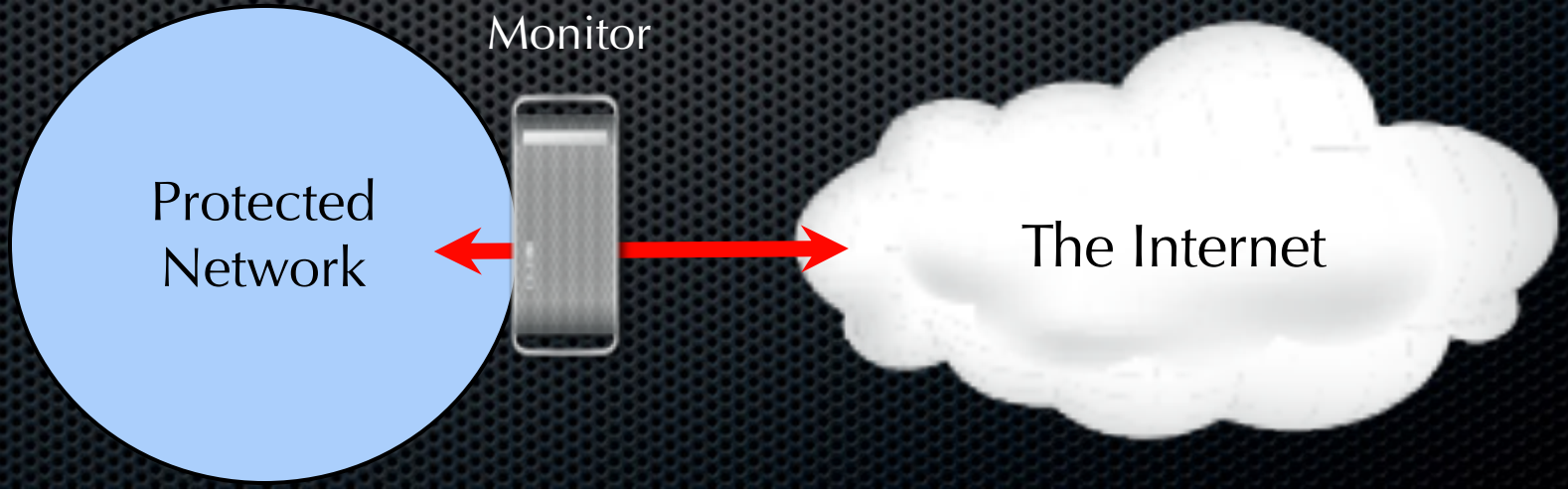
Behavior-Based Internet Worm Detection

- *Problem*: We can detect Internet worms based on their signatures, but not *0*-day worms and polymorphic worms. Traffic content inspection is also costly.



Behavior-Based Internet Worm Detection

- *Research*:
  - We compared state-of-the-art behavior-based worm detectors.
  - We designed a new behavior-based worm detector.

Shad Stafford and Jun Li, "Behavior-based worm detectors compared," in 13th International Symposium on Recent Advances in Intrusion Detection (RAID), Ottawa, Canada, September 2010, p. 20 pages.

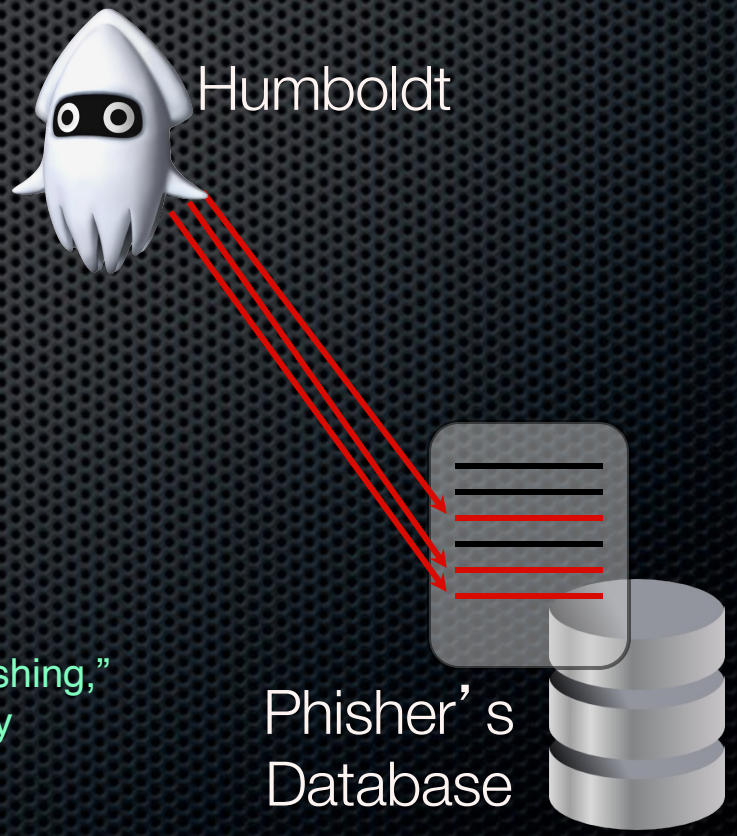
Jun Li, Devkishen Sisodia, and Shad Stafford, "On the detection of smart, self- propagating Internet worms," IEEE Transactions on Dependable and Secure Computing (TDSC), vol. 20, no. 4, pp. 3051–3063, July-August 2022.

