knew? Then customers would avoid known spam havens and flock to clean ESPs. That could turn IT security cost centers into profit centers that attract and retain customers.

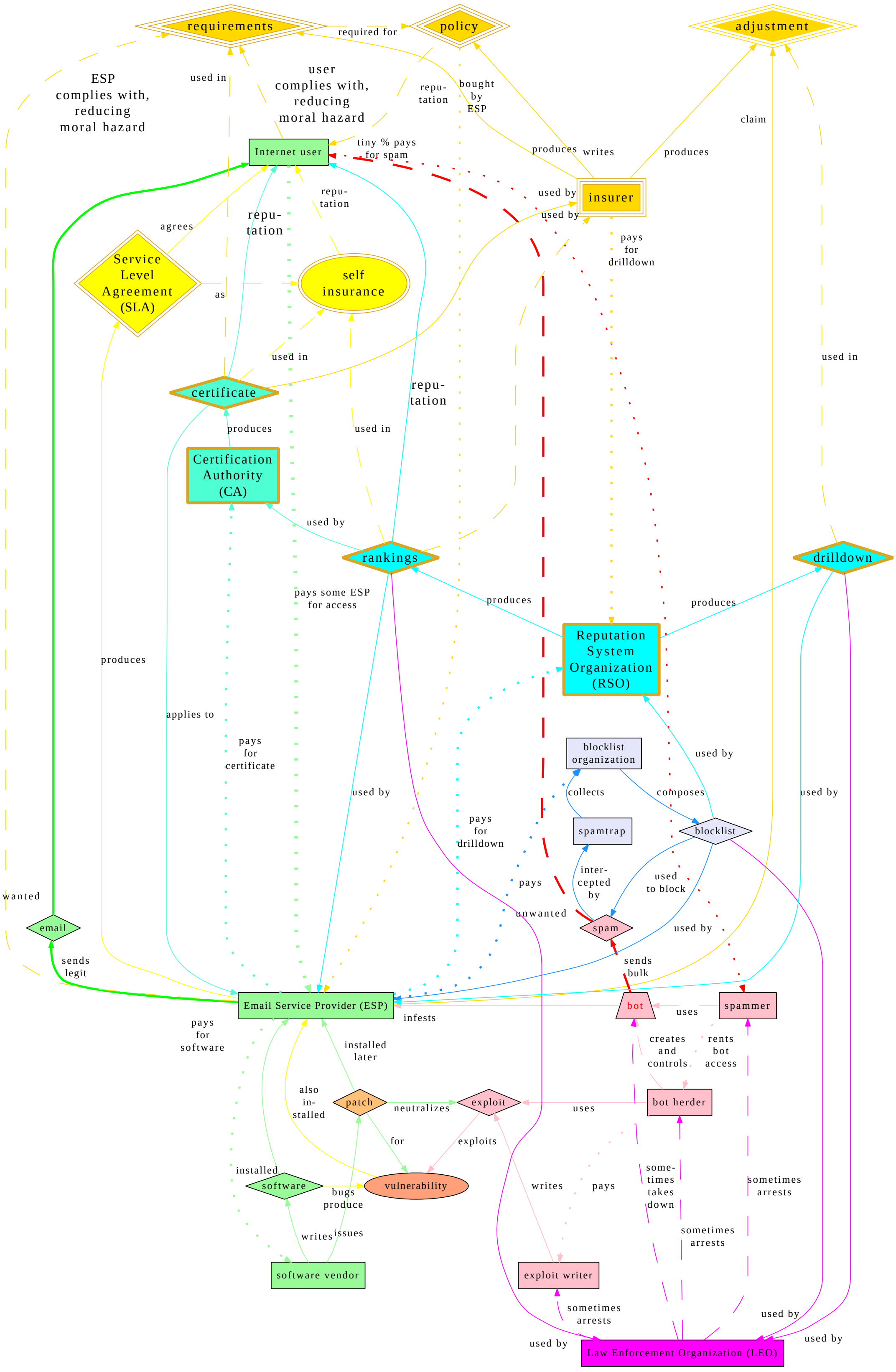


Figure 1: Incentives through New Organizational Layers
http://cism.mccombs.utexas.edu/iiar-project antispam@quarterman.com

