Reengineering cybersecurity: A simulation study

Research in progress

Bongsik Shin

San Diego State University

Research Background

- AIS Grand Vision Project for the ICT-enabled Bright Society
  - Adopted by the AIS Council in Dec. 2014, and established a task force.

- Bright Internet (BI) as a core of Bright ICT (Lee, 2015)
  - Bottom-line: The cyberspace is anarchy.
  - Lets re-engineer the governance of cybersecurity

Research Background

Bright Internet (Lee, 2015)

- Principles
  - Origin responsibility
  - Deliverer responsibility
  - Traceable anonymity
  - Rule-based digital search warrants

Our Research Goal

- Understand the effects of *origin* and *deliverer responsibilities* on cybercrimes.
- Methods
  - (1) Define origin and deliver responsibilities at different levels
  - (2) Perform empirical simulations of compliance (or no compliance)
- Threat model for this project: email spam
- Significance: one of the early theory-building efforts

A Research Framework

- Framing solution space
- Cross-section of enforcement and responsibility dimensions
- Each cell may need a structure (e.g., OSI model) to guide technical & policy solutions

Solution Space Dimension: Technical & Governance Solutions		Enforcement Dimension		
		Threat Detection	Traceable Anonymity	Compliance Measurement
Responsibility Dimension	Origin Responsibility	OSI layer-driven solutions ?		
	Deliverer Responsibility			

Enforcement Dimension

- ***Threat Detection:*** real/non-real time inspection of suspicious messages in transit or on arrival.
- ***Traceable Anonymity:*** *T*racing of adversaries, while protecting the privacy of ordinary users.
- ***Compliance Measurement:***
  - Gauge damages inflicted by criminal or abusive activities
  - Indicate how well message origins and deliverers comply with pre-defined responsibilities
  - Define punitive mechanisms for cybercrimes.

Responsibility Dimension

- ***Origin responsibility:*** The message source bears responsibilities for
  - Intentional creation of a harmful message
  - Negligence of its dissemination
  - Can be at the individual, system, company and country levels

- ***Deliverer responsibility:*** Message deliverers (e.g., ISPs) bear responsibilities
  - Even if the delivery of harmful messages is unintended.
  - Victimized computers, ISPs, and their countries are considered as deliverers of spam

Research Methodology

1. Conceive Origin and Deliverer Responsibilities
2. Delineate Spam-based Threat Model
3. Develop a Simulation Model
4. Conduct Simulations
5. Analyze Data

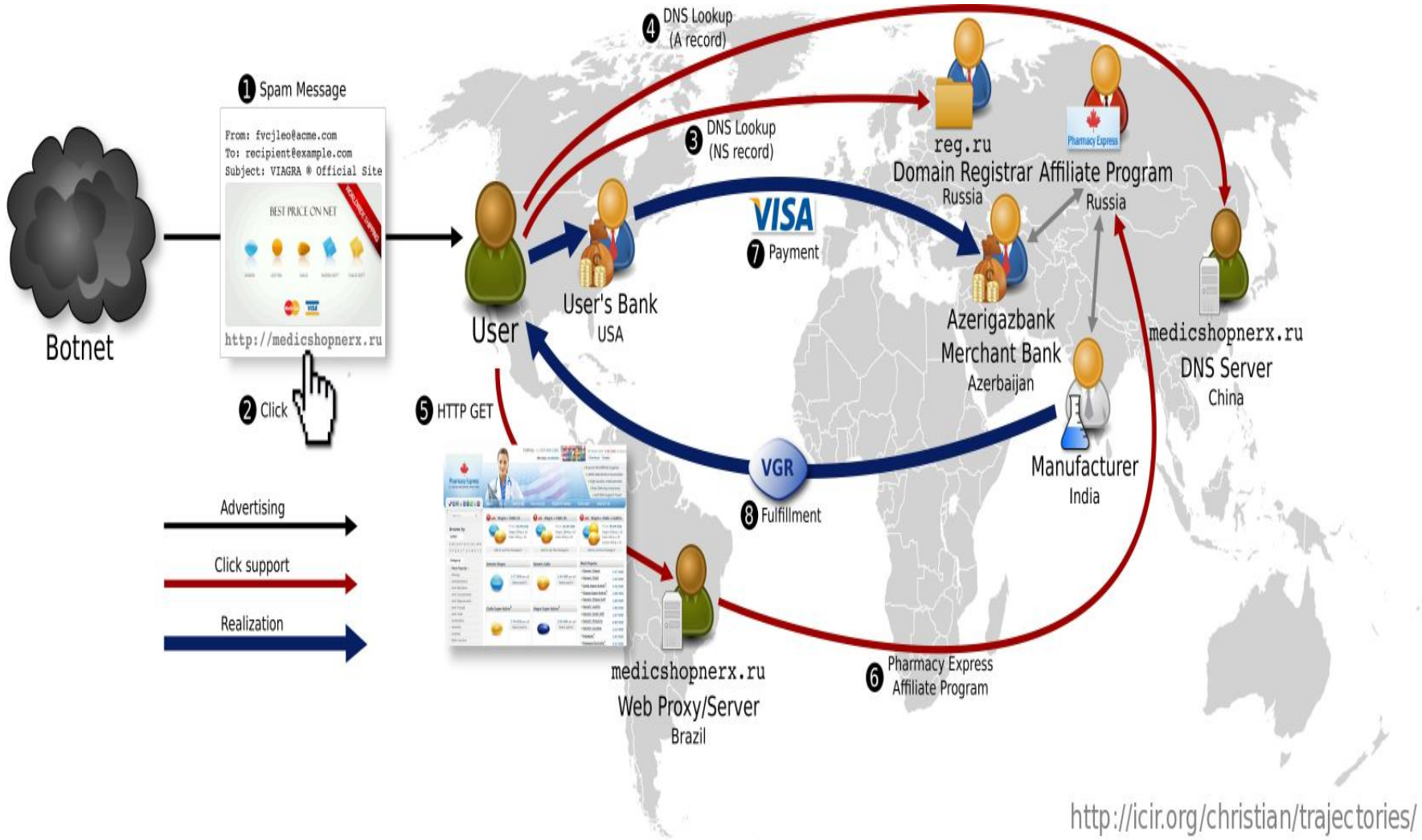
Research Method: Conceive Origin and Deliverer Responsibilities

