Reengineering cybersecurity: A simulation study

Bongsik Shin
Management Information Systems
San Diego State University
bshin@sdsu.edu

Dan Kim
Information Technology and Decision Sciences
North Texas University
Dan.Kim@unt.edu

ABSTRACT

Stories of grave security breaches in the cyberspace are abound. In the wake of the rampant threats and security breaches, there is a widespread realization that the current incremental and rather reactive countermeasures have only marginal success in battling the criminals and aggressors, and some transformative approaches should be considered to turn the table. As a related effort, the *Bright Internet* vision was proposed in the editorial article of *MIS Quarterly* in order to push fundamental reengineering of current practices in battling cybercrimes (Lee, 2015). Lee (2105) proposed that the *Bright Internet* research be anchored on four principles - *origin responsibility*, *deliverer responsibility*, *traceable anonymity*, and *rule-based digital search warrants* – in order to reverse the current trajectory of massive cybersecurity problems. Realizing the *Bright Internet* vision demands a massive undertaking. As a step forward, this project is going to perform an empirical simulation to understand the effects of *origin responsibility* and *deliverer responsibility* principles in discouraging cybercrimes. More specifically, we will define different hierarchical levels of origin and deliverer responsibilities and examine their influences on disrupting the spam supply chain network.

Keywords: cybersecurity, spam, bright internet, simulation

RESEARCH METHODOLOGY

1. A Research Framework

As an initial work, we developed a high-level framework (see Figure 1) that defines *Bright Internet* solution space based on Lee's (2015) work. It consists of *enforcement* and *responsibility* dimensions and their cross-section reveals areas to be researched in terms of technical and non-technical (e.g., policy) solutions to realize the *Bright Internet* vision.

Enforcement Dimension: This dimension defines solutions intended to: detect current or looming threats and determine their severity; trace threat sources; gauge compliance with defined responsibilities; and enforce responsible behaviors of communication parties. It has three core requirements that form strong and virtuous relationships to achieve the overall 'enforcement' goal.

(a) ***Threat Detection*** represents mechanisms to effectively share threat intelligence and also formally trigger the real/non-real time inspection of suspicious messages in transit or on arrival by the deliverer or receiving nodes.

(b) ***Selective Traceability*** allows 'tracing' of adversaries should the need arises, while protecting the privacy of ordinary users. This is intended to discourage crimes or misbehaviors committed in the shadow of anonymity, while guaranteeing freedom of expressions.

(c) ***Compliance Measurement*** includes metrics/indices that gauge damages inflicted by criminal or abusive activities; indicate how well message origins and deliverers comply with rule/governance and pre-defined responsibilities; and also define punishment mechanisms for cybercrimes.

Responsibility Dimension: This dimension defines responsibilities of message origins and deliverers.

(a) ***Origin responsibility:*** The message source bears responsibility for intentional creation of a harmful message or negligence of its dissemination, and this requires a mechanism of monitoring source behaviors without jeopardizing user privacy.

(b) ***Deliverer responsibility****:* Message deliverers (e.g., ISPs) bear responsibilities even if the delivery of harmful messages is unintended. This is to encourage their fair share of responsible behaviors in spreading incriminating messages.

Dimensional Solution Space: Technology, Policy & Governance		Enforcement Dimension		
		Threat Detection	Selective Traceability	Compliance Measurement
Responsibility Dimension	Origin Responsibility			
	Deliverer Responsibility			

Figure 1. Research Framework

2. Research Procedure: The research will be undertaken according to the following procedure:

(a) Delineation of spam-based threat model
The simulation focuses on understanding the possible effects of the added sender and deliverer responsibilities on disrupting the complex spam value chain. According to Levchenko et al (2011), the spam value chain consists of three distinct stages of advertising (i.e., spam vector such as email), click support (i.e., redirection sites, domains, name servers, web servers, stores, and affiliate programs), and realization (i.e., payment services, and fulfillment). Our simulation model is grounded on the international spam network.

(b) Design origin and deliverer responsibilities
Origin and deliverer responsibilities, and their enforcement measures will be designed. The origin responsibilities will be defined at the individual, server, company and country levels in both practical and philosophical relationships. As for the deliverer responsibilities, victimized computers, ISPs, and their countries are considered as deliverers of ill-intended messages (e.g., spam) as aggressors generally launch detoured attacks through victims or through 'dark network' channels difficult to trace. The design of responsibility will factor in different practical and technical issues including: message source identification based on the victim's report; reporting mechanism of threat information; deep packet inspection; origin's confirmation protocol of victim's report; blacklist management; and prevention of the message source from spoofing or impersonation. Also, the different levels of responsibilities may be devised through the lens of the three 'enforcement' dimensions.

(c) Model the general architecture of the simulation environment
The network topology for simulation will be modeled at the autonomous system (AS) level in which each AS includes at least one entity of the spam supply chain network. To reflect the global-scale of the spam network and better reflect the role of ISP responsibilities, it is assumed that none of the autonomous systems are served by the same ISP. Reflecting the fact that the botnet is the biggest source of spam these days, the simulation assumes that bots are the production source of spam emails in each AS.

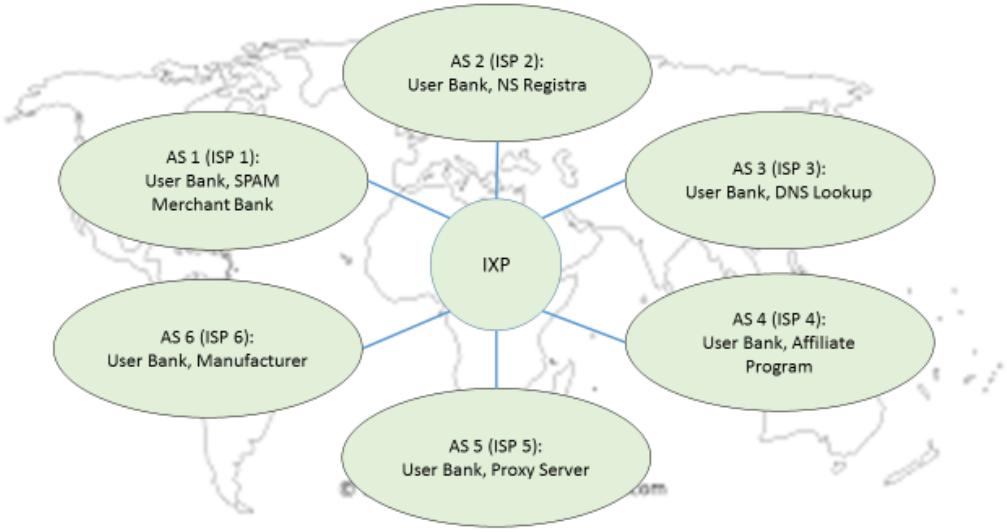

Figure 1. SPAM supply chain and high-level simulation model

(d) Conduct empirical simulation and data analysis

Simulations will be performed using the popular open source software, OMNET++, which allows simulation of complex systems. OMNET++ is supported by a number of software libraries such as INET and ReaSE to facilitate effective simulations.

References

1. Lee, J. K. (2015). Guest Editorial: Research Framework for AIS Grand Vision of the Bright ICT Initiative. *Management Information Systems Quarterly*, *39*(2), iii-xii.

2. Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Félegyházi, M., Grier, C., ... & McCoy, D. (2011, May). Click trajectories: End-to-end analysis of the spam value chain. In *2011 IEEE Symposium on Security and Privacy* (pp. 431-446).