New Organizational Layers

Mining blocklists can provide the data to let everybody know, by enabling three new Internet organizational layers (see Figure 1) that add economic incentives (profit and reputation) to endogenize the externality of outbound spam by motivating participants to control attacks at their origin, without interfering with decentralized protocols, producing some measure of security predictability for users, by promoting dynamic security assessment, investment, and implementation, Quarterman et al. (2010).

1. (cyan with bold outlines, middle of figure): A Reputation System Organization (RSO) publishes rankings of ESPs by amount of outbound spam, endogenizing that externality by adding visibility to make it part of ESPs' organizational reputation, just as business schools care whether they are in the top 10 in the Financial Times (FT) rankings, which are highly visible, come under frequent criticism, presumably improve due to such criticism, and are thus authoritative. *Nobody wants to be branded a spam or botnet haven!* An ESP can improve its rankings by better IT security deployment, sometimes paying for RSO drilldown for infosec effectiveness. *Organizations that do good work want to be recognized,* and can attract and retain customers with good rankings. Rankings provide a common language for organizations ranked and transparency for customer choice, turning IT security costs into a potential source of profit. LEOs may also use rankings and drilldown to spot culprits.

   A Certification Authority (CA) distills multiple RSO rankings over time to certify an ESP in a certain category. An ESP buys a certificate and uses it in marketing, just like a bond rating, or like a Good Housekeeping or Underwriting Laboratories seal of approval for successful spam prevention. ESPs already advertise certificates for specific security technologies. This CA certificate will go beyond that, to *success* of security technologies and procedures. The RSO and the CA thus enable a reputation system.

2. (yellow with double outlines): Service Level Agreements (SLAs) say an ESP will provide service to its users within certain thresholds or pay penalties. *An ESP can use rankings and certificates as external validation to turn an SLA into self-insurance to sell to its customers.* A non-customer may want to sign up with an ESP that provides self-insurance SLAs, which thus enhance the ESP's reputation.

3. (gold with triple outlines): Traditional insurers can use rankings in writing and pricing insurance policies for ESPs, or they may buy self-insurance SLAs from ESPs as a form of reinsurance. *To reduce moral hazard, an insurer may impose requirements on ESPs and their users.* Just as a fire insurance policy often requires a sprinkler system, a cyber-insurance policy may require a certificate from the CA. When an ESP files an insurance claim, the insurer may pay for an RSO drilldown to find out how well the ESP has really been doing. This insurance process will enhance an ESP's reputation.

These three new levels of organization provide economic incentives via reputation and direct economic payments and penalties for ESPs (and users and security firms and software vendors) to coordinate and improve anti-spam (and anti-botnet) efforts, thus mobilizing the white hats to beat the illicit black hat economy, Quarterman (2010).

Commons Theory

These layers can bring quantification and experimental rigor to a commons model of the Internet, providing the missing Internet key to Elinor Ostrom's Nobel-prize-winning work, Ostrom (1990): transparency of the effects of IT security per organization.

Traditional government, being slow and geographically organized, cannot handle the fast and worldwide spam and botnet problem. Private parties alone have clearly failed to do so. What is needed is the kind of multi-level multi-organizational loose cooperation that studies of governance of many types of commons indicate works, Dietz et al. (2003). The key feature is ″management by the users themselves," Axelrod (2010).

> The reliability and security of the Internet, however, is a public good that cannot be ignored. The security of the Internet is a public good because availability to one user does not diminish its availability to another user.
> ...in large and complex systems, there should be multiple layers of nested enterprises (p. 101 f). In the case of the Internet, individual users operate at a low level, while organizations and user communities operate at a middle level.