- Literature survey on the theory of Responsibilities & cybersecurity responsibilities
- Particular role of ISPs
- Through the lens of threat detection, traceable anonymity, and compliance measurement

Research Method: Delineate Spam-based Threat Model

- A spam value chain consists of:
  - Advertising (i.e., the delivery of email spam)
  - Click support (i.e., redirection sites, domains, name servers, web servers, stores, and affiliate programs)
  - Realization (i.e., payment services and fulfillment)
- Products: Illegal pharmaceuticals, replica luxury goods and counterfeit software, Nearly 95% of emails
- Source: Levchenko et al. (2011)

A SPAM Value Chain, Levchenko et al. (2011)

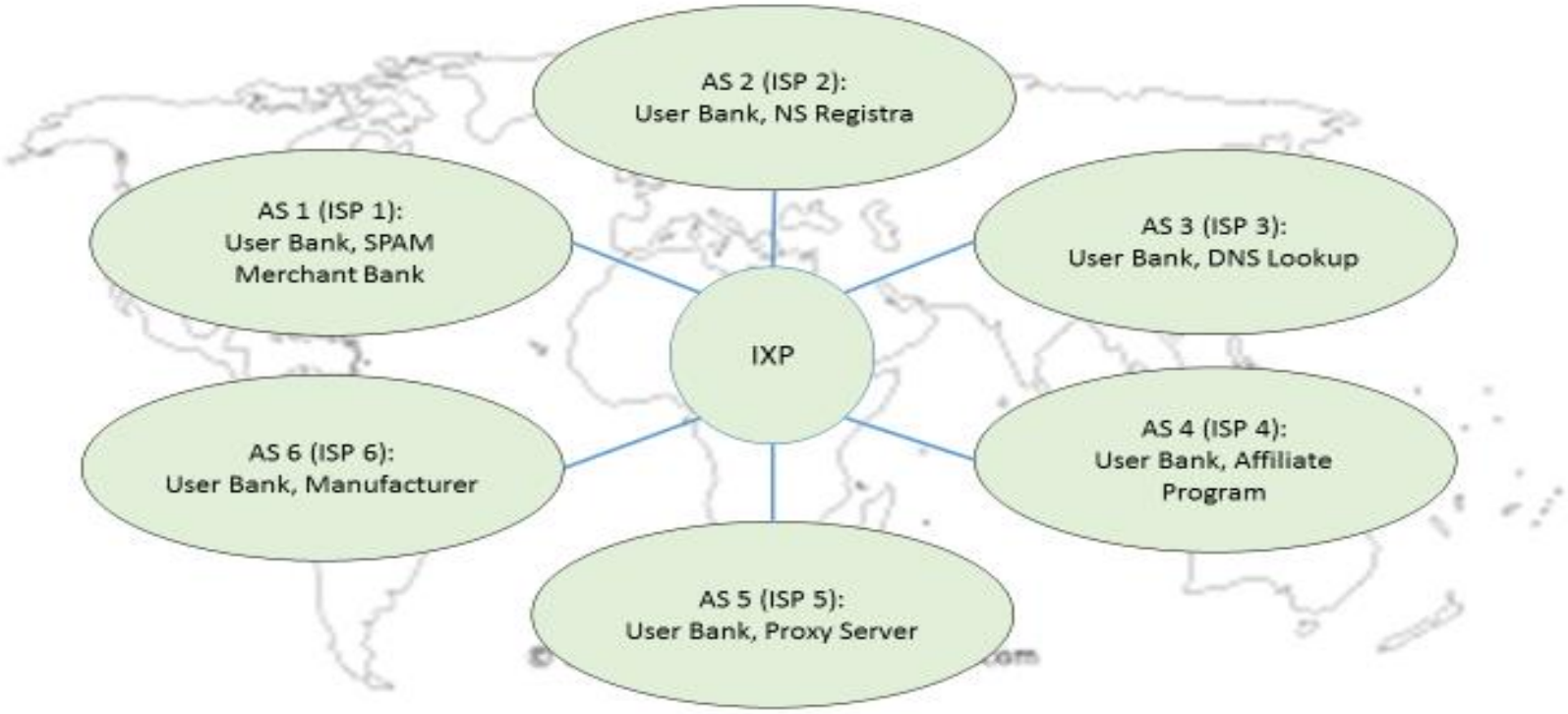


Research Method - Develop a Simulation Model

- Network topology:
  - Modeled at the autonomous system (AS) level
  - Each AS includes at least one entity of the spam supply chain network.
- Assumptions:
  - Bots are the production source of spam emails in each AS.
  - Each AS is assumed to represent an ISP and also a country
  - Each continent/country includes an actor of SPAM value chain
  - Each ISP connects both bots and benign nodes

Research Method: Develop a Simulation Model

The high-level view needs more detailing of various parameters.



Research Method - Conduct Simulations

- Based on the popular open source software, OMNET++,
  - Allows simulation of complex systems.
  - Supported by a number of software libraries such as INET and ReaSE

Thank you.