R209 Essay: Security Economics

Chongyang Shi (*cs940*)

October 24, 2017

1 Summaries of research

The review paper by Anderson and Moore [1] examined the emergence of economical and psychological view points in security research, motivated by the fundamental issue of misplaced liabilities in information security. Starting with economical view points, the paper first discussed misaligned incentives caused by widespread hidden information and hidden actions in security interactions. Next examined were negative effects of security externalities. Different approaches in handling vulnerability disclosures and their economical effects were then discussed. Potential of applying economical and legal measures to protect online privacy of users, as well as topologies of social networks modelling conflict dynamics were noted. Finally, on the influences of psychology on security, the paper discussed security issues that could be explained through psychology analysis such as social engineering and exaggerated perception of risk.

Van Eeten et al. [2] performed statistical analysis on trapped spam data to confirm the control point roles of internet service providers (ISPs) in efforts against email spamming. The authors determined that many ISPs are not making sufficient efforts towards controlling botnet-initiated spams within their network, often a result of economical or regulatory constraints. Based on additional data sourced within a wide range of areas, the authors were also able to prove or disapprove hypotheses about factors contributing to level of spam activity, such as sizes of the ISPs and the average level of education of users. The authors concluded by suggesting areas where solutions could be sought to improve spam mitigation. A possible extension to the analysis performed is determining whether ISPs in dominant or monopolistic positions of markets perform differently to ISPs that are merely large in their market.

The book chapter by Anderson et al. [3] produced a general analysis on the cost of cybercrime to both the world and the UK's economy, and examined a previous disputed estimate of annual cost of cybercrime to the UK. The authors first justified a new framework for differentiating cybercrime and decomposing the cost, different from the framework used by the previous estimation. Each category of cybercrime in the framework's cost decomposition was then carefully analysed, and an estimation was produced based available data with varying uncertainties. Costs generated by identifying and removing infrastructures supporting cybercrime were also considered. An estimate of cost of cybercrime was produced on a type-by-type basis, while it was noted that a summational figure could not be produced beyond magnitudes due to the uncertainties in individual estimations. A potential addition to the conclusion is discussion on whether the magnitudes produced may confirm or refute the previous disputed estimate.

2 Key themes of research

2.1 Legal and regulatory approaches can be insufficient or misaligned

It was noted in all three research efforts that legal and regulatory powers have been applied by states in an effort to combat cybercrime, but they are often misaligned and insufficiently effective. Anderson and Moore [1, Sec. 4] observed that due to the lack of vendors' liabilities on vulnerabilities in their software, consumers often bear the blunt of impact when exploits are exposed. Van Eeten et al. [2, p. 13] also noted that in the context of spam mitigation, country-level measures are insufficient without creating incentives for ISPs to oblige, and the incentives themselves may cause contradictory effects. Anderson et al. [3, 12.6] concluded their chapter by noting the importance of changing regulatory focus from mitigating the effects of cybercrime to catching the perpetrators.

2.2 Users insufficiently care about their privacy and security

Many users interact with security economics due to their carelessness in protecting their online privacy and security. Anderson and Moore [1, Sec. 1] noted that users introducing infected devices into a network may not be aware of their actions, and that users often undervalue the privacy of their data in the face of short-term benefits [1, Sec. 5]. In addition to concurrence with the first observation by Anderson and Moore, Van Eeten et al. [2, p. 2, pp. 19-24] discussed the effects of a higher average level of education on user awareness of malware risk. Anderson et al. [3, 12.3.2, 12.3.8] observed the large number of users tricked into disclosing online banking credentials, or into sending money to scammers.

2.3 Misplacement of liabilities is a source of imbalance in risk

There is often significant imbalance in risk of cybercrime between parties of a transaction, as a result of misplacement of liabilities. Anderson and Moore [1, Sec. 2] observed that liability rules have been shifted in favour of the banks during the transition from branch banking to online banking, which also unexpected resulted in an increase in fraud prevention spending by UK banks. In the book chapter, Anderson et al. [3, 12.3.1] also noted that banks reduced their losses in card frauds partly because liabilities were dumped on merchants and cardholders. Van Eeten et al. [2, p. 3] examined whether an ISP should be assigned liability to spams originated from infected machines in their network, but noted that many ISPs are voluntarily taking on the liability by paying the cost of assigning staff to alert customers.

3 Ideas of current context

Anderson and Moore [1, Sec. 5] noted the ever stronger incentives for firms to collect customer personal information in 2009. Capabilities of customer personal information have increased significantly since then, with vast increases in adoption of smartphones and wearable technologies. Through a wide range of onboard sensors and APIs, information of the user can be collected efficiently [4], and potentially without the user's knowledge (such as identifying what

a user has typed on the keyboard through an accelerometer on their smartwatch). Permission controls partly mitigated this issue, but are subject to bypass vulnerabilities [5].