Transparency can enable "rewards for those with a good reputation in the public goods game," Milinski et al. (2002). Neither the RSO nor the CA is a governing body; neither tells anyone what to do, and neither has any enforcement power. Rather, each provides information and incentive for the stakeholders to organize themselves to collectively manage the Internet commons, Dietz et al. (2003).

Social Comparison Theory

Currently ESPs have no direct incentive to control for spam that may originate from their network and impact others, and their investments are usually prompted by the incentive to provide better service for their own customers, or sometimes not even that: "Businesses put their profits above defending their customers and business partners," Herzog (2010). Internet security professionals are starting to recognize that security metrics are required to replace fear, uncertainty, and doubt in the Internet, Jaquith (2007), but to date while metrics have been deployed extensively within organizations, Seiersen (2010),

Fifty years of social science research and literature indicates making behavior public changes that behavior, Festinger (1954). People actually do care how well they are doing compared to similar people, and if they are given a way to accurately make such comparisons, they tend to act on them.

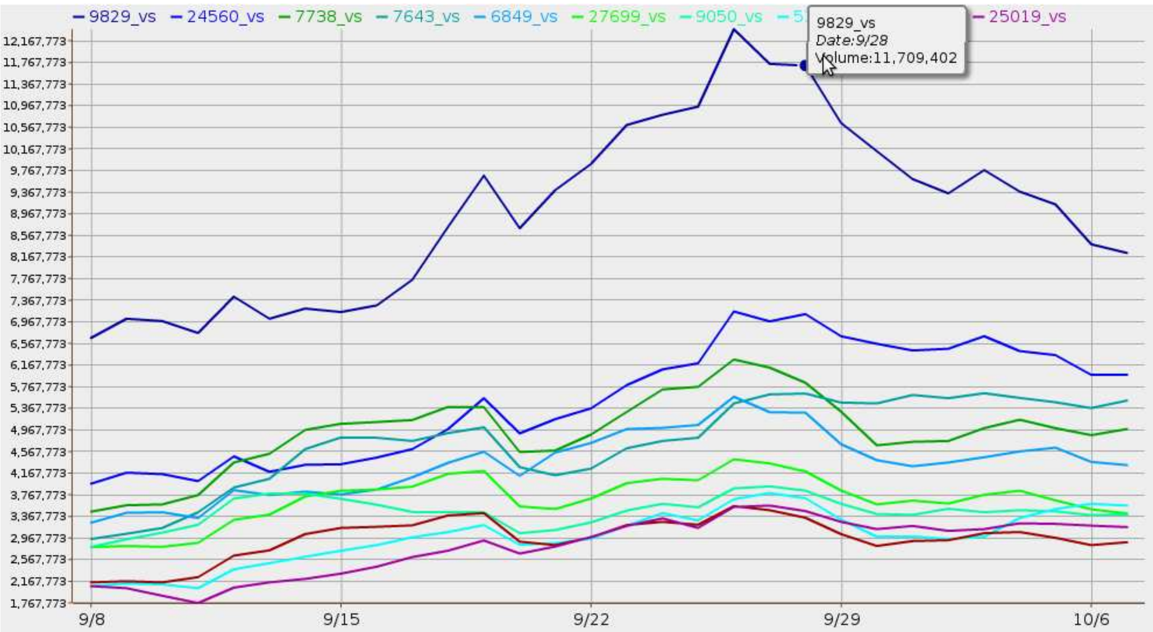
In examining Internet movie ratings, letting everybody know how others rated movies changes behavior positively, Chen et al. (2010):

> When given outcome information about the average users net benefit score, above-average users mainly engage in activities that help others. Our findings suggest that effective personalized social information can increase the level of public goods provision.

Applying the same kind of transparency to Internet organizations should affect organizational behavior similarly.