Active Phishing Disruption

- *Problem*: No matter how good a phishing detection solution is, phishers can always find victims.

Active Phishing Disruption

- *Research objective*: Being able to Inject fake credentials to phishing sites, and to detect the usage of such credentials.
- *Challenge*: Must ensure phishers won't detect which credentials are from real victims and which from us.



Jason Gustafson and Jun Li, "Leveraging the crowds to disrupt phishing," in First IEEE Conference on Communications and Network Security (CNS), Wash- ington, DC, October 2013, pp. 82–90.

Paul Knickerbocker, Dongting Yu, and Jun Li, "Humboldt: A distributed phishing disruption system," in The Anti-Phishing Working Group eCrime Researchers Summit, October 2009.

Trusted and Incentivized Peer-to-Peer Data Sharing Between Distrusted and Selfish Clients

- *Problem*: When the clients of a server share the downloaded data between them, every client must be able to ensure that
  - the data it receives from a peer client is authentic, *and*
  - its providing data to others can be reliably credited.

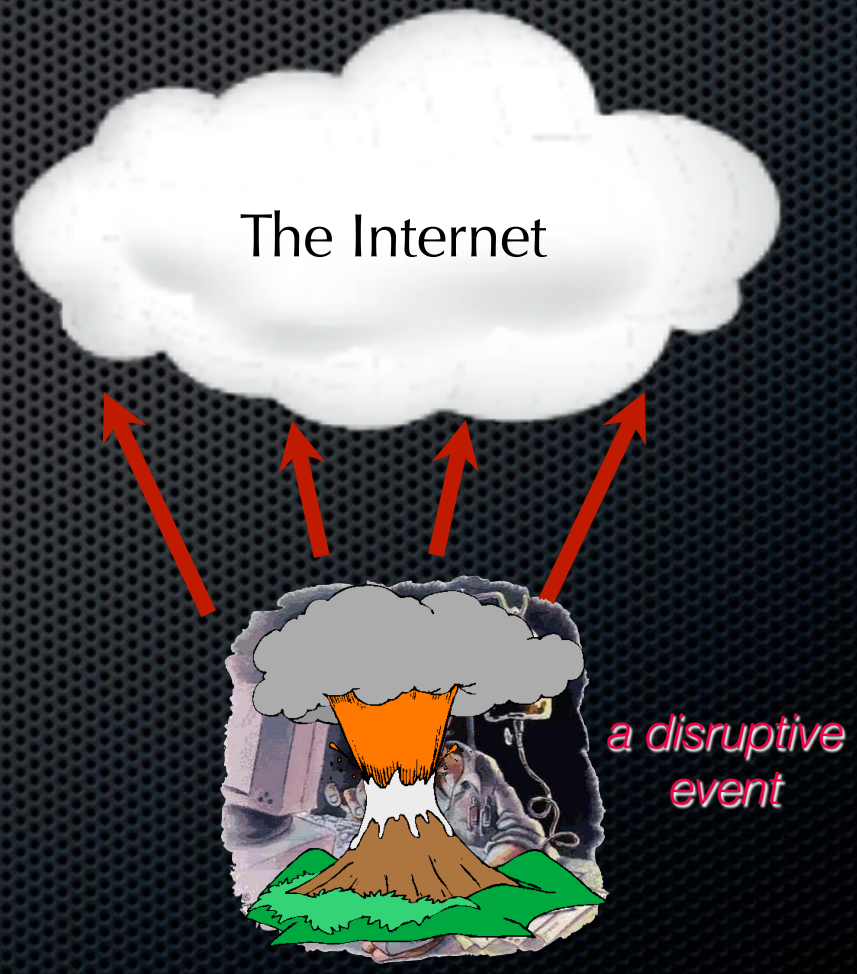
Trusted and Incentivized Peer-to-Peer Data Sharing Between Distributed and Selfish Clients

- *Research*:
  - We designed a highly efficient and flexible solution for a client to verify data integrity.
  - We also devised a proof-of-service protocol for a provider client to obtain an accurate proof for its data sharing service.

Jun Li, "mSSL: A framework for trusted and incentivized peer-to-peer data sharing between distrusted and selfish clients," Peer-to-Peer Networking and Applications, Accepted: 27 June 2010.

Internet Routing Forensics

- *Problem*:
  - Is the Internet resilient to various disruptive events such as large-scale power outage or security attacks?
  - Can we monitor, detect, classify, and quantify the impact from such events?