Also noted by Anderson and Moore [1, Sec. 3] was the pattern of vendors locking down a platform through excessive security, this is an ongoing issue with both Apple and Android platforms. Lock downs have caused effects opposite to security, such as security vulnerabilities on Android devices caused by vendors not providing system updates after sale [6], due to the heavy fragmentation of the Android market.

Anderson et al. [3, 12.6] stressed the importance of states putting more efforts into catching perpetrators behind cybercrime. While slow progress have been made since 2012, the emergence of terrorism threats motivated governments into disputes with the technology sector about the use of end-to-end encryption implemented in popular messaging applications. Whether their efforts are misplaced is a topic of ongoing discussion [7].

4 Literature review

Heightened awareness of organised cybercrime suggested by Anderson and Moore [1] was reflected in a study of public privacy concerns in European countries by Miltgen and Peyrat-Guillard [8]. The concept of insuring vulnerabilities has been further developed through game theory, with possible business models suggested [9]. The importance and implications of psychological factors in the user's approach to security have been further studied by Baddeley [10].

Analysis by Van Eeten et al. [2] provided a reference figure for Anderson et al. [3, 12.4.1] in botnet distributions. Broader issues in internet governance was later raised by Van Eeten and Mueller, inspired by the observed voluntary collaborations between ISPs in controlling spam [11, p. 730]. A model in spam intervention strategies was developed by Hofmeyr et al. [12], suggesting that it would be more effective for large ISPs to simply block malicious traffic rather than attempting end-user remediations.

Soska and Christin [13] utilised similar methods to Anderson et al. [3] to measure the growth of anonymous online marketplaces. A research report for the Home Office [14] recognised the cost estimation method used by Anderson et al., while also raising its limitations, and drawing attention to non-financial impacts of cybercrime as well. Findings by Anderson et al. about users limiting online activities due to cybercrime risks [3, 12.3.2] was also reflected in the study of search engine poisoning by Leontiadis et al. [15], with the belief that it is important to maintain users' trust in search engines.

(1239 words according to texcount.)

References

[1] R. Anderson and T. Moore, "Information security: where computer science, economics and psychology meet," *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 367, no. 1898, pp. 2717–2727, 2009.

[2] M. Van Eeten *et al.*, "The role of internet service providers in botnet mitigation an empirical analysis based on spam data," 2010.

[3] R. Anderson *et al.*, "Measuring the cost of cybercrime," in *The economics of information security and privacy*. Springer, 2013, pp. 265–300.

[4] D. T. Wagner *et al.*, "Device analyzer: Large-scale mobile data collection," *ACM SIGMETRICS Performance Evaluation Review*, vol. 41, no. 4, pp. 53–56, 2014.

[5] Z. Fang *et al.*, "Permission based android security: Issues and countermeasures," *computers & security*, vol. 43, pp. 205–218, 2014.

[6] X. Zhou *et al.*, "The peril of fragmentation: Security hazards in android device driver customizations," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 409–423.

[7] S. Sharwood, "Uk spookhaus gchq can crack end-to-end encryption, claims australian a-g," July 2017. [Online]. Available: https://www.theregister.co.uk/2017/07/14/uk_spookhas_gchq_can_crack_endtoend_encryption_says_australian_ag/

[8] C. L. Miltgen and D. Peyrat-Guillard, "Cultural and generational influences on privacy concerns: a qualitative study in seven european countries," *European Journal of Information Systems*, vol. 23, no. 2, pp. 103–125, 2014.

[9] R. Pal and P. Hui, "Cyberinsurance for cybersecurity a topological take on modulating insurance premiums," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, no. 3, pp. 86–88, 2012.

[10] M. Baddeley, "Information security: lessons from behavioural economics," in *Workshop on the Economics of Information Security*, 2011.

[11] M. J. Van Eeten and M. Mueller, "Where is the governance in internet governance?" *New Media & Society*, vol. 15, no. 5, pp. 720–736, 2013.

[12] S. Hofmeyr *et al.*, "Modeling internet-scale policies for cleaning up malware," in *Economics of Information Security and Privacy III*. Springer, 2013, pp. 149–170.

[13] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem." in *USENIX Security Symposium*, 2015, pp. 33–48.

[14] M. McGuire and S. Dowling, "Cyber crime: A review of the evidence," *Home Office Research Report*, vol. 75, 2013.

[15] N. Leontiadis *et al.*, "A nearly four-year longitudinal study of search-engine poisoning," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 930–941.