For example, Secunia examines the security of computers, software, and software vendors, including such metrics as how many patches are not installed, Frei (2010). The most insecure programs and vendors are not who you might think. Not Microsoft: actually some well-known third party software wins that honor. Microsoft has already reacted to its bad reputation by implementing an automatic update system that is widely used. The author when presenting that paper mentioned another example of a software vendor (open source in this case) that had come out poorly in these rankings before, and then (apparently because of that poor showing) implemented a better automatic update system and greatly improved its ranking.

Since blocklist data is derived from messages already emanating from organizations, it applies to all organizations on the Internet without requiring permission first. Frequent, fine-grained, regular, ongoing, global data fusion of blocklist and other data can enable temporal or longitudinal statistical studies to determine how organizations become clean or unclean over time, Collins et al. (2007).



Such a reputation system, and the certificates, SLA self-insurance, and insurance policies that can be built out of it, should provide transparency and economic incentives to help all Internet stakeholders, from banks to ISPs to LEOs to users, cooperate to implement a much more secure Internet.

Acknowlegments

This material is based upon work supported by the National Science Foundation under Grant No. 0831338.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

We also gratefully acknowledge custom data from CBL, PSBL, Fletcher Mattox and the University of Texas Computer Science Department, Quarterman Creations, and especially Team Cymru. None of them are responsible for anything we do, either.

References

Axelrod, R., 2010: Governing the cyber commons. *Review Symposium: Beyond the Tragedy of the Commons*, http://www-personal.umich.edu/~axe/.

Chen, Y., F. M. Harper, J. Konstan, and S. X. Li, 2010: Social comparisons and contributions to online communities: A field experiment on movielens. *American Economic Review*, **(100)**, 1358–1398, http://www.aeaweb.org/articles.php?doi=10.1257/aer.100.4.1358.

Collins, M. P., T. J. Shimeall, S. Faber, J. Janies, R. Weaver, M. De Shon, and J. Kadane, 2007: Using uncleanliness to predict future botnet addresses. In *IMC '07: Proceedings of the 7th ACM SIGCOMM conference on Internet measurement*, ACM, New York, NY, USA, ISBN 978-1-59593-908-1, pp. 93–104.

Dietz, T., E. Ostrom, and P. C. Stern, 2003: The struggle to govern the commons. *Science*, **302(1907)**.

Festinger, L., 1954: A theory of social comparison processes. *Human Relations*, **(7)**, 117–140, http://www.soc.ucsb.edu/faculty/friedkin/Syllabi/Soc147/ATheoryofSocialComparisonProcesses.pdf.

Frei, S., 2010: The security of end-user pcs an empirical analysis. In *DDCSW: Collaborative Data-Driven Security for High Performance Networks*, Internet2 and WUSTL, http://security.internet2.edu/ddcsw2/docs/sfrei.pdf.

Herzog, P., 2010: Better security through sacrificing maidens. *infosecisland*, http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-survey.

Jaquith, A., 2007: *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional.

Milinski, . M., D. Semmann, and H.-J. Krambeck, 2002: Reputation helps solve the 'tragedy of the commons'. *Nature*, **415(24)**.

Ostrom, E., 1990: *Governing the Commons: The Evolution of Institutions for Collective Action (Political Economy of Institutions and Decisions)*. Cambridge University Press, ISBN 0521405998.

Quarterman, J. S., 2010: Economic incentives for cooperation to fight spam. *RIPE Labs*, http://www.ripelabs.net/Members/jsq/content-cooperation-to-fight-spam.

Quarterman, J. S., S. Sayin, J. Reinikainen, E. V. Kumar, and A. B. Whinston, 2010: Data, reputation, and certification against spam. In *DDCSW: Collaborative Data-Driven Security for High Performance Networks*, Internet2 and WUSTL, http://security.internet2.edu/ddcsw2/docs/Quarterman-darepcert.pdf.

Seiersen, R., 2010: Practical security metrics in the 4th dimension. In *Metricon 5.0*, http://www.securitymetrics.org/content/attach/Metricon5.0/metricon5%20-%20seiersen%20-%20kaiser4d.ppt.