Internet Routing Forensics

- *Research*:
  - We designed the Internet routing forensics framework.
  - We measured Internet routing (mainly BGP) dynamics.
  - We developed an *Internet seismograph* to measure "Internet earthquakes."

Mingwei Zhang, Jun Li, and Scott Brooks, "I-seismograph: Observing, measur- ing, and analyzing Internet earthquakes," IEEE/ACM Transactions on Network- ing (ToN), vol. 25, no. 6, pp. 3411–3426, December 2017.

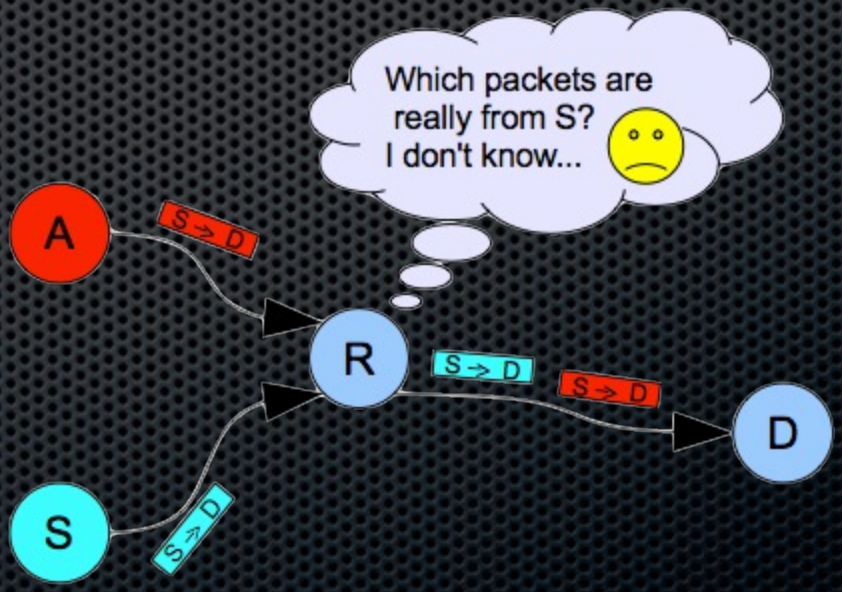
Jun Li, Dejing Dou, Zhen Wu, Shiwoong Kim, and Vikash Agarwal, "An Internet routing forensics framework for discovering rules of abnormal BGP events," ACM SIGCOMM Computer Communication Review, vol. 35, no. 5, pp. 55–66, Octo- ber 2005.

Jun Li, Michael Guidero, Zhen Wu, Eric Purpus, and Toby Ehrenkranz, "BGP routing dynamics revisited," ACM SIGCOMM Computer Communication Review, vol. 37, no. 2, pp. 7–16, April 2007.

Jun Li and Scott Brooks, "I-seismograph: Observing and measuring Internet earth-quakes," in Proceedings of Infocom, April 2011, p. 9 pages.

IP Spoofing Prevention

- *Problem*: The source address of IP packets can be easily forged.



IP Spoofing Prevention

- *Research*:
  - We surveyed the state of IP spoofing defense.
  - We designed solutions for routers to build an *incoming table*, which specifies the valid incoming interface for every source address.
- *Open topics*:
  - IPv6 spoofing?

Toby Ehrenkranz and Jun Li, "On the state of IP spoofing defense," ACM Transactions on Internet Technology, vol. 9, no. 2, May 2009.

Jun Li, Jelena Mirkovic, Toby Ehrenkranz, Mengqiu Wang, Peter Reiher, and Lixia Zhang, "Learning the valid incoming direction of IP packets," Computer Networks, vol. 52, no. 2, pp. 399–417, February 2008.

Toby Ehrenkranz, Jun Li, and Patrick McDaniel, "Realizing a source authentic Internet," in 6th SecureComm, Singapore, September 2010, p. 18 pages.

Jun Li, Jelena Mirkovic, Mengqiu Wang, Peter L. Reiher, and Lixia Zhang, "SAVE: Source address validity enforcement protocol," in IEEE INFOCOM, New York, June 2002, pp. 1557–66.

Reliable IP Prefix Monitoring

- *Problem*: an IP prefix (i.e., a block of IP addresses) can undergo many types of routing anomalies, which can cause loss of business, identity theft, or many other devastating effects. Unfortunately, current prefix monitoring solutions are quite limited.

Reliable IP Prefix Monitoring

- *Research Goal*: investigate, design, and evaluate a new approach to reliable monitoring of IP prefixes.
- We tackle this problem in the domain of the Border Gateway Protocol (BGP).
- *Our idea*: Surround a prefix with a buddy system, and monitor the behavior of the prefix against that of its buddies.

Jun Li, Toby Ehrenkranz, and Paul Elliott, "Buddyguard: A buddy system for fast and reliable detection of IP prefix anomalies," in 20th IEEE International Conference on Network Protocols (ICNP), Austin, TX, October 2012, 10 